TECHNOLOGY, COMMUNICATION, AND WESTERN PLURALISTIC DEMOCRACIES: ALIGNING DIGITAL PRIVACY TO FACILITATE CITIZEN-SOLIDARITY

A Thesis

Presented to

The Faculty of Graduate Studies

of

The University of Guelph

by

CHRISTOPHER PARSONS

In partial fulfillment of requirements

for the degree of

Master of Arts

December, 2007

Your file Votre référence
ISBN: 978-0-494-36556-4
Our file Notre référence
ISBN: 978-0-494-36556-4

ABSTRACT

TECHNOLOGY, COMMUNICATION, AND WESTERN PLURALISTIC DEMOCRACIES: ALIGNING DIGITAL PRIVACY TO FACILITATE CITIZEN-SOLIDARITY

Christopher Ahlric Parsons
University of Guelph, 2007

Advisor:
Professor Omid A. Payrow Shabani

This thesis is an investigation of the role of digital discourse in Western nation-states and the value of developing a privacy archetype sensitive to digital technologies. The developed archetype must enable citizens to develop solidarity without fear of surveillance while maintaining nation-states' political stability as they transition to digital communications. In making this argument, I draw on Jürgen Habermas to trace the theoretical development of contemporary nation-states and the role of non-coerced discourse in maintaining political stability. Current privacy archetypes were (partially) realized to facilitate public and private discourse and are ineffective in securing communicative privacy along digital networks. In light of Western states' adoption of digital communications technologies, I propose my reciprocal archetype of informational privacy, which can establish digital communicative privacy. My archetype shields digitized discourse from non-democratically sanctioned surveillance and supplements Habermas' political project by preserving the discursive principles beating at the of heart Western pluralistic democracies.

To my stepfather, Tim,

for inspiring me.

ACKNOWLEDGEMENTS

This work finds its origins in the discussions that I have had over the past decades with friends, family, and colleagues surrounding the roles and possible impacts of digital technology across the spectrum of daily life. I would like to thank these individuals generally and, in particular, recognize Timothy Pengelly, Brad Meszaros, Sean Yo, Brad Richard, Scott Schau, and James Dutrisac for their influences in how I approach the relationships between digital technologies and political association.

I would also like to thank my advisor, Dr. Omid Payrow Shabani, for providing me with the support and assistance that I have needed to develop and complete this project. Dr. Karen Houle has also been instrumental in guiding and refining many of the arguments and positions asserted in this text, and I am grateful for her insightful comments. Also, the conference presentations and informal discussions at 'The Revealed I' conference that was held at the University of Ottawa gave me the opportunity to test and evaluate my arguments with academics who focus on a spectrum of privacy-related topics, and was invaluable in tuning elements of this thesis.

Finally, I am indebted to my mother Joyce Parsons and my partner Luciana Daghum. My mother has tirelessly edited this work and offered poignant comments responsible for reshaping and clarifying areas of this text. Luciana has offered her encouragement, support, and thoughts throughout the development, writing, and editing processes. My thesis is stronger because of these women and the topics and issues they drew to my attention.

Table of Contents

INTRODUCTION

Technological advances over the past century have transformed how humans can communicate with one another. Whereas analogue technologies, such as writing with pen and paper, taking pictures on film, and transmitting messages using the telegraph were once the dominant ways of expressing oneself, these systems are being replaced by digital technologies, such as electronic mail (email), instant messaging, and cellular communications. Analogue and digital communication technologies are radically different from one another because analogue systems lack inherent interoperability while digital technologies are, at their most basic levels, capable of interoperability. Analogue communications technologies such as telegraphs, which create vibrations that are sent over a wire and transmitted to a receiver, and writing, which involves placing marks on a receptive medium, use divergent technological languages – telegraphs naturally deal with wave frequencies and writing with impressions on media. Digital technologies, such as email and Voice over Internet Protocol (e.g. Skype) use an identical underlying technological language – each is underwritten by the binary programming language. The process of amalgamating communications to the binary language is called digitization.[1] Digitization facilitates the development of increasingly sophisticated and interoperable digital networks – digital networks are rapidly multiplying and, with each new network, increase the efficiencies flowing from their integrated and interoperable structures.[2] As these digital networks are increasingly

[1] Vincent Mosco (2004) *The Digital Sublime: Myth, Power, and Cyberspace,* 155.
[2] Michael Hardt and Antonio Negri (2000) *Empire,* 32.

deployed, they are able to more comprehensively capture forms of discourse along their fibre-optic webs – personal correspondence, pizza orders, family photos, state secrets, political statements, and affirmations of philosophical ideals are all routinely routed along these networks. As digital systems capture more and more of people's daily discourse, it is important that we attend to the possibilities and challenges that accompany the centralization of communicative to a single medium.

In my thesis, I focus on the composition and role of discourse in political environments and the importance of establishing a privacy archetype that is sensitive and responsive to the possibilities and consequences towards discourse that accompany the digitization of communication. In chapter one, I examine the role of discourse in Western nation-states. In examining discourse's role, I turn to Jürgen Habermas' insights surrounding the development, value, and effects of civil discourse within the nation-state. By integrating the Kantian notions of right and maturity, along with Hegelian insights concerning individuals' situatedness in particular dialogical political bodies, Habermas is able to theorize about the role of discourse in establishing and recognizing norms. While in ideal situations a norm is "valid when the foreseeable consequences and side effects of its general observance for the interests and value-orientations of *each individual* could be *jointly* accepted by *all* concerned without coercion,"[3] political systems can only approximate this ideal situation. Norms in political environments are based on constitutional rights that are born from citizens' discourse. These constitutionally recognized norms function as the basis for citizen-solidarity as citizens

[3] Jürgen Habermas (1998) *The Inclusion of the Other,* 42. Hereafter referred to as IO.

internalize, argue from, and act based on these rights and their corresponding duties. While the nation-state presently faces challenges in assisting citizens to substantively realize their constitutional rights, I argue that these challenges are not chronically debilitating so long as citizens can communicate with each other without fearing the presence of illegitimate surveillance that could stunt their discourse.

Based on the role of discourse in constituting and maintaining the nation-state, in chapter two, I reflect on privacy's role in facilitating and maintaining the civic bonds of solidarity that presently exist in Western nation-states. In creating a communicative environment where citizens' communication is shielded from non-democratically legitimized surveillance, citizens are released from pressures that could inhibit their self-expression. Within these environments, people can consider, debate, and refine their political positions, befriend eclectic groups of people, or engage in unorthodox practices that promote personal fulfillment or education – in these spaces citizens can freely communicate and develop bonds with one another, as well as develop the values that will guide their life-projects and tune their political discourse. In essence, personal privacy is critical in developing the values that structure the facets composing people's lives.

In my evaluation of how people's liberties of speech have been historically shielded from unwanted interference, I examine the archetypes that protected citizens' privacy when analogue technologies were the prevalent means of communication. Through this examination, I find that each prior privacy archetype is unable to effectively recognize and respond to the challenges to privacy that arise when transitioning from analogue to

digital communications networks. Whereas analogue privacy archetypes were only marginally concerned with the possibility of all-encompassing national data aggregations, digitization has meant that privacy violations now often involve collections of massive volumes of citizens' personal data that is compiled in digital dossiers, which are stored databases that remain clouded with secrecy. Computer algorithms scan individuals' digital dossiers, and these algorithms' computations lead to discriminatory practices without individuals ever knowing that access to services is often based solely on computational results, rather than personal need or implicit merit. While the secrecy archetype, which focuses on protecting privacy by establishing and guaranteeing confidentiality between contracting parties, is somewhat effective in mitigating the disclosure and transmission of citizens' personal information in cyberspace, it is ineffective in shielding citizens from computer algorithms that crawl through databases and that have significant consequences on citizens' daily lives and, as such, cannot be considered adequate for the digital era. The analogue privacy archetypes that have been used to craft law responsible for protecting privacy are inadequate to protect privacy in digital systems. Were these archetypes adopted citizens would be less likely to communicate with one another, which would undermine their discursively generated solidarity and consequently threaten the viability of Habermas' discursively grounded political project.

In light of past privacy models' limited effectiveness in digitized societies, in chapter three I propose my own privacy archetype to address the challenges arising in digitized environments. My archetype, the reciprocal archetype of information responsibility,

focuses on the partnerships that individuals form with data collectors and insists on maintaining accountability and transparency in these relationships. This archetype requires the original content holders/providers to opt-in to data transmissions between third parties before these parties can collect, trade, or analyze people's personal information. As a side effect, this archetype would decelerate the rapidity that information, the capital of digital environments, flows at and produce at least two effects. First, by promoting citizen awareness of how their digital dossiers are developed, transferred, and used, citizens could collaboratively work towards asserting common privacy norms and codify these norms using positive, democratically legitimized, laws. Second, with cohesive and competent data and communication privacy laws citizens could communicate without fearing surveillance, which would let them discuss and legitimize any possible transitions to alternative governance systems without having the legitimization process tainted by stunted discourse that accompanies fears of non-democratically legitimized surveillance. Rather than focus on the possible composition of any such an alternate governance system, however, I focus on why national communicative privacy establishes the necessary precondition for any shift to a wider-reaching political system.

In the course of my thesis I assert the need to establish a new privacy archetype that can shield citizens' digital communications and consequently entrench the rights of privacy and free speech that have historically beat at the heart of Western democracies. To make this argument, I initially provide an account of how citizens develop bonds of association in pluralistic democratic nations, and I then reflect on privacy's central

facets, several prevalent privacy archetypes, and difficulties that these archetypes encounter when thrust onto digital environments. In light of their difficulties, I propose that the reciprocal archetype of informational privacy can overcome the challenges accompanying the rapidity and ease with which digital records are accumulated and exchanged by requiring parties associated with digital records to receive citizens' consent before transferring data to third-parties. Were my model adopted, citizens could craft positive laws that codified their shared values and norms towards communicative privacy without fear that their discourse was being surveyed for unknown (and potentially harmful or discriminatory) purposes. Ultimately, the reciprocal archetype of informational privacy ensures that the transparent and free discourse that has been essential to maintaining Western nation-states and citizen-solidarity will continue to be realized in the contemporary digital millennium.

