

BOURDIEU AND PRIVACY AS CONTEXTUAL INTEGRITY

Adam Molnar

PhD Student

Department of Political Science

University of Victoria

Engaging Privacy: Module One Paper

Please do not cite without permission of the author

apm@uvic.ca

Introduction

The development of privacy theories has been predominantly tied to North American legal theoretical traditions. From Warren and Brandeis' (1890) pioneering '*Right to Privacy*', Alan Westin's (1967) claims of informational privacy, to Richard Posner's (1978) understanding of privacy on economic-institutionalist terms, these cornerstones of privacy thought all maintain close ties with their liberal-democratic legal and economic foundations.

It comes as little surprise, then, that theories of privacy have rarely been explored through the epistemological lineages of European social theory. Indeed, social theory of all forms is underrepresented in the realm of privacy. Accordingly, this paper takes up the opportunity to bridge privacy literatures with European social theory. Helen Nissenbaum's notion of "privacy as contextual integrity" provides an excellent entry point for an exploration of privacy through the lens of social and political philosophy.

Nissenbaum does not seek to develop a full theory of privacy; rather, she provides a theoretical account of a right to privacy as it applies to the cultural values of information sharing between individuals. Nissenbaum's argument borrows heavily from Pierre Bourdieu's trademark social theoretical concepts of social space as field, domains and contexts (Bourdieu and Wacquant 1992). On this basis, Nissenbaum's argument is more concerned with the spatially bounded normative implications of information exchange and how normative positions concerning privacy are themselves culturally produced, stratified, differentiated, and also (crucially) context-specific.

In addressing the underrepresentation of social theory in privacy literatures, this paper engages in a critical social theoretical analysis of Helen Nissenbaum's notion of privacy as "contextual integrity". I begin with a brief summary of Helen Nissenbaum's idea of "privacy as contextual integrity," drawing significantly on social theoretical ideas of context, spheres, or fields. This section details the two main normative principles that Nissenbaum argues regulate acceptable modes and practices of informational exchange.

I follow up Nissenbaum's account by returning to the roots from which it draws most heavily: the core concepts comprising Pierre Bourdieu's theory of social practice. In this section, I unpack Bourdieu's notion of social practice, formulaically expressed as, $[(habitus)(capital)] + field = practice$. After briefly exploring habitus, capital and field respectively, I examine how Nissenbaum's argument of privacy as contextual integrity aligns with Bourdieu's theory of social practice. Here, I argue that Nissenbaum's "privacy of contextual integrity" could be further supplemented by the concept of symbolic, cultural and economic capital that was also so central to Bourdieu's theory of social practice. I argue that Nissenbaum's selective reading of Bourdieu leads to a limited account of 'context', subsequently leading to a reductionist account of "privacy as contextual integrity".

Subsequently, I argue a return to the social and philosophical foundations of Nissenbaum's own argument reconfigure our understanding of privacy as contextual integrity. The discussion in the final section raises both theoretical and substantive implications of how Nissenbaum's approach be reconfigured on Bourdieusian terms. In the conclusion, I address how this speaks to the overall role of social theory in informing theoretical approaches to privacy.

Nissenbaum: Privacy as Contextual Integrity

Nissenbaum proposes two main kinds of informational norms that characterize “privacy as contextual integrity”. First, norms of *appropriateness* “dictate what information about persons is appropriate, or fitting, to reveal in a particular context” (Nissenbaum 2004: 120). For example, in medical contexts it might be appropriate for an individual to share intimate personal details about his or her physical health, but this information sharing would not be reversed. The core point is that informational norms govern, shape and constrain the sharing of information within particular places; therefore, the misappropriation of information from one individual to another in specific contexts can violate appropriate norms of confidentiality and reasonable expectations of privacy in our social relationships.

The second main kind of informational norms that comprise the “privacy as contextual integrity” framework are norms of *distribution*. Norms of distribution involve the “movement, or transfer of information from one party to another or others” (Nissenbaum 2004: 122). Drawing on normative-philosophical ascriptions of justice (Walzer 1983), Nissenbaum directs attention to how contextual norms of appropriateness also regulate the distribution or flow of information across multiple and discrete “distributive spheres”. These spheres are each uniquely conditioned through differentiated sets of normative accounts of justice (Nissenbaum 2004: 122). Understanding privacy on the basis of distributive principles provides explanations of not only whether information is appropriate or inappropriate in a given context, but whether the distribution of information upholds contextual norms of information *flow* (Nissenbaum 2004: 123). Examples here are also profuse. For instance, it is normatively inappropriate for information collected on public electronic health records to be distributed to insurance agencies in order to influence the differential value and distribution of insurance plans to customers.