CHAPTER ONE - HABERMAS, DISCOURSE, AND SOLIDARITY

Contemporary western communities are being reshaped as mass emigration, immigration, and cultural transmissions provoke replacements, transmutations, and re-entrenchments of traditional community values. Jürgen Habermas constructs his political theory against the backdrop of increasing social diversity and strives to retain the insights of modernity while remaining sensitive to contemporary communities' growing diversity. Habermas' political theory finds essential points of reference in the Treaty of Westphalia, Immanuel Kant's philosophy of right, and Hegel's discursive turn – Habermas' political theory preserves and carries on these core elements of modernity to produce a theory based in critical reflexivity. Critical reflexivity, or the process of analyzing validity claims against normative criteria, is tied to freedom of speech and action insofar as these liberties entail the capacity to evaluate the past, present, and future. With this in mind, the theoretical development of the nation-state, which internalizes these freedoms, and the role of discourse in establishing and maintaining the civic bonds that tie citizens in pluralistic nation-states together – bonds that are rooted in constitutionally asserted norms and values – becomes a focus. While the nation-state's ability to assist citizens substantively realize their rights is a concern, we ought to re-entrench its ability to substantiate these rights rather than abandoning it for an alternate system of governance that might perhaps restore these liberties.

1 Habermas' Antecedents

The Treaty of Westphalia, Kantian theory of right and notions of maturity, and Hegelian insights concerning discourse in particular communities provide the roots to

Habermas' analysis of discourse in Western states. The Treaty of Westphalia emerged at the conclusion of the Thirty Years War in 1648, and established and recognized states as autonomous and secular bodies.[4] Following the Treaty, all existing political states in Europe were political equals and were legally confined to particular localities. Perhaps most importantly, it marked the point when major European powers publicly and legally distinguished the public and private domains by recognizing the separation of church and state. The Treaty of Westphalia asserted that individual citizens held the legal right to private worship and religious expression; private religious pursuits had finally escaped the state's decree.

Centuries later, in the late 18th century, Immanuel Kant wrote a series of essays that developed the principles of autonomy, freedom, and equality that were nascent in the Treaty of Westphalia. His essays, "On the Common Saying: 'This May be True in Theory, but it does not Apply in Practice'" and "Perpetual Peace – A Philosophical Sketch," present his insights through the theory of right. For Kant, nations were constituted according to a particular set of values and norms, and after constituting the nation citizens had responsibilities and duties born of its constitutional values. Kant's understanding of citizens' shared rights follow from his understanding of freedom – individuals are free because of their rational faculty and express their freedom whilst performing rationally universalizable actions. The scope of free (and therefore rational) actions follows from the public rights that are codified in civil constitutions, rights that ought to be universalizable and are responsible for asserting the legitimate ranges of

[4] Roberta Guerrina (2002) *Europe: History, Ideas, Ideologies*, 30.

citizens' political freedoms. In constituting the nation according to reason, citizens recognize and universally assert that they are mutually bound by three *a priori* principles:

1. The *freedom* of every member of society as a *human being*.
2. The *equality* of each with all the others as a *subject*.
3. The *independence* of each member of a commonwealth as a *citizen*.[5]

The principle of freedom asserts that all citizens' liberties extend as far as they accord with reason and harmonize with the freedom of all other citizens. The principle of equality maintains that all members of society are equally subject to the state's laws – no individual, save the sovereign, is above coercion. The principle of independence recognizes that each person who is involved in constituting the nation is a co-legislator, and that individuals cannot legislate by themselves on behalf of the entire commonwealth – legislation is a group effort, where decisions ought to be rationally acceptable, even if they come at the expense of personal happiness.[6] These principles are best realized (for Kant) in a patriotic republican government, where citizens recognize themselves as "authorised to protect the rights of the commonwealth by laws of the general will, but not to submit it to his personal use at his own absolute pleasure."[7] This government develops solidarity through the shared and reasonable

[5] Immanuel Kant (2002) "On the Common Saying: 'This May be True in Theory, but it does not Apply in Practice'", *Political Writings*, 74. Hereafter referred to as "OCS", *PW*.
[6] Immanuel Kant (2002) "OCS", *PW*, 77.
[7] Immanuel Kant (2002) "OCS", *PW*, 74.

practice of lawmaking, a practice that endorsed public debate and critique of lawmaking, rather than through state-sanctioned pursuits of mass-euphoria.

Kant's attitude towards lawmaking is poignantly expressed in his transcendental formula of public right, which proscribes that "[a]ll actions affecting the rights of other human beings are wrong if their maxim is not compatible with their being made public."[8] As rational actors, citizens evaluate laws' rightness or wrongness by independently evaluating whether they accord with reason – citizens must be able to accept laws on the basis of reason alone – but to judge law they must know of it. On the basis of this formula, it follows that communication cannot be limited so as to prevent law from being made public. To accept law as a rational imposition, one that citizens can recognize themselves as the rational authors and addressees of, the law's proscriptions must be compatible with being made public.

In addition to these elements of Kantian thought, Habermas preserves Kant's notion of maturity. Individuals are mature insofar as they employ their "cognitive powers so as to take charge of [their] actions and judgements instead of referring the responsibility to an external authority of tradition (such as God, myth, religion)."[9] In other words, individuals who critically reflect on their relation to present, past and future actions and perceive themselves as responsible for those actions, take hold of their destinies. In realizing their responsibilities, individuals must be free to evaluate their situations and to act on their reflections. The difficulty facing Kant's theory is its monological character;

---

[8] Immanuel Kant (2002) 'Perpetual Peace a Philosophical Sketch', *Political Writings*, 126.
[9] Omid Payrow Shabani (2003) *Democracy, Power, and Legitimacy: The Critical Theory of Jürgen Habermas*, 17. Hereafter referred to as *DPL*.

while enlightened rationality confronts religion's dogmatic and uncritical positivity, reason becomes its own positivity by turning to the noumenal realm as a reference for what reason cannot deduct.[10] Partly because of this problem, Hegel reflects on freedom's unfolding from within subjectivity to realize humanity's immanent freedom.

Hegel's analysis of freedom in *The Philosophy of Right* identifies three core moments in freedom's unfolding. First, individuals come to understand that the will gives rise to its subjective disposition and realizes its freedom by possessing its being in itself. Freedom, at the first stage of subjectivity's unfolding, is realized in asserting the individual's autonomy from and authority over other things in the world. Emerging from this freedom individuals recognize that they are in the process of separating from and dominating other things (which they had been negating by their will) and recognize freedom through particularity. This leads individuals to recognize themselves as existing in collectives that share common values and life-projects and is where they come to realize freedom by asserting their autonomy and liberty in the set of social norms and regulations responsible for guiding social interactions. Their awareness of these norms and regulations arises not on the basis of their monological self-reflection (as in the case of Kant), but through the process of discourse. Their situatedness in society leads them to recognize the role of discourse in developing an awareness of their environment. At this stage, individuals realize that their fulfillment and expression of freedom involves both the particular exertions of the individual and the unifying character of the community, leading them to finally realize their freedom through the unity and harmony

[10] Omid Payrow Shabani (2003) *DPL*, 18.

of the state's actions. At this final stage, they realize that the state's actions establish the common structure that affirms and expresses the homogenous cultural values that each citizen has internalized while participating in the state's particular actions. Ultimately, the sphere of the ethical – that of the public – is subjugated to the primacy of the "*higher-level subjectivity of the state* over the subjective freedom of the individual."[11] The state's primacy causes reason to assume "a form so overwhelming that it not only solves the initial problem of self-reassurance of modernity, but it solves it *too well*."[12] Reason becomes a totalizing force and loses the emancipatory character that it held at the beginning of modernity by concluding history. Hegel's unfolding, while recognizing the role of discourse, concludes with the assertion that "[w]hat is rational is actual, and what is actual is rational."[13] The state, as the ultimate source of realized freedom, is thus right in restricting discourse should it choose to, negating Kant's insights regarding the importance of critically evaluating law through relatively unbounded public discourse.

When developing his analysis of discourse in political systems, Habermas draws on both Kant's insights concerning citizens' need to be able to publicly and critically analyze law and Hegel's recognition of the role of discourse in establishing norms and recognizing freedoms. By drawing on facets of Kant's and Hegel's philosophical systems

---

[11] Jürgen Habermas (1990) "Lecture Two," *The Philosophical Discourse of Modernity: Twelve Lectures*, 40.
[12] Jürgen Habermas (1990) "Lecture Two," *The Philosophical Discourse of Modernity: Twelve Lectures*, 42.
[13] Georg Wilhelm Friedrich Hegel (1991) *The Philosophy of Right*, p20. Hegel took pains later in his life to point out that he was not suggesting "everything was as it ought to be or (more particularly) that the existing political order is always rational" (*Philosophy of Right (1991),* 389-90[n]22). Rather than referring to external, contingent, events, Hegel is referring to freedom itself. Its actualization in the world, while dynamic, necessarily follows a particular path – even in the face of Hegel's clarifications reason becomes a totalizing force and loses its emancipatory character.

Habermas generates a critical account of discourse's role in constituting the normative characteristics of Western nations following the Treaty of Westphalia, characteristics that find freedom of speech at their heart.

2 Discourse Ethics: Morality, Ethics, and the Political Turn

According to Habermas, discourse is the process of challenging, validating, and re-challenging positions, of communication about communication that reflects on what has preceded it. Discourse should not be mistaken as a verbal free-for-all; it is a reflective form of speech where participants work towards common consensus and is open-ended; past or new participants can (re)join the discussion at any point to remedy past confusions or misconceptions. Discourse is initiated by one person challenging the validity of another person's statement and operates using the following rules:

1 Every subject with the competence to speak and act can take part in the discourse.

2 a. Everyone can question any assertion whatsoever.

b. Everyone can introduce any assertion whatsoever into the discourse.

c. Everyone can express their attitudes, desires, and needs.