For Nissenbaum then, privacy is (a) circumscribed by context-dependent norms implicated in both the appropriateness of the information exchange *internal* to context, and is also (b) governed by normative expectations of acceptable exchanges (distribution, flow) of information *across* contexts. Thus, a normative account of privacy understood through the lens of contextual integrity holds that privacy violations result when norms of appropriateness *internal* to context or when norms of information flow *across* contexts have been disrupted.

Privacy as contextual integrity is distinct from other accounts of privacy rights in two main ways. First, it ‘solidifies’ personal information within the context of its communication or revealing. That is, it involves a close attention to the particulars of social context including the dispositions of the individuals implicated in the context when evaluating privacy breaches. Second, norms are relative (i.e., non-universal) in this framework. Because the very scope of informational norms are always considered in an internal relation to the context itself, privacy is contingent on the normative dispositions of those implicated in the information exchange and the routinized institutional practices that govern informational exchange.

The benefits of Nissenbaum’s social theoretically bound approach are readily apparent. Privacy as “contextual integrity” offers up much in the way of ‘rounding out’ legal-reductionist accounts of privacy that rely on previous case-law as a referent for distinguishing and adjudicating breaches of privacy. The problem with the legal reductionist approach to privacy, most thoroughly identified by Ruth Gavison (1980), is that broader contextual factors recede from (or are absent altogether) from analysis in place of a more narrowly defined scope of privacy that relies on strict legal protections for privacy. Here, legal decisions reign supreme in delineating the basis for definitions

of privacy. Gavison argues that this approach reduces privacy to decisions on a limited number of principles of liability, thereby allowing judges and lawyers to rely on legal tradition as the benchmark for subsequent claims to privacy invasion. Taking judicial decisions as a starting point in evaluating privacy concerns leads us down the path of narrow understandings of privacy that are devoid of 'external' theoretical and ontological examination. It is worth noting here that my own position in acknowledging this aspect of Nissenbaum's argument is not to deny importance of regulatory mechanisms around fair information practices. Rather, I argue that the complexities of (un)acceptable modes of information exchange are often more complex than simple case-law discourses that rely on zombie legal-philosophical concepts such as the 'public-private divide'.

In any case, Nissenbaum's attention to context-dependent normative dimensions of privacy is a powerful antidote to case-law reductionism of privacy concerns.¹ Her 'extra-legal' contribution to understandings of privacy foregrounds the social embeddedness of cultural and normative properties of privacy in context-specific orders. The advantages of Nissenbaum's framework, however, are limited by her reliance on a narrow version of social reality. Before turning to this particular critique of Nissenbaum's framework from a social theoretical perspective, I raise some common critiques of "contextual integrity" from the standpoint of more traditional privacy literatures.

Privacy theorists and advocates would likely criticize Nissenbaum's framework of "contextual integrity" as a relativist and conservative offering. They would argue first that it is an unconvincing resource for developing morally prescriptive analyses regarding information exchanges and reasonable expectations of privacy (see also Kerr 2007). As a praxis based account of information exchange and "normative appropriateness" on an individual basis, the theory of contextual integrity is left open to charges of conservatism since it establishes a normative presumption in favour of the status quo—only shared between individuals. That is to say, it fails to account for the differential power relations that inflect all debates concerning informational exchange, primarily those established by the institutions and organizations that establish the normative 'rules of the game' regarding the use of new media technologies. The point here is that the basis for "norms of appropriateness" concerning information exchange might be conditioned to a greater effect through ideas about consumerism rather than ideas about human rights, justice, and informational exchange.