3 No speaker can be prevented, by internal or external coercion, from exercising their rights as laid down in (1) or (2) above.[14]

These rules are implicitly realized by language-using people, rather than being realized when learning the rules of a game such as canasta or chess.[15] An objective

[14] Jürgen Habermas (1990) *Moral Consciousness and Communicative Action*, 89.

awareness of the rules of discourse is not needed to know if the rules are being followed because engaging in any give-and-take discourse, where all parties are genuinely attempting to reach a consensus, requires upholding the rules. When working to achieve consensus, a wide range of claims can lead to contestation that must be resolved before reaching a consensus. While a universal consensus requires the recognition of individuals as equal to one another (as reflected in the common right to engage in the discourse itself), this equality cannot come at the expense of individuality – discursive participants must be allowed to retain their unique particularities. As Habermas puts it, the "equal respect for everyone else demanded by a moral universalism sensitive to difference thus takes the form of a *nonleveling* and *nonappropriating* inclusion of the other *in his otherness.*"[16] The inclusion of others' otherness and the repudiation of a common metaphysical grounding for establishing the common good, leads Habermas to replace appeals to a transcendent good to ground norms with an immanent set of norms that emerge from deliberation itself.

The deliberation process replaces the moral content of transcendent morality with a self-referential process of developing norms that remains neutral to the conclusions of deliberations themselves. The process of evaluating a norm's universality is captured by the *discourse principle* (D), which states that "[o]nly those norms can claim validity that could meet with the acceptance of all concerned in practical discourse.[17] While (D) establishes the grounds for potentially realizing moral norms, it indicates only which

---

[15] James Gordon Finlayson (2005) *Habermas: A Very Short Introduction*, 43. Hereafter referred to as *H:VSI*.
[16] Jürgen Habermas (2002) *IO*, 40.
[17] Jürgen Habermas (2002) *IO*, 41.

norms are *invalid.* At this stage, individuals can use only sincere speech acts to generate consensus and, while they cannot assert which moral norms exist, they can hypothetically propose what it would mean to justify a norm. The *principle of universalization* (U) is intended to test the validity of first-order moral norms (i.e. those identified using (D)) by checking whether they can be universalized. (U) states that: "A norm is valid when the foreseeable consequences and side effects of its general observance for the interests and value-orientations of *each individual* could be *jointly* accepted by *all* concerned without coercion", [18] effectively asserting that "the amenability to consensus in discourse is both a necessary and sufficient condition of the validity of a moral norm."[19] When there are contestations surrounding the logical relationship of validity and consensus, participants engage in argumentation that resembles a cooperative competition that is oriented towards reaching a consensus. In the process of argumentation what counts as a good or bad argument may itself become contested – norms are evaluated as they emerge in discourse rather than being born of and applied on the basis of pre-existing conceptions of the good. As such, these rules remain neutral to ethical content, and one can evaluate discourse based on the force of argumentative rationality.

Simone Chambers, a critical theorist, notes that in replacing Kant's monological test with (U), Habermas cannot expect to arrive at fully conclusive determinations of moral norms because (U) requires real people to participate in moral conversations. Since the particularities involved in argumentation are impossible to remove, moral

[18] Jürgen Habermas (2002) *IO*, 42.
[19] Gordon Finlayson (2005) *H:VSI*, 82.

argumentation "fails to transcend concrete communities."[20] (U)'s inability to escape the clutches of the particular has led other theorists, such as Albrecht Wellmer, to suggest that rather than using (U) to legitimize morality, (U) can more appropriately function as a way of testing democratic legitimacy in nation-states.[21] In essence, the criticism is that (U) can offer only conditional confirmations of validity.

In turning to conditional confirmations of validity, we pass from morality to the ethical-political sphere, that is, the sphere concerned with ethics and politics. In this sphere, discourse is concerned with evaluating possible conclusions that take "one's desired ends as given and, deliberates the best means to achieve them."[22] Albrecht Wellmer, in focusing on the legitimization of state actions, captures ethical discourses' focus on whether or not actions are good or bad for the individual, the community, or both. In ethical discourse, goodness or badness is motivated by happiness – what actions can be taken that accord with a conditional affirmation of (U) and lead to happiness without negatively affecting others. In focussing on the conditional affirmation of (U) we can recognize that gradients are involved in actual discourses – actions can be more or less good, whereas they are either just or they are not.[23] Thus, the choices made in democratically legitimized societies can be better or worse, though not necessarily right or wrong. Discourse guides these decisions and ideally "asks participants to exclude all strategic and instrumental attitudes toward interlocutors

---

[20] Simone Chambers (1995) "Discourse and democratic practices," *The Cambridge Companion to Habermas*, 234. Hereafter referred to as "DDP," *CCH*.

[21] Albrecht Wellmer, in "Ethics and Dialogue: Elements of Moral Judgement in Kant and Discourse Ethics", pp. 145-88 has levelled this charge.

[22] Gordon Finlayson, *H:VSI*, 92.

[23] To illustrate, whereas a particular religion may be better or worse for a person's happiness, genocide and cold-blooded murder are inherently unjust.

from the conversation"[24] – there should be no coercion that would limit or exclude participants from the discourse. This discursive attitude suggests that, despite the spectrum of value-structures guiding participants' lives and communication, (a) discursive participants can identify all of the actors that would be affected by a deliberative decision; and (b) all affected members can and are willing to participate. Whereas in an ideal situation (a) and (b) could be met, ethical discourse approximates the ideal and, as such, cannot be assured of wholly meeting either (a) or (b). The questions that then confronts us are 'How can we establish a normative guidepost that can order discourse so that it at least approximates the conditions of moral discourse?' and 'How can we guarantee that those affected by law can vocalize their attitudes towards it?' To address these questions we turn to theorized modes of political association (section three) and their constitutions that are responsible for ordering ethical-political discourse (section four).

3 Constituting the Nation-State

Europe's political structure following Westphalia set the stage for civic and ethnic modes of political association. However, these modes of political association were unable to sustain political stability in light of their dominant modes of political association, which stimulated the development of thought that led to the inception of the nation-state. In investigating the theoretical structure of states following Westphalia we initially (A) turn to the civic-state's development, which adopts civic models of association to ground citizens' relationships in commonly held principles and rights, and

[24] Simone Chambers (2005) "DDP," *CCH*, 239.

then to (B) the ethnic-state's development, which follows "the trail blazed by an anticipatory national consciousness disseminated by propaganda."[25] After outlining these modes of post-Westphalia political association I examine (C) the theoretical challenges facing both models and (D) how they appropriate each others' strengths to rebuff these challenges, causing civic- and ethnic-states to transition into nation-states.

(A) The civic-state

The modern conception of 'state' is a legal term that refers to a politically organized power that "possesses both internal and external sovereignty, at the spatial level of a clearly delimited terrain (the state territory) and at the social level over the totality of members (the body of citizens or the people)."[26] State power is constituted through positive law that is shaped by citizens, who act as bearers "of the legal order whose jurisdiction is restricted to the state territory."[27] The political and bureaucratic structures of civic-states reflect the wills and actions of the principal actors - lawyers, diplomats, and military officers belonging to the military's administrative staff – who established the state's administrative apparatus,[28] an apparatus that maintains itself through taxation. As an administrative body tied to economic markets it must be flexible to respond to market fluctuations, a flexibility that has historically been able to realign administrative rules and policies alongside market developments.

By separating administrative tasks and the market, civic-states separate the tasks of administration from the processes of production, both of which were historically

[25] Jürgen Habermas (1998) *IO*, 105.
[26] Jürgen Habermas (1998) *IO*, 107.
[27] Jürgen Habermas (1998) *IO*, 107.
[28] Jürgen Habermas (1998) *IO*, 105.

captured in the framework of political power.[29] This disjunction of political power recognizes the market as a self-regulating system that depends on market participants' decentralized decisions.[30] The division of legal and productive competencies symbolizes a transformation in positive law, where this division identifies and differentiates between public and private laws and recognizes that markets are guided by different logics than the state's. While markets are regulated by politics, they obey a logic that often aims towards escaping state control, insofar as markets strive to release and accelerate the rate of capital flows[31] and the state is charged with maintaining political stability, potentially at the cost of reduced market competitiveness. Markets are essential to the state's maintenance and vice versa; the civic-state's administrative system would collapse without taxing market participants and, without a defined system of stable governance that distances the state's metric from the market, the market would find it challenging to maximize profits. While the two systems operate along divergent logics they mutually profit by each other's healthy existence, just as they mutually suffer when one is weakened.

As an administrative state, the civic-state was effectively open to new members. New members were required to limit their actions in accordance with law and to participate in the state by relinquishing taxes but, beyond this, they were free to pursue their unique visions of the good-life. Following Westphalia, civic-states are best

[29] Jürgen Habermas (1998) *IO*, 108.
[30] Jürgen Habermas (2001) *The Postnational Constellation*, 63. Hereafter referred to as *PC*.
[31] Michael Hardt and Antonio Negri (2000) *Empire*, 31-2.

understood as theoretically inclusive, equal, and autonomous members of the international political sphere that saw all citizens as possessing common civic rights.

(B) The ethnic-state

Writers, historians, scholars, and other intellectuals worked in tandem with diplomatic and military unification processes to propagate the "more or less imaginary unity" of cultural nationalism.[32] Instead of developing an administrative state that minimizes the imposition of a particular ethical life on its members whilst remaining open to future members, the ethnic-state asserts a particular version of the good-life to ground a common pre-political unity that functions as the bedrock of political unity and stability.[33] The ethnic-state repudiates "everything regarded as foreign, [by] devaluing other nations, and [by] excluding national, ethnic, and religious minorities."[34] To elucidate, using the common good to establish solidarity means that being recognized as a German requires members to trace their personal constituting elements to the state's pre-political myth – Germanness is demonstrated in the historical relation to German particularities, such as language, blood, cultural ties, family history, and/or religious beliefs. Thus, being German in an ethnic-state involves not belonging to groups that dilute Germans' Germanness – citizens possess homogeneous, rather than heterogeneous, cultural compositions. Legitimate law in ethnic-nations manifests from the citizenry's implicitly understood will – Carl Schmitt notes that any inclusive or

[32] Jürgen Habermas (1998) *IO*, 105.
[33] Mark Poster (1999) "National Identities and Communicative Technologies", 237-8. Poster notes that it is only in examining the plethora of print articles that the unified discourse of an ethnic-nation is manifest and, based on Benedict Anderson's analysis of print, argues that analyzing individuals' norms and communicative principles cannot reveal a homogeneous state-wide ethnic-political discourse.
[34] Jürgen Habermas (1998) *IO*, 111.

deliberative process of lawmaking only "provides threshold requirements and limitations for parliament, though not for the people's will itself, about which one has known since ancient times that the people cannot discuss and deliberate."[35] In this political environment, public discourse is not absolutely necessary – the people naturally and implicitly legitimize law born of themselves – and the laws created by parliament are only legally binding. Under the metric of ethnic-nationalism, the people's will, not the state's legal affirmations, confers legitimacy on the legislatures' actions.

(C) Challenging both models

Within civic- and ethnic-nations, individuals develop solidarity with others who would have historically remained as strangers. The solidarity develops in civic-nations from shared involvement in lawmaking, whereas in ethnic-nations it is rooted in the people's homogenous cultural identity. As we will see, neither the civic- or ethnic-nation can independently overcome the subsequent problems of legitimization or social integration, which leads the two models of political association to draw from each others' strengths to ultimately create the nation-state.

The challenges facing these early post-Westphalia modes of political association are significantly related to the schism of Christendom during the Reformation, which gradually eroded the common metaphysical authority that had traditionally grounded common ethical attitudes and norms.[36] Unable to appeal to a common externally validated law, nations had to ground their laws without appealing to metaphysical foundations, which created a problem insofar as a new way of legitimizing law had to be

[35] Carl Schmitt (2004) *Legality and Legitimacy*, 64.
[36] Roberta Guerinna (2002) *Europe: History, Ideas, Ideologies*, 30-2.

found. The problem of social integration was connected to "urbanization and economic modernization, [and] with the increasing scope and acceleration of the circulation of people, goods, and news."[37] This acceleration isolated people because they were uprooted from previously fixed localities and projected into alien locations where they lacked common local bonds to bind them to their new community and its members. The pluralism that arose from mixing 'native' and 'foreign' peoples, cultures, and news upset traditional modes of social integration, where members' sharing traditional cultural value had drawn them together.

Civic-nations struggled to alleviate these problems by turning to democratic participation to establish a legally mediated solidarity – common participation in lawmaking let citizens see themselves as equal partners in the civic-nation. They could participate in politics on the basis of their shared rights but these 'thin' bonds of shared rights and lawmaking lacked the strength to generate more abstract notions of solidarity. While the constitution created a minimum set of attachments that ensured the nation did not immediately collapse with the withdrawal of religion as law's foundation, the constitution could not entirely overcome the problem of integration – universal rights alone were insufficient to establish a common, cohesive, national identity. While these rights ensured that all members could engage in discourse, this model of political association only saw discourse as an expression of right rather than as a path towards developing the abstract conception of deliberatively-grounded solidarity.

[37] Jürgen Habermas (1998) *IO*, 111.

Ethnic-nations confronted the problems of legitimization and integration by grounding law and shared meaning in the common cultural stratum responsible for defining the nation. Members of ethnic-nations generated solidarity out of their common language, history, and religion and, while these 'thick' bonds drew members together, they prevented the nation from establishing an inclusive and permeable system that was sensitive to its increasingly pluralistic composition. Having separated 'legality' and 'legitimacy', the ethnic-state asserted the primacy of its national myths and values over the plurality of values and concerns accompanying the influx of foreign aliens. While the ethnic-nation successfully resolved the problem of legitimization by appealing to the will of its citizenry, it effectively failed to integrate others into the society and accord them the respect and dignity provided to full members of the nation. Regardless of what foreign aliens said, their utterances could at best become legally asserted law – legitimization escaped their discursive practice on the basis of their otherness.

(D) The rise of the nation-state

The civic- and ethnic-nation models' inability to independently overcome the problems of legitimization and integration led them to draw from each others' strengths. The civic-nation, recognizing that it enclosed a particular geographic space and held sovereignty over particular people, drew on the ethnic-state's notion that members of the civil society existed in a common cultural substratum to initially tie individuals together in order to overcome the problem of integration. This cultural substratum was largely constituted through public discourse, but left discourse open to

new civic members – it was not a closed system. In recognizing the role of its cultural substratum, the civic-nation could use its history to act as a ground of law, but could reject the position that participation in creating the original shared history was a necessary precondition for later political participation. Thus, the nation-state could rely on previously developed cultural practices to assist in realizing solidarity without having those practices necessarily exclude new members.

The ethnic-nation gradually changed from a political body that asserted the overarching importance of thick bonds to legitimize politics to one that recognized the need to equate legitimacy and legality and to attend to the shared practice of lawmaking. If the ethnic-nation denied the legitimacy of laws made by those not sharing in societal 'thick' bonds then it would become increasingly challenging to maintain political stability because 'foreign' members of society would not recognize themselves as authors and addressees of law; their non-involvement in legitimizing law would prevent them from perceiving themselves as equal members in the practice of lawmaking and would contribute to social fragmentation.

It is essential that we understand that the nation-state recognizes all members as equal to one another and remains open to changes in law based on the discursive efforts of its constituents. These efforts are protected by positive law born of the nation's constitution. Whereas the civic-state saw discourse as a common right, but failed to see its core integrative function, and the ethnic-state discounted the role of discourse in legitimizing actions, for the nation-state discourse functions as the basis upon which citizen-solidarity develops.

4 The Role of Discourse in Developing Citizen-Solidarity

Constitutions come to be alongside the nation's legally asserted birth and they embody the values that the nation's creators fuse to the nation. In civic-nations, this means that the values of inclusivity, sovereign power over a delimited territorial space, citizen-equality and independence, as well as decisions regarding the distribution of governmental power are encapsulated in transformative constitutions – these constitutions act injunctively, standing between the time the state was not and the time when it asserts its formal values through codified and formalized basic law. Codifying constitutions, which assert a nation's formalized basic law, develop after transformative constitutions and are responsible for establishing the core laws responsible for guiding the form of the nation's laws and political arrangement, as well as acting as the final ground of appeal for legal challenges. These constitutions entrench particular values against the winds of change and, as such, provide a degree of long-term political stability that transformative constitutions cannot.[38] Basic law establishes members' core rights and privileges and, in recognizing members as bearers of rights that can formally participate in the political process, legally identifies members as citizens. In receiving citizenship, members accept the rights and duties prescribed in the codifying constitution and, at least probationally, agree to the governance structure it sets down.

As a living document, the constitution can change alongside the citizens who are responsible to and for it. Constitutional norms are changeable insofar as "even the basic norms that the constitution itself has declared non-amendable share, along with all

[38] Lawrence Lessig (2006) *Code Version 2.0,* 314. Hereafter referred to as *CV2*.

positive law, the fate that they can be abrogated, say, after the change of a regime"[39] or by making constitutional amendments. As a reflexive document, the constitution remains perpetually open to new interpretations and adjustments, which enables it to remedy any constitutionally asserted norms that would justify excluding possible members of the nation-state. These changes take place by having disenfranchised members informally raise awareness of the injustice which, over time, injects their discourse into the dominant political discourse. This gradual process has been demonstrated throughout history when minorities and excluded groups have gained the right to vote after injecting their informal discourse into that of the public. For such an injection to occur rapidly, all members of the nation-state must be able to communicate without fear that alerting others to perceived social injustices might provoke state-sanctioned coercive responses.[40]

The same open discourse that is based on constitutional norms that disenfranchised individuals can draw on to rectify injustices is also used to develop citizens' shared civic-bonds. The constitution grounds the ethical-political argumentation that occurs in the nation-state – as its basic law, the constitution is the final source of appeal for legitimated political argumentation. Citizens recognize the constitution as their common legal ground and repertoire of ethical-political norms when referring to its norms in the

[39] Jürgen Habermas (2001) *PC*, 117.

[40] Without the possibility of constitutional amendments to address normative discrimination the state may turn to explicit coercion on benign neglect to maintain political stability in the face of growing pluralism and cultural heterogeneity. Will Kymlicka, in *Multicultural Citizenship*, identifies benign neglect as the failure of pluralistic nation-states to recognize the value of, and subsequently protect, minority cultures. Benign neglect is exercised on the basis that once individuals' rights are protected their communities would similarly be protected. Unfortunately, such attitudes fail to account for the importance for protecting groups to preserve the repertoires of cultural value that give meaning to members' lives and are responsible for instilling particular cultural values in them.

justification of their arguments. These justifications often take the form of appealing to common constitutionally internalized principles of equality, fairness, and independence. Whereas the ideal rules of discourse are (theoretically) understood by all participants in discourse, the constitution provides a (relatively) transparent set of rules that citizens can use in appeal when they feel they are being discriminated against – this corpus transparently asserts the rights, such as freedoms of speech and privacy, which are implicitly recognized in the ideal rules of discourse.

While relatively weak bonds are initially formed between citizens when they work together to establish the constitution, these bonds expand and become increasingly substantive as citizens continue to engage in discourse with one another and share and confront subsequent challenges. When citizens strive to resolve commonly experienced issues and have their discursively developed resolutions framed by the constitution, they develop a substratum of meaning based on civic concerns, values, and responses.