It seems as though Nissenbaum's understanding of norms are devoid of cultural *content*. A key question here is: how does the cultural and economic system structure whose norms are considered legitimate or hegemonic? Nissenbaum's inattention to the stratification of normativity,

¹ Indeed, it could be argued that Daniel Solove's (2006) attempt at developing a taxonomy of privacy for legal audiences might also succumb to a sort of legal-reductionism (see Parsons this course!). I am inclined to believe that Solove has not committed a categorical error that over-extends case law as a substitute for normative values. Neither is Solove actually expecting legal definitions of tort law to do the explanatory work of culturally situated normative ascriptions of privacy. Solove is mounting a strategic attempt to address, and reverse, how more "abstract incantations of the importance of privacy" generally fail when pitted against more concretely stated (legalistic) countervailing interests. I would argue this issue speaks mainly to the challenge of bridging legal-juridical discourses with social theoretical discourses on privacy. Put another way, the pedagogical significance of privacy concerns when understood through social theoretical arguments should have a place in the judicial sphere. This is, in part, Nissenbaum's purpose. The extent that the receiving audiences (academics vs. judges, lawyers, and so on) draw on different sets of epistemological and discursive referents for their explanations, the insulated social and intellectual fields of each does much to constrain the ability to develop and utilize a robust notion of privacy.

and how norms themselves are inflected with different forms of power, limits the degree to which we might understand invasions of privacy as not merely the direct result of normative transgressions. Violations of privacy can also be understood in a productive sense—through a whole host of other factors, and are only partially related to how norms of appropriateness govern informational distribution.

I argue that Nissenbaum's conclusion is the result of a reductionist account of social reality—or contexts. Indeed, Nissenbaum clearly states "there is no need to construct a theory of these contexts", casting her intellectual lot in the position that "it is enough for our purposes that the social phenomenon of distinct types of contexts, domains, spheres, institutions, or fields is firmly rooted in common experience" (Nissenbaum 2004: 119). It seems odd that since a notion of context is the core principle of Nissenbaum's theoretical framework, not only is it not reflected upon, we are *encouraged* that we need not explore what we might take to be included in context. This should not be our worry, we are told; this "work has already been done by social theorists and philosophers"! (Nissenbaum 2004: 119). Nissenbaum makes a claim for the significance of social philosophers, yet they remain remarkably underexamined in her article. In any case Nissenbaum provides justification for drawing on social theoretical accounts, noting that "any of these sources could provide foundational concepts for articulating the concept of contextual integrity in relation to personal information" (Nissenbaum 2004: 119-120).

Indeed, Nissenbaum's claim for the significance of social theory in articulations of privacy is just such a proposition that I take up in the following section. To close this section, however, I argue that Nissenbaum's reliance on a weak notion of context seems a peculiar basis for unpacking the core tenets of privacy as contextual integrity. To borrow a line from Lane (2000), my concern is that there is "a danger in confusing this model of reality for the reality of the model". Put another way, a reduced understanding of context to the strata of norms presents a weak understanding of how it is not only normative positions that govern information exchange. It might be argued that 'ideas about privacy' or 'privacy literacy' have a partial impact on the appropriateness of information exchange, where other social forces might be regarded as a presupposition to our normative position. To remedy this shortcoming, I examine Nissenbaum's framework of "contextual integrity" in spirit of the social theoretical foundations upon which it rests, which are underexplored in her paper.

As mentioned at the outset of this paper, Nissenbaum's conceptual apparatus is largely derived from Pierre Bourdieu's *leitmotif* of "*field theory*". With the concept of "*field*", Bourdieu aimed to map objective structural relations and show how such objectivity was also constructed by individual subjectivities. One of the core components of this Bourdieusian methodological approach to understanding context is to consider the structure and operations of fields (Nissenbaum's "context" or "spheres") as "Field mechanisms" (Bourdieu 1989).

On Bourdieu's terms, Nissenbaum's appropriation of field or context is rather dubious, and I argue, leads to an oversimplification of Bourdieu's framework that also hinders Nissenbaum's own notion of privacy as contextual integrity. Simply put, rearticulating Nissenbaum's conceptual apparatus with Bourdieu's critical methodological approach provides an interesting opportunity to incorporate some forgotten elements of *context* that allow for an immanent critique, revision and extension of Nissenbaum's understanding of privacy as contextual integrity.

More specifically, I argue that a failure to understand how norms of appropriate information exchange are articulated with forms of capital leads to a limiting account of privacy as contextual

integrity. If privacy is understood merely as normative appropriateness, “reasonable expectations of privacy” are surely to be eroded on the basis of the power of capital to shape the field of new information technologies as well as the dominant cultural frames (predominantly structured around discourses of consumerism) that establish the parameters for appropriate information exchange.

Bourdieu, Privacy and the Reconstruction of Contextual Integrity

This section deals more closely with a truncated version of Bourdieu’s theory of social practice. In what follows, I discuss the key concepts associated with Bourdieu’s theory of practice, specifically the role and function of *habitus*, *capital*, and *field*. I argue that a return to Bourdieu’s understanding of social practice allows us to recover absent and undervalued aspects from Nissenbaum’s account of privacy as contextual integrity that might serve as a basis for its reformulation.

Summarizing Bourdieu’s theory of social practice

Bourdieu reconfigures the conventional agency/structure divide with an alternative methodology that understands the co-production between *field*, *capital*, and *habitus*. It is expressed in a tight formulation as:

$$[(\textit{habitus})(\textit{capital})] + \textit{field} = \textit{practice}$$

The idea of *habitus* is the first key concept that was developed in Bourdieu’s methodology. Habitus refers to a property of social agents that:

...expresses first the *result of an organizing action*, with a meaning close to that of words such as structure; it also designates a *way of being, a habitual state* (especially the body) and, in particular, a *predisposition, tendency, propensity or inclination*.

(Bourdieu 1977: 214)

The habitus refers to the “structured and structuring predispositions” of an embodied agent. It gets at the institutionalization of habits, dispositions and norms and therefore conditions the realization of social practice. In Nissenbaum’s framework the habitus is the subjective realm that embodies norms and values that govern the appropriate forms information exchange.

Capital, by contrast, is implicated in the process of how all agents in a social space occupy an objective position that is conditioned through various forms of economic and cultural capital. For Bourdieu, power and dominance is derived through the distribution and possession of both material resources, as well as, cultural and social resources, as capital. The concepts of *cultural*, *social* and *symbolic capital* are the key features that distinguish Bourdieu’s approach from

orthodox Marxist approaches that rely on materialist reductionist accounts of economic capital and class.

Symbolic capital refers to a few different forms of capital. First, symbolic capital refers to values, tastes, and lifestyles of some social groups (embodied in the habitus, but held in common between various group formations that often reflects the differential distribution of power relations) in society in ways that confers social advantage over others. One example of this form of social capital is educational attainment, or particularized knowledge that conditions our general “ways of getting on” in the world. It is worth noting that internal stratification of group formations along the lines of cultural and social capital leads to differing enabling or constraining capacities of individuals and groups to act. That is, not all forms of habitus are accorded an equal value of cultural capital in society—both within and between various group formations.

Accordingly, Bourdieu’s identification of multiple forms of capital is more attentive to the complexities of social stratification. On the one hand, capital is *objectified*. That is, it is represented in material terms as artifacts, such as technologies, books, galleries, museums, and so on. In another form, capital is *embodied*. That is, the conditions of the field are incorporated into the corporeal elements of the body and consciousness, such as the habitus, expressed through the attitudes or disposition of persons. These forms of capital are mutually constitutive or co-productive and condition the “rules of the game” (Bourdieu 1984: 71).

Bourdieu’s theory of capital then, refers not only to the conditioning influences of the *habitus* through norms, values, tastes and attitudinal dispositions, but also serves as a means for understanding the significance of how cultural processes contribute to hierarchies of discrimination. Such hierarchies are reproduced in part through the differential distribution and enactment of various forms of symbolic capital in particular social spaces. Simply put, symbolic capital serves as a sort of asset that enables social and cultural advantage or disadvantage.

In this way, symbolic capital is also coterminous with the structure of the economic field. Fields of symbolic capital are implicated with the underlying objective structure of unequal economic relations (resource-to-resource relations, class and power). Here, symbolic and cultural capital has a role to play in reproducing fundamental economic structures of social inequality (Moore 2008: 104). Bourdieu might also put this in different terms, by explaining that the economic capacity of different individuals, groups and institutions structures the field of symbolic capital. This, in turn, inculcates the *habitus* (including the normative dispositions) of agents and the broader conditions of the field.

Bourdieu’s notion of *field* (as social space or ‘context’) should be relatively straightforward by now and so deserves less descriptive attention. The idea of *field* explains how certain contexts are shaped by their own rules, histories, and roles that are also inflected with different forms of cultural and economic capital. Social spaces, *fields*, or contexts, can be thought of as relatively self-contained social spaces and are governed by common sets of practices that function to reproduce power relations. Power relations in the field refer to how the occupation of social positions is each accorded different amounts and kinds of cultural and economic capital. And finally, *fields* are many. Each has their own “distinction” (Bourdieu 1984); thus, religious, IT, economic, legal, and engineering fields are governed through a common set of social, cultural and economic practices. This is what offers the uniquely bounded character of the field as a methodological limit on the explanatory frame.