While engaging in discourse citizens develop 'communicative power', which "is identified with the realization of a rational public opinion formation and will formation in the process of lawmaking that comprises a complex network of processes of reaching understanding *and* bargaining."[41] To exercise communicative power and for citizens to identify with one another on the basis of their shared use of communicative power to informally advance their concerns to governments, a series of (relatively) demanding preconditions must be met that develop from constitutional norms. Habermas notes that to enjoy communicative power:

---

[41] Kenneth Baynes (1995) "Democracy and the *Rechtsstaat*: Habermas' *Faktizität und Geltung*," *The Cambridge Companion to Habermas*, 213.

- individuals must be willing to assume the views held by other discursive partners;[42]
- the public sphere (where individuals formally communicate with one another) cannot be distorted by undue coercion;[43]
- a liberal environment emphasizing individual freedom must be maintained;[44]
- the elements of private society that would be affected by imposing a particular law must be recognized and permitted to enter the communicative discourse.[45]

Moreover, political parties must actively bridge the divide between the informal and public domains – they cannot become so engrained in the state's administrative elements that they cannot interact with the citizenry.[46] Thus, communicative power is initially realized in the informal domain where understanding is reached, and then transmitted to the citizens' legislative representatives. These representatives resolve citizens' issues, but the representatives participate in bargaining sessions to reach these solutions rather than developing a shared consensus amongst themselves (as citizens do when reaching their understandings in the informal domain) because of the limited time to enact legislation and the finite resources available to the nation-state. This entire communicative process is predicated on the assumption that citizens are free to communicate with each other and their political representatives – if this is not the case,

[42] Jürgen Habermas (1998) *IO*, 42.
[43] Jürgen Habermas (1998) *IO*, 44. While Habermas uses the term 'coercion' expansively, it should be noted that non-democratically legitimated surveillance that impacted an individual's behaviour would classify as undue 'coercion'.
[44] Jürgen Habermas (1998) *IO*, 44.
[45] Jürgen Habermas (1998) *IO*, 44.
[46] Jürgen Habermas (1998) *IO*, 160.

then citizens' ability to develop and reform law is denigrated, if not lost entirely. Importantly, as Western nation-states shift toward new digital communication systems, new challenges arise alongside the imposition of these systems. These challenges must be identified and overcome so that citizens can communicate without fearing surveillance or coercion when using these new networks; email must be as private as handwritten letters if digital networks and their associated communication systems are to stand in and replace traditional modes of communication.

Having evaluated the weight placed on discourse, we now attend to the centre of gravity this discourse revolves around – the constitution and the emergence of citizens' patriotism towards it. Citizens, by referring to the constitution, identify themselves as its authors and guardians,[47] and their self-recognition in the constitution has two effects; it immanently justifies the norms and conditions affirmed in the constitution as the citizenry's own (that is, they recognize that the constitution does not assert values that require citizens to be members of particular cultural bodies to identify with it) and it asserts that its values are shared amongst the nation-state's members. These elements of self-recognition and other-recognition based on constitutional rights generate what Habermas terms 'constitutional patriotism'. His term identifies the solidarity that emerges when citizens recognize each other as sharing in the practices of lawmaking that are fundamentally grounded in, and guided by, their common constitutional rights.

[47] It should be noted that when citizens refer to the constitution they does not necessarily have to be in full support of the entirety of its articles for them to perceive themselves as its authors and guardians; authorship and guardianship can involve calls for remedying errors in a draft, or guarding particular constitutional principles from the over-extension of other principles. In this sense, a constitutional *culture*, rather than a constitutional *identity* emerges as citizens immerse themselves in the constitutional state. For more, turn to Jan-Werner Müller's *Constitutional Patriotism*, 53 – 67.

This patriotism extends beyond the weak legalistic association of individuals that crippled early civic-states because, in the process of creating law, discursive deliberation takes place between parties and leads them to see each other as co-legislators and to appreciate each others' life-projects, values, and dreams. The identity that emerges from constitutional patriotism realizes a common expansive inclusivity that extends equal rights to anyone who accepts the rights and duties of membership. Instead of relying on ethnic bonds to hold groups together, the civic nation-state relies on the constitution to act as "a legal device for institutionalizing deliberative procedures through which citizens come to recognize each other as such."[48]

Constitutional rights enable citizens to participate in the political element of society without having to first abandon their particularities. Particularities, such as cultures, "are valuable, not in and of themselves, but because it is only through having access to a societal culture that people have access to a range of meaningful options"[49] – culture is essential for establishing the values that guide individuals throughout their lives. It is in this medium of everyday communicative processes where individuals immerse themselves and develop their culture that Habermas terms 'the lifeworld'. The lifeworld "is the context of meaningfulness against whose background human actions find their objective, subjective, and normative references."[50] It is where traditions and cultural meanings are passed down, where people participate in social integration through which norms of cooperation and interaction are learned, and is where people develop

[48] Omid Payrow Shabani (2006) "Constitutional patriotism as a model of Postnational political association: The case of the EU," *Philosophy and Social Criticism, Vol 32, no 6,* 702.
[49] Will Kymlicka (1995) *Multicultural Citizenship*, 83.
[50] Omid Payrow Shabani (2003) *DPL*, 87.

identities as members of groups and as unique individuals in the course of socialization. The processes of the lifeworld involve communication and discourse – humans develop in the lifeworld while discussing their situation with others and without using intense bargaining sessions – and require communicative privacy if individuals are to develop their mature identities without experiencing formative retardations of their identity that could arise should individuals perceive the need to self-censor their discourse in light of possible coercion arising from their discourse. Given the growing transition to digital communicative systems in Western nation-states it is imperative that attention be paid to digitized discourse, given that the process of digitization facilitates the covert aggregation, storage, and analysis of digital communication – digital technologies extend the possibilities of surveillance and, as a result, extend the possibilities that individuals will feel the need to self-censor their discourse.

A material substratum supports the lifeworld's existence. This substratum is maintained by systems that are guided according to purposive action and are oriented towards achieving objective goals using strategy and bargaining. The systemic domain provides the materials that are needed to (re)generate elements of culture, independent development, and maintenance – systems are responsible for reproducing great pieces of literature, for providing incense used by millions in their religious practices, producing artefacts that certify and remind individuals of their personal achievements, and for transmitting discourse across vast stretches of space using digital technologies. As such, the systemic domain is not inherently problematic; so long as the lifeworld's communicative infrastructure is not undermined by the systemic domain's

strategic interests (e.g. so long as market logics do not overwhelm individuals' right to communicative privacy across digital networks), systems can remain a positive complement to the lifeworld.

Problems arise when systemic imperatives overcome the imperatives of the lifeworld. When the lifeworld experiences systemic invasion it faces the possibility of colonization. A clear example of such colonization was evidenced during attempts to amend the Canadian constitution. During the 1989 round of constitutional negotiations at Meech Lake, elites dominated the amendment process and engaged in a sustained process of bargaining, trade-offs, and pressure tactics.[51] Intensive negotiation was used, where participants tried to develop binding contractual agreements rather than participating in sustained argumentation and discourse aimed towards contemplating, analyzing and articulating the normative aims of the amendments. The latter process is extensive, time consuming, and demanding of all involved. While cutting a deal might have temporarily alleviated issues facing Canadians at the time, it would have entrenched basic laws that lacked a "deeper and popular moral agreement on principles" and would have subsequently caused Canadians to "lack the commitment and allegiance necessary to sustain a constitution over time."[52] In this instance a systemic invasion failed in its colonizing efforts, but its motivation to assuage empirically realized issues demonstrates the nation-state's inability to substantively guarantee its citizens their full range of constitutionally guaranteed rights. While in the case of Meech Lake, the nation-state repudiated the systemic domain's colonization, this is not always

[51] Simone Chambers (1995) "DDP," *CCH*, 251.
[52] Simone Chambers (1995) "DDP," *CCH*, 253.

the case, as seen when market logics dictate government policy responses rather than policy being directed by normative criteria. Despite the nation-state's failure to wholly guarantee citizens their full range of rights, so long as citizens can freely communicate with one another and generate non-coerced communicative power capable of motivating elected officials to end the 'race to the bottom' style of politics that has accompanied market liberalization, it is possible to avert a total colonization and chronic infection of the lifeworld can be averted. Currently, governments,

> terrified of the implicit threat of capital flight, have let themselves be dragged into a cost-cutting deregulatory frenzy, generating obscene profits and drastic income disparities, rising unemployment, and the social marginalization of a growing population of the poor.[53]

Nations, in the process of repealing social services, have advocated a turn to neo-liberal politics that focus on equal market participation and that operate on the assumption that all market agents can equally participate in said market. This position was abandoned following the catastrophes of the Second World War, and welfare-states developed, because liberal markets developed class conflict that threatened to finally undue political stability.[54] Without a reversal of liberalizing trends it is increasingly likely that the citizenries will fragment; individuals, lacking the nation-state's protective aegis, will refuse to share the burdens and duties that accompany citizenship because, quite simply, citizenship has to pay "in the currency of social,

[53] Jürgen Habermas (2001) *PC*, 79.
[54] Jürgen Habermas (2001) *IO*, 173.

ecological, and cultural rights."[55] There are extensive responsibilities that follow from citizenship, and if individuals are not 'compensated,' they will cease seeing themselves as the authors and addressees of laws that deviate from the normative prescriptions established in the constitution. A core (or *the* core) element of assuring citizens that they can continue to participate in political life is assuring them the right to communicative privacy in digital environments. If essential constitutional norms that guarantee freedom of speech are abandoned, if citizens are left to defend themselves against issues of social justice, and if citizens cannot communicate using contemporary communications networks without fearing illegitimate coercion, the integrative function of constitutionally shielded discourse will vanish.

This account of the lifeworld's colonization should not be taken to mean that the nation-state is doomed to collapse. Citizens, so long as they can organize, communicate, and collectively exert pressure on their elected representatives, can reassert themselves and their political power as the dominant social forces. While money presently supplants the regulatory power of politics, this inversion need not be permanent. Instead, it can be read as a continuing challenge in balancing the interests of the lifeworld and systems. Indeed, with the transition to information economies, avenues are opening for citizens to reassert themselves as the principal actors motivating state actions.[56] By encouraging their legislative representatives to carefully safeguard individuals' personal information and discourse that spans digital networks across the world, citizens' constitutional rights can be substantively re-entrenched – citizens would

[55] Jürgen Habermas (2001) *PC,* 77.
[56] Michael Hardt and Antonio Negri (2000) *Empire, 298-300.*

effectively receive 'payment' in the form of digital communicative privacy for adhering to their constitutional obligations. The causes of social justice are far from being lost but, because the nation-state as it has been theoretically realized in the course of this thesis depends on deliberative *discourse,* it is critical that citizens be able to participate in open and free communication that is not perverted by the possibility of illegitimate systems of surveillance to maintain their discursive solidarity and political stability.

CHAPTER TWO - DISCOURSE, PRIVACY, AND DIGITAL NETWORKS

American Supreme Court Judge Louis D. Brandeis, a devoted privacy advocate, is well-known for his role in establishing contemporary rights to privacy. In a dissenting opinion in 1928, he drew on a law review that he and Samuel Warren had published in 1890, and asserted that the American constitution held a latent right to privacy. His early assertion of public privacy rights aligned with American Judge Thomas Cooley's legal treatise on torts in 1880 where Cooley asserted that individuals held a right to be left alone.[57] The challenges and importance of asserting privacy rights have been amplified significantly since Cooley's and Brandeis' contributions, often as the result of innovations in communication technologies. In light of these challenges, a series of privacy archetypes have been developed to assist lawmakers in creating laws that can competently identify and respond to privacy invasions. These archetypes provide normative criteria to shield distinctive elements of individuals' private lives from unwanted publicity. Unfortunately, these archetypes often fail to strictly separate privacy from the associated spheres of liberty, autonomy, and secrecy, which weaken their ability to mitigate analogue privacy invasions and are responsible for limiting their effectiveness in preventing contemporary privacy invasions that arise as citizens increasingly communicate along digital systems. Ultimately, I will argue that even the most 'successful' analogue privacy archetype, the secrecy archetype, cannot effectively protect individuals' digital communicative privacy. If the secrecy archetype is adopted to guide lawmaking for digital environments, as we will see, individuals' digital

[57] Judith Wagner Decew (1997) *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology,* 14. Hereafter referred to as *IPP*.

communications cannot be adequately secured from illegitimate surveillance and discrimination. Without adequately securing citizens' communications from non-legitimized surveillance, citizens may experience deteriorations of their discursively generated solidarity and the contemporary nation-state may fragment or dissolve as a consequence.

1 What is Privacy?

Privacy is often understood as a state free from external obtrusions or disturbances to one's private affairs. Such a broad understanding of privacy conjoins a series of interrelated, though distinctive, privacy classifications: freedom to control one's personal information (informational privacy); freedom to physically isolate oneself (accessibility privacy); and the freedom to speak and associate with others without being surveyed (expressive privacy). Broadly classifying privacy as freedom from obstruction fails to transparently distinguish privacy from the closely related concepts of autonomy, secrecy, and liberty. In this section, I briefly outline the three interrelated privacy classifications and distinguish privacy from autonomy, secrecy, and liberty. After providing a granular account of what privacy is and is not, I proceed to discuss privacy's value to individuals in their public and private lives.

At its most basic level, informational privacy describes the right to know who knows what about you and to control the flow of your personal data to other parties.[58] Personal data encompasses information that is on and off the public record, and includes information about daily activities, personal lifestyle choices, medical history,

[58] Information and Privacy Commissioner/Ontario (2001) "An Internet Privacy Primer: Assume Nothing," 1.

finances, academic achievements, religious or philosophical beliefs, distinctive physical descriptions, employment history, personal relationships, sexual orientation, life goals, and preferred customer habits, to name a few. Under this privacy classification, individuals experience privacy invasions "by publication or even broader publication of such information; by intrusive snooping, observation, or wiretapping; by testing to gain or attempt to gain the information."[59] This last point is especially important; it is not that someone has successfully collected information without first gaining an individual's consent – the mere attempt to access this information constitutes invasion. Informational privacy often overlaps accessibility privacy, which is infringed upon when another person enters an individual's physical proximity in violation of the individual's reasonable attempts to seclude themselves from the eyes of others. Judith Wagner DeCew, a noted privacy and legal theorist, notes that even "surveillance of normal, everyday activities can lead one to be distracted and to feel inhibited. Such behaviour can intrude on one's solitude or seclusion even if it is not yet noticed or discovered, because of the fear its potential recognition can generate."[60] According to Wagner Decew's account, an individual's accessibility privacy is breached when a person surreptitiously watches a woman shower or undress, for example. This stealthy behaviour intrudes on the woman's reasonable right to privacy and, if the behaviour is left unchecked, can generate fear of discovery in the woman and sense of personal violation. Like accessibility privacy, expressive privacy relates to the individual's ability to control who surveys and records their personal expressions. Expressive privacy protects

[59] Judith Wagner Decew (1997) *IPP*, 75.
[60] Judith Wagner Decew (1997) *IPP*, 76.

individuals from the fears or pressures to conform to homogenized viewpoints or attitudes that can follow from suspecting that one's privately uttered speech might be being monitored or could be made public. This kind of privacy is, as an example, intended to protect people so that they can express their sexuality, regardless of whether it accords with dominant social norms. Because expressive privacy tends to involve the collection of information as well as some proximity to collect or verify the collected information, this last privacy classification is often intimately linked with the two previously mentioned classifications.[61]

In addition to commonly compressing the three aforementioned privacy's classifications to a lone and somewhat nebulous privacy classification, privacy is also often unintentionally compressed with the theoretical concepts of autonomy, secrecy, and liberty. While privacy is intimately involved with each of these concepts, it acts as an umbrella that is deployed to shelter individuals' autonomy, secrecy, and liberty, rather than being intimately and unavoidably bonded to any one of them. While autonomy and privacy interests often align when either autonomy or privacy is violated, this is not always the case because people are autonomous insofar as they can make independent and self-legislating choices. When a person decides to blare their car stereo in a busy neighbourhood, their autonomous action cannot be considered private. In contrast, when they make decisions concerning their basic lifestyle, they can reasonably expect to have their autonomous choices kept from the public eye. Moreover, not all privacy invasions directly threaten a person's autonomy – electronic

[61] Judith Wagner Decew (1997) *IPP*, 78.

surveillance, for example, doesn't necessarily violate a person's ability to make self-legislating choices so long as they never experience consequences resulting from the surveillance or realize that they are being electronically surveyed. Because of these complications, we cannot legitimately claim that autonomy and privacy concerns are necessarily conjoined.

Similarly, privacy and secrecy often align with one another, though they do not always do so – some events are secret but not private, and vice versa. To expand, a secret treaty or military plan may be kept secret from the public, but the fact that it is kept secret does not mean that it deserves the privacy protections that cloak people's sexual activities in their homes. It is important to note that "[c]haracterizing privacy as what is *intended* to be concealed is no help"[62] because, while military secrets are intended to remain secret, it does not follow that their intention to be kept secret necessarily means that they are private. In light of the difference between privacy and secrecy, we can say that secrecy aligns with privacy protections when private individuals engage in actions that they can reasonably expect to be concealed from the public eye. This said, there is (again) no necessary equation between privacy and physical secrecy. While physical seclusion is often used to evaluate whether a person's accessibility or expressive privacy has been invaded, it does not stand that secret actions in secluded spaces are necessarily private – politicians who meet in secret to negotiate legislation cannot justifiably expect privacy laws to protect their very public discussions.

[62] Judith Wagner Decew (1997) *IPP*, 48.

Finally, we must make a distinction between privacy and liberty. Privacy is intended to prevent unnecessary interference in our personal lives and, to a limited extent, does promote liberty of action. Personal liberty encompasses the range of actions that a person can perform, whereas privacy shields people from intrusions that would limit individuals' possible ranges of publicly sanctioned actions. In light of this disjunction between liberty and privacy, we can envision cases where a person's privacy could be invaded without infringing on their liberty and vice versa. If, for example, I am unknowingly placed under surveillance, my liberty is not necessarily impeded – I am still free to enjoy my customary ranges of action even though all my actions might be recorded. Alternately, I could be physically assaulted on the street and have my liberty limited without experiencing a privacy invasion. While privacy and liberty often align with one another, the division between privacy breaches and injustices towards personal liberty reveal that the degradation of one's liberty does not necessarily indicate that a privacy breach has occurred.

2 Privacy's Value to Personal Development and Discourse

Liberty, the absence of external restraints or coercion, plays a central role in forming the political bonds between citizens. In the absence of coercion, citizens are free to communicate with one another without fearing that another person is recording their private actions and could later threaten or shame the citizen. With the liberty to act on their autonomous choices, citizens can associate with others, utter statements or participate in publicly controversial actions that can fundamentally shape the values that structure their public and private attitudes – private actions influence public

attitudes and vice versa. If citizens believe or expect that their actions might be monitored, while actual restraints (i.e. coercive or preventative techniques or technologies) might not restrict their actions, they can fall prey to imagined restraints and adjust their behaviour in light of imaginary bonds that are as strong (or stronger) than shackles of steel. These self-imposed restraints can diminish the range of liberty that individuals feel safe exhibiting, which is conjoined with a corresponding diminishment of autonomy as citizens feel unable to make self-legislating choices, let alone act on them. In this light, we can say that "the right to liberty embraces in part the right of persons to make fundamentally important choices about their lives and therein exercise significant control over different aspects of their behaviour."[63] Privacy is the umbrella that protects core principles that all citizens share, and it ensures that citizens can make the decisions that are fundamental to their private and public development. Privacy facilitates the environment where people can learn, experience, and experiment without fearing hidden or latent punishments for making choices that deviate from public norms in ways that are neither self- nor other-harmful.