Reviewing the facets of Bourdieu's theory of social practice points to how we might begin to understand a model of informational privacy in terms of a reconfigured notion of privacy as contextual integrity. Thus, I argue for a deeper appreciation for the social theoretical foundations that Nissenbaum's theory draws on. Bourdieusian social theory is a valuable addition for developing currently under-theorized elements of privacy as contextual integrity. Below I describe a theoretical and methodological toolkit for developing a more robust notion of privacy as contextual integrity.

Reconfiguring Privacy as Contextual Integrity

Bourdieu's analysis opens us up to considering how different forms of capital are at work in the contexts of information exchange and concerns of privacy. First, it offers a critical interrogation to how "norms of appropriateness" are themselves shaped and constrained by various forms of capital within specific fields or contexts, thereby introducing an understanding of *power* in the framework of privacy as contextual integrity. In what follows, I draw on the analytical resources provided by both Nissenbaum and Bourdieu and explore an example that illuminates how "norms of appropriateness and distribution" are not immune from forms of symbolic, cultural and economic capital.

On June 9, 2009, the Office of the Information and Privacy Commissioner of Ontario (OIPC) held a public event that announced a new joint partnership with McAfee, a large Internet security firm. The partnership, Dr. Ann Cavoukian, OIPC Commissioner stated, "will elevate the level of privacy protection locally by adding privacy to the security protections presently offered by McAfee" (Kavur 2009).

The event however, was also meant to serve as a product launch for McAfee's latest Internet security software for families (Kavur 2009). This latest addition to McAfee's line of internet filtering software monitors and records instant messaging (IM) conversations and social networking posts, provide website and email blocking, and is able to limit amounts of time children spend online. Overall, McAfee is offering surveillance capacities to parents that make them able to ascertain a "complete review of all internet usage activity and IM activity" (McAfee website).

Ross Allen, General Manager for McAfee, was at hand for the OIPC event. Summarizing the firm's position on youth internet use and security concerns, Allen stressed "any threats now come through our children visiting legitimate Internet sites which cybercriminals have hacked into" (Kavur 2009). Parry Aftab, family Internet safety advisor to McAfee and chairman of the McAfee Consumer Advisory Board further adds that "the single most important factor in determining how at risk kids are is the amount of time they are online ... too much time means too much time to get into trouble" (Kavur 2009).

For McAfee and the OIPC, Internet filtering technology for parents is jointly promoted as the obvious technological solution for parents who are concerned about their child's privacy concerns. This position might seem unassuming. After all, McAfee tells us that monitoring your children not only protects them from online sexual predators and cyberbullies, but also protects parents themselves from the threats presented from their own kids -- a persuasive and convincing argument. This argument is further bolstered since it is presented by the most competent and

professional specialists when it comes to privacy and internet security—the OIPC and the Internet security specialists McAfee.

Returning to Bourdieu’s framework, we are able to see how various forms of capital are at work in this case—thereby shaping the normative appropriateness of information exchange and distribution. Recall that for Bourdieu, the political economy of symbolic power is an extension of the idea of capital to all forms of power—material, cultural, social or symbolic. That is, individuals, groups and institutions are able to draw on a range of cultural, social and symbolic resources to boost their position in the social field. In our example, McAfee is drawing on the symbolic capital of the OIPC (legitimacy, expertise, professionalism) to advance the institutional interest and strategy that is accumulated through engaging in ‘noneconomic’ activities.

Put another way, culture (which includes the very shaping of norms of appropriateness surrounding information exchange and distribution) is a *power* resource. First, the joint partnership between the OIPC and McAfee *institutionalizes* cultural capital by allocating credentials, status, and legitimacy to the solutions offered by McAfee. Second, cultural capital exists in an *objectified* form, referring to the software package itself as a technological solution that requires special cultural abilities to use. And third, the OIPC provides the legitimate symbolic platform for McAfee to cultivate the dispositions of parents in a way that reflects capital in an *embodied* state.

To state it in general terms, the economic capital of McAfee’s Internet security solutions make it more possible to shape (albeit in particularized, unstable and differentiated ways) the cultural arenas of the field of regulation of information exchange surrounding norms of privacy.