Moreover, the right to secrecy is invaluable because it opens a space for individuals to act and express themselves to others in deeply intimate ways, ways that they might be uncomfortable or unable to mirror in the public sphere and that are essential to their personal development. Donald Winnicott, a widely-influential psychoanalyst, notes that in public environments where we must conform to particular rules and norms we adopt a "False Self" to mask our "True Self" so as to avoid being overly vulnerable to strangers.

[63] Judith Wagner Decew, referencing Parrent (1997) *IPP*, 41-2.

Winnicott notes that some of his patients feel so ashamed of their "True Selves" that they are utterly incapable of accessing their inner world and, as a consequence, cannot manifest it to others[64] –they are perpetually trapped in the public gaze. 'Normal' people do not experience this crippling insecurity, but their relative fearlessness would likely evaporate were they deprived of their privacy rights. If co-workers, police, clergy, and your employer could all learn about anything that you said, the likelihood of freely expressing your "True Self" would diminish alongside your reasonable expectations of privacy. Within zones of secrecy – in the arms of a lover, the deathbed of a relative, or in letters between distant but good friends – privacy preserves safe spaces where individuals can be vulnerable to one another without being paralyzed by the possibility of their words being disclosed. Privacy rights are legal affirmations that spaces of vulnerability ought to exist so that individuals can develop and express their most intimate thoughts and beliefs.

In panoptic environments, where individuals' public and private actions are persistently monitored (effectively abolishing the substantive realization of physical or communicative seclusion), subjects feel as though the possible application of coercion could occur at any moment. Individuals experience a constant pressure to conform to public norms even before taking actions that deviate from the dominant ethical-political norms. The thought alone of deviating from social norms leads individuals to worry that authorities might have detected the individuals' deviancy. In situations where individuals persistently fear being monitored they reduce the scope of their actions so

[64] Donald Winnicott (1965) *The Muturational Processes and the Facilitating Environment: Studies in the Theory of Emotional Development,* 140-52.

that none of their actions could possibly be recognized as deviating from the public's norms; they self-censor their words, they feel incapacitated to even ponder certain decisions, they 'rehabilitate' their deviant physical behaviours. In short, they experience deprivations in their ranges of choice. These environments do not just stop individuals from engaging in actions they want to perform, but mould their very behaviour. The operation of bodily surveillance in panoptic environments leads the individual to restructure cognitive pursuits to harmonize their actions with the norms held by the surveying parties.[65]

Discussions of panopticonism almost invariably lead to discussions of Michael Foucault's *Discipline and Punish*, but perhaps rather than attending to his work, we should turn to Oscar Gandy's conception of the 'panoptic-sort'. Gandy, writing with an awareness of the sorting potential of computer databases, suggests that what is at issue isn't so much that we are being watched, but that the watchers allocate those observed into particular categories. These categories are based on normatively ambiguous search and sort criteria that those observed are not made aware of, nor have given their consent to. Generally, three core issues arise when panoptic-sorting causes individuals to experience deprivations of their informational, accessibility, and expressive privacy. The first is that individuals must often bear the burden of proving their innocence rather

[65] While outside the scope of this thesis, the issue of what norms the surveying party holds is of particular importance. Without knowledge of the surveyor's norms the problem of ontological security arises, where a person is unable to ground their identity. In environments where actions are being passively monitored without noticeable consequences individuals can experience a compression of public and private spaces and their associated norms. These compressions can lead to extensive spatial neuroses. For excellent evaluations of the effects of the development of neurosis that emerge from the experience of ontological insecurity I refer you to John Russon's *On Human Experience* and R. D. Laing's *Politics of the Family* and *Politics of Experience*.

than others having to prove the individual's guilt. To elucidate, a panoptic-sorting could occur at any time and place an individual in an undesirable category based on an out-of-context comment that was repeatedly quoted in popular media. The individual becomes perpetually guilty of any comment they have made and must be prepared to defend themselves against its potential implications at any point in their lives. The second issue is that these sorting environments impose a set of homogenous norms. As Lawrence Lessig notes,

> [w]e all desire to live in separate communities, or among or within separate normative spaces. Privacy, or the ability to control data about yourself, supports this desire. It enables these multiple communities and disables the power of one dominant community to norm others into oblivion.[66]

The plurality of nation-states, and the dignity each person deserves, can become endangered if individuals are not shielded from a totalizing normative structure that forcefully imposes itself across the entirety of their lives. The nation-state, as an inclusive body that remains sensitive to the particularities accompanying new members, faces political stagnation if it cannot continue to resolve the dual problems of legitimization and integration. These problems have been resolved through the use of discourse to legitimatize political norms. Importantly, this discourse incorporates a diverse range of privately and publicly generated norms instead of exclusively drawing on homogeneous ethnic-logics. Yet, the compression of normative spaces threatens to return the nation-state to a normative attitude bearing resemblance to that of ethnic-

[66] Lawrence Lessig (2006) *CV2*, 218.

states, which were unsuccessful at generating citizen-solidarity in pluralistic environments. Finally, the panoptic-sort is accompanied by the exertion of micro-control over subjects – discipline develops that can strike perfectly at particular individuals. This micro-control develops as individuals increasingly become wrapped in what Cass Sunstein terms 'data cocoons'.[67] Sunstein, a distinguished professor of jurisprudence, suggests that when a person's life is entirely accessible and searchable, it becomes possible to accurately determine the person's preferences, dreams, fears, loves, and hatreds. The accuracy of such predictions lets authority figures perfectly supply information that a person is interested in and, by reinforcing preferred data streams, data cocoons develop as individuals' liberty and autonomy are eroded alongside the possibility of encountering philosophies, products, or news that deviate from their already established preferences.[68] This creates an especially problematic environment for developing critical political awareness because these cocoons deprive individuals of contrasting political discourse. Without knowledge of divergent political discussions surrounding the common ethical-political narrative and discourse that could resonate and promote shifts in political positions, individuals are effectively isolated from the range of discourse that is aimed at altering ethical-political norms to reduce

[67] Cass R. Sunstein (2006) *Infotopia: How Many Minds Produce Knowledge*, 97. Hereafter referred to as *I:HMMPK*.

[68] Cass R. Sunstein (2006) *I:HMMPK*, 75 – 102. This is the precise danger that arises when relying on new aggregation services, such as Google News, to collect and deliver targeted news that computational algorithms have identified as 'interesting' to an individuated reader based on their past news interests. Personalized news feeds are useful, insofar as they reduce the time individuals spend searching for news they are interested in, but they simultaneously decrease the likelihood of finding topics that are unrelated to or in contradiction to already demonstrated interests. It is new or contradictory attitudes and philosophies that often spur innovative thinking, whereas persistently receiving the same thoughts and opinions dulls individuals' critical faculties.

social injustice and enhance social cohesion. If slavery were still a legitimate practice in North America and all news provided to North Americans offered reasons justifying the validity of this practice, slavery would be less likely to be abolished than in an environment where such cocoons were more challenging to develop and reinforce.

Privacy protects individuals' liberty, autonomy, and secrecy. It mitigates the problems and dangers brought on by panoptic technologies by ensuring that individuals can freely associate, communicate, and argue with one another without fearing that they are either being surveyed or captured and inserted into meticulously crafted data cocoons. Privacy is valuable because it shields the essential liberties that citizens require in order to develop and express both their private and public normative attitudes, attitudes that provide the foundation for the political discourse responsible for maintaining citizen-solidarity.

3 Dominant Analogue Privacy Archetypes

All western nation-states use some normative framework to establish and evaluate their privacy laws. European Union (EU) member states abide by the EU Privacy Directive, the United States of America draws on its constitution's nascent privacy rights, and presently Canada relies on the Personal Information Protection and Electronic Document Act (PIPEDA) to guide and evaluate privacy legislation. In this section, I examine four dominant privacy archetypes that inform Western privacy frameworks and the challenges that they face in environments that are dominated by analogue technologies. Specifically, I examine (A) the intrusion archetype, and its difficulties in recognizing privacy breaches when private utterances are spoken in public;

(B) the market archetype, and its blindness to the actual inequalities and discrimination in capitalist markets; (C) the intimacy archetype, which protects personal statements but not impersonal private data; (D) the secrecy archetype, which emphasizes the role of compacts in establishing duties that govern information disclosures but that fails to register privacy violations when illegitimately disclosed information is subsequently rebroadcast. After examining these archetypes, I proceed (in section four) to consider the additional challenges that these archetypes face as records and conversations are increasingly digitized.

(A) The intrusion archetype

The intrusion archetype establishes guidelines that identify and respond to situations where a person's personal seclusion is violated. This archetype is intended to protect individuals' private affairs or concerns, and it bears remarkable resemblance to Judge Cooley's characterization of privacy as the right to be left alone – individuals can expect that there are places, such as their homes, that are free from surveillance. This archetype typically identifies public and private spaces (and the subsequent expectation to privacy) along conservative lines – the home and other enclosed personal environments are the only spaces where individuals can expect seclusion.[69] This stark division often contradicts how we perceive what merits privacy protections – when lovers seek a secluded space in national parks for a private rendezvous, they consider the space they use as private based on the intimacy of their exchanges. Under this

[69] As a note, it is these divisions that privatize the home that deeply concern feminist critiques of liberal privacy, as exemplified in Catherine MacKinnon's analysis of liberal discourse surrounding privacy. She argues that the stark public/private distinction facilitates domestic violence towards women and, as such, should be reformed.

archetype, however, if the private activity or conversation occurs in what is traditionally identified as a 'public space,' "it will fail to be secluded if it is in the public view or if it is overheard, seen, or otherwise observed by others,"[70] where 'it' refers to the private action in a public space. Moreover, this archetype does not register a privacy breach in cases where a public personage has their non-private information aggregated to form a comprehensive personal dossier about themselves. So long as information is not collected in an unreasonably intrusive fashion (i.e. it does not intrude on attempts to seclude themselves), and what is collected is not confidential, then consolidating the person's public records so as to predict future actions does not register as a violation of a person's right to privacy.[71]

(B) The market archetype

Market efforts to mediate possible privacy breaches generally involve the equation of privacy and individuals' private information with commercial property like jewellery, hard currency, or land. Under this archetype, individuals should be allowed to sell elements of their privacy for goods and services just as they exchange personal capital for goods and services. Daniel Solove, a law professor who specialized in digital privacy law, notes that proponents of the market archetype's solutions insist that the market

[70] Judith Wagner Decew (1997) *IPP*, 48.