Cultural capital—like norms—is unstable and subject to resistance and displacement. In a recent email exchange on a well known Canadian privacy list-serv, University of Ottawa Professor Valerie Steeves, questioned McAfee’s assertion that more time spent online by children is what creates higher risk. Steeves went on to cite an APA meta-study finding that “the disclosure of personal information online was not associated with higher incidence of stalking and related dangers” (Steeves, email exchange). Therefore, the norms of appropriateness on information exchange that McAfee and the OIPC are promoting, expressed in the statement that an increase in the amount of personal information given online means a similarly increased risk of being attacked by a predator, are wide off the mark. Steeves also notes that the same study indicates that children who are surveilled by parents, aided through surveillance technologies like McAfee’s Internet filtering software, are “more likely to ‘misbehave’ than kids who—you guessed it—have a relationship with their parents that’s based on trust and mutual respect. Who knew?” (Steeves email).

Looking at the ways that forms of capital condition informational norms suggests that there is a distinct political and social function implicit in Nissenbaum’s idea of contextual integrity. Norms of appropriateness and distribution are contingent on various forms of symbolic and cultural capital. As such, the symbolic power of the OIPC and McAfee’s joint partnership legitimizes existing economic, cultural and political relations. Most importantly, however, the political economy of symbolic power based on the joint partnership of the OIPC and McAfee contributes to taken-for-granted assumptions about (a) what effective privacy policy is, (b) conditions the *field* of parent-child relations surrounding Internet use, and (c) ultimately conditions the norms of appropriateness surrounding information exchange and contextual integrity in favour of private economic interests.

The formulation of privacy policy that considers more deeply what we actually know about the online behaviour of children on the basis of norms of appropriateness and distribution (the constitutive features of contextual integrity) are unfortunately excluded from the discussion. In its place, policy formulation reflects the ideological interests of McAfee and subsequently leads to the reproduction of privacy policy and informational norms on the basis of marketing principles and less about what we *actually* know about the privacy behaviours of children.

Norms of appropriate information exchange (reflecting the economic interests of the private sector) are buoyed by institutionalizing and embodying forms of symbolic power. Symbolic capital, therefore, is an unassuming but powerful form of capital as it relates to the idea of privacy as contextual integrity. In this case, privacy discourses are generally restricted to the narrow confines of consumerism. As long as the OIPC and McAfee draw on the symbolic capital of internet filtering technology as the 'obvious solution' to problems of online privacy, the normative appropriateness of disclosure of personal information online will continue to be associated with higher incidence of stalking and sexualized and violent narratives of fear—accurate or not.

In addition, the policy response by the OIPC and McAfee reduces discussion of the privacy problem, and its solution, a consumerist discourse that requires a technological surveillance solution. Here, norms of appropriate information exchange are reduced to the parameters of consumerist ideologies and limits the prospects of developing informed ethical and moral debate on informational exchange. This, of course, raises a larger concern that there is a lack of democratic pedagogy that might enhance lay literacy of technological and privacy matters on different terms, arguably the role of the OIPC as a public institution.

Conclusion

The ideas presented in this exploratory paper offer a few new directions for 'engaging privacy'. First, I argue that social theory can usefully supplement existing privacy theories. Much of the privacy literatures mentioned at the outset of this paper developed from a liberal-oriented legal theoretical background and as a result, they are often lacking when it comes to relational accounts of power. Indeed, even recent attempts to theorize the gendered dimensions of privacy have largely done so without an adequate account of the field of power relations, arguably repeating past mistakes by relying heavily on legal-reductionist accounts of privacy (see Allen & Mack 1990).

On the surface, Bourdieu's theory of social practice might seem an odd addition to the chorus of voices in privacy debates. However, Bourdieu's theory offers a valuable framework for exploring the political economy of symbolic and cultural power in the development and application of privacy issues – a perspective that deserves further analytical and empirical attention in the realm of surveillance and privacy studies.

Specifically, this paper brought the significance of various forms of capital to bear on Helen Nissenbaum's theory—privacy as contextual integrity. I argued that Nissenbaum's theory summoned the theoretical resources of Bourdieu in a partial and dubious manner. As such, I urged that a recovery of the Bourdieusian social theoretical foundations of Nissenbaum's own framework would serve well for an immanent critique, revision, and extension of aspects of the privacy as contextual integrity framework. By recovering Bourdieu's concepts in a more robust

manner, I have demonstrated how the normative propositions in Nissenbaum's account remain under-developed and tend to hide as much as they reveal about normative accounts of information exchange.

I argued that informational norms governing communication exchanges and privacy are more fully understood through an understanding of how they are constituted within a field of power relations. Specifically, I argued that forms of symbolic and cultural capital are a form of power resource that structures the boundaries of what are appropriate or acceptable normative responses to privacy.

The example of the recently announced joint partnership between the OIPC and McAfee illustrates how informational norms are legitimized and supported through various forms of capital as symbolic, cultural, and economic. Accounting for forgotten understandings of capital as a power resource contributes a deeper understanding of how informational norms are institutionalized and embodied across specific sites and scales.

This way, we see how informational norms are tied to particular symbolically dominant interests in differentiated and contingent respects. The consumer based discourses on privacy advanced through the OIPC and McAfee, as Valerie Steeves has pointed out, serves to misinform and perpetuate normative principles that support the economic interests of the private sector. This comes with an opportunity cost to developing normative and policy formation that considers more deeply what we know about the online behaviour of children and how our normative principles might subsequently address the issue based on an alternative perception of the problem. One implication being that the 'consumer based' perception of the problem (conditioned by a specific set of informational norms) necessitates the obvious technological solution.

Nissenbaum's framework of informational norms would have a difficult time explaining the powerful *production* of contexts, and subsequently norms on this basis. The problem is that informational norms (and subsequently what constitutes a privacy breach) in Nissenbaum's framework are only ever understood in a reactionary sense—not in a *productive* sense—as being shaped and becoming dominant through actors' and institutions capacity to draw upon the resources of various forms of capital.

The full implications of applying critical social theories, like that of Bourdieu, in the realm of privacy still remain to be explored. Indeed, the sometimes broad conceptual abstractions inherent in social theorizing point toward a limiting element. The concern of broad abstractions is only if, however, analysts mistake what we *expect* social theories to explain about privacy. Indeed, social theory offers a useful explanatory addition for how privacy and surveillance analysts might reconfigure theories of privacy and develop subsequent methodological instruments to be used in the service of engaging privacy on more critical terms.

Bibliography

- Allen, Anita L. & Erin Mack. 1990. "How Privacy Got its Gender," *Northern Illinois University Law Review* 10: 441-78
- Bourdieu, P. 1977 [1972]. *Outline of Theory of Practice*, R Nice (trans.). Cambridge: Cambridge University Press.
- 1984. *Distinction*, R Nice (trans.). Cambridge: Cambridge University Press.
- 1989. "Social Space and Symbolic Power", *Sociological Theory* 7, 14-25.
- Bourdieu, P. and L. Wacquant 1992. *An Invitation to Reflexive Sociology*, L. Wacquant (trans.). Cambridge: Polity.
- Gavison, R. 1980. "Privacy and the Limits of Law" *The Yale Law Journal*, Vol. 89(3).
- Kavur, J. 2009. "McAfee launches software that monitors Facebook", found online: <http://www.itbusiness.ca/IT/client/en/CDN/News.asp?id=53488>
- Kerr, I. 2007. "Emanations, Snoop Dogs and Reasonable Expectations of Privacy," *Criminal Law Quarterly*.
- Lane, J. 2000. *Pierre Bourdieu: A critical introduction*. London: Pluto.
- Moore, R. 2008. "Capital", in *Pierre Bourdieu: Key Concepts*: Acumen Press. Pp. 101-111. Michael Grenfell (ed).
- Nissenbaum, H. 2004. "Privacy as Contextual Integrity," *Washington Law Review*. Vol. 79(1): 119-158.
- Posner, R. 1978. "The Right of Privacy," *Georgia Law Review*, Vol. 12(3).
- Regan, P. 1995. *Legislating Privacy: Technology, Social Values and Public Policy*.
- Solove, D. 2006. "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, Vol. 154(3)
- Steeves, Val. 2009. *Personal email exchange*, June 10, 2009.
- Warren, S. and L. Brandeis, 1890. "The Right to Privacy" *Harvard Law Review*, Vol.4(5).
- Walzer, S. 1983. *Spheres of Justice: A Defense of Pluralism and Equality*. New York: Basic Books.
- Westin, A. 1967. *Privacy and Freedom*. New York: Atheneum Press.