[71] Judith Wagner Decew (1997) *IPP*, 49. Notably in the United States, before Ralph Nader released a report damning General Motors' vehicles, he was placed under surveillance by the company – they tracked all of his movement in the public, interviewed acquaintances about his political, racial, and sexual views, and eavesdropped on telephone conversations. When brought before an American court, because the information collected wasn't gathered intrusively and didn't capture confidential information, the courts saw that under the intrusion archetype Nader did not have any cause to action. Moreover, in Canada, so long as the data for these dossiers is gathered from public spaces the data is 'fair game'. This means that if information is gathered by someone who planted a camera above your backyard fence to watch your actions in the backyard, so long as your intimate actions aren't recorded the data collection is typically legitimate.

will "achieve the ideal amount of privacy by balancing the value of personal information to a company . . . against the value of the information to the individual and the larger social value of having the information within the individual's control."[72] Under this archetype privacy breaches occur when personal information is acquired in violation of national laws that establish the process that market transactions are legally obliged to follow. The market archetype ignores the fact that markets for personal information will be biased and inefficient as a result of inequalities of information, resources, and power between market agents – individuals cannot evaluate the value of their information to particular corporations or government agencies without a complex understanding of the buyers' market status, their intent concerning the information, and the far-reaching consequences of selling away aspects of their privacy shield. In essence, individuals are unlikely to appropriately evaluate what the fair exchange rate for their privacy is,[73] and markets are unlikely to educate the public on the basis that such education could reduce profits. Moreover, individuals are often pressured into revealing information about themselves regardless of their privacy interests – they may be forced to reveal personal information before they can receive necessary services, products, or even employment. As corporate and governmental privacy notices presently stand, they are little more than sign posts that alert individuals of the policies, much like signs of yore warned travellers of nearby dragons. Privacy notices do not currently offer differing degrees of service based on the individual's interests; individuals are forced into take-all or nothing 'negotiations'. While the market archetype may force corporations to adopt flexible

[72] Daniel J. Solove (2004) *The Digital Person*, 78. Hereafter referred to as *DP*.
[73] Oscar H. Gandy Jr. (1995) "It's Discrimination, Stupid!" *Resisting the Virtual Life*, 42.

privacy policies that render different services based on what an individual reveals about themselves or face charges of price-fixing and mass corporate conspiracy, adopting these laws would subjugate the nation-state's norms to market logics and shift civic law from its constitutionally founded normative claims to foundations based on utility. The uncertainties that this archetype would introduce in private spaces and its unbalancing of civic norms make it a harrowing path to securing privacy rights, if a proposed commercialization of rights would let them continue to be termed 'rights' (as we presently understand them) at all. Without a set of normative rights to draw citizens together, citizens' solidarity would be jeopardized as they were less able to identify themselves with other citizens through their shared rights – rights would become a commodity that were possessed or realized according to individuals' unique market decisions rather than acting as a common normative bond. In the absence of common rights to guide ethical-political discourse, citizens would be less likely to recognize one another as equal co-legislators of law that was based in commonly asserted norms and, as a consequence, this archetype would contribute to social and political fragmentation.

(C) The intimacy archetype

The intimacy archetype recognizes that intimate information and/or activity "is that which draws its meaning from an agent's love, liking or care."[74] This archetype protects information based on intimate motivations rather than manifest behaviours. Unlike the intrusion archetype, the intimacy archetype protects private utterances in public spaces on the basis that the utterances draw their meaning from the agent's "True Self".

[74] Judith Wagner Decew (1997) *IPP*, 55.

Privacy breaches occur when an individual's intimate information – such as their sexual preference, spiritual beliefs, political orientation, or private dreams and aspirations – is revealed to the public without the individual's consent. While this archetype establishes norms that can guide legislation and establish when privacy breaches occur, it misses numerous events we classify as privacy breaches because it focuses solely on intimate expressions and activities. Information that does *not* draw its meaning from the agent's intimate life, such as bank records, credit reports, food choices, and other minutiae that people often desire to conceal, is not classified as private under this account. People's behaviour to conceal this information is not enough for it to be deserving of private status according to this archetype's norms; for any behaviour to be so deserving the behaviour must be the consequence of an intimate motivation. Consequently, legislation using the intimacy archetype's normative framework cannot secure the full range of information that individuals perceive as personal and as deserving privacy protections. This deficiency disqualifies the intimacy archetype from functioning as the sole archetype to guide lawmaking because it would lead to people censor their actions to avoid having possible deviant actions and behaviours recorded by others and, as a result, potentially stunt ethical-political discourse.

(D) The secrecy archetype

The secrecy archetype "focuses on breached confidentiality, harmed reputation, and unwanted publicity."[75] Under this archetype, when private information is publicly disclosed in violation of shared trust, or causes an individual to experience shame, or

[75] Daniel J. Solove (2004) *DP*, 43.

makes private matters public without legally acceptable justification, a clear privacy violation has occurred. This archetype registers privacy breaches when a private citizen's or public personage's seclusion is invaded and information about them that could be damaging to their reputation is acquired – acquisition is all that is required for a breach to occur, additional disclosure is not required. Moreover, when individuals must disclose their private information before gaining access to required services,[76] this model could characterize such revelations as unwanted publicity of personal information. This would act as a normative ground for dismissing company privacy fiats – this archetype would require such contracts to involve genuine negotiations to be legitimate; claiming 'here there be dragons' is not enough. Its capacity to represent the reconstitution of privacy policies would enable the secrecy archetype to realize the market archetype's ideal privacy norms, insofar as this archetype can provide grounds to punish market agents that require unmitigated personal disclosure before delivering essential services. Further, this model adopts the intimacy archetype's most positive contributions while avoiding its drawbacks because the initial publication of private information (i.e. making others aware of the actions that had occurred between private individuals) would be characterized as privacy breeches, as would be the collection of banking, health, or employment information, unless the individuals had expressly consented to the disclosure and collection of these latter types of information.

The difficulty before the secrecy archetype is that, while it recognizes initial breaches of confidentiality, it does not recognize rebroadcastings of illegitimately

[76] Services could include shelter, food, employment, bank accounts, travel tickets, mortgages, enrolment in educational institutions, et cetera.

revealed information as similarly damaging.[77] We expect to have a measure of privacy when purchasing condoms, haemorrhoid medication, or personal hygiene products – the pharmacist is not expected to rebroadcast our purchases, and we may be deeply embarrassed and/or shamed if the pharmacist did. By rebroadcasting our personal information, the pharmacist would have breached the transactions' implicit confidentiality. Unfortunately, by making my medical condition a matter of public record, a separate and unique breach is not recorded if a customer who overheard the pharmacist proceeds to then publicly rebroadcast my ailment. Moreover, the secrecy archetype cannot reliably provide guidelines that can distinguish between my desire to keep my purchases secret from some people and not from others – it's possible that I want my significant other to know that I've purchased contraceptives, but I don't want my orthodox Catholic employer to know that I'm acting contrary to their deeply held religious beliefs. What the secrecy archetype highlights is that we want to be able to control the flow of our information and limit its use to ways that we approve of. While this archetype does establish norms confirming that individuals ought to be the original 'owners' of their privacy, it does not provide guidelines capable of adequately distinguishing between legitimate and illegitimate public disclosures of private information and, as such, misses a core element of the socialized role of privacy.

4 Digitization and Its Effects

Western nations are currently in the midst of an information revolution. As fibre-optic cables are spun like spider webs, there is an accompanying impetus to transform

[77] Daniel J. Solove (2004) *DP*, 144-5.

past records, pictures, conversations, and media broadcasts into digital formats so that they can be easily searched, modified, synthesized, and transferred alongside other digitized media. This process of digitization, or translation of information to computer-readable formats, is leading to incredible gains in speed and flexibility of data transmission and analysis. Using digital networks, it is possible to send a packet of a voice conversation along a fibre-optic cable, followed by a packet holding several pixels of a digital picture, followed by another packet carrying characters in an email, and followed by another packet of the same voice conversation. Digitizing information increases the realizable efficiencies from fibre-optic networks – whereas cabled networks were once limited to distributing a single type of communication media, networks are now simultaneously instant message, video, and picture distribution networks.

Most citizens leave digital breadcrumbs that can be used to trace their routine activities. When paying for bread with a credit or debit card, the transaction is recorded by a major financial institution. When paying a bill, either late or on time, the record of payment is entered into a digital database holding information on millions of other customers. When returning a census to the government, all of the information is then inserted into government databases to determine citizen preferences, compositions, and values. When travelling with a cell phone, the associated mobile company can record where their customers go and the durations spent at each location. Individually the information from discrete transactions or transit paths is not terribly valuable, but as data aggregators acquire a vast swath of information about a wide range of people

and their activities, they develop a considerable predictive ability. Aggregated databases are perhaps well understood as digitized Seurat paintings; while individual dots may not be revealing, after they are juxtaposed against one another, they present a cohesive image. Knowing that you drink Pepsi-cola rather than President's Choice cola, prefer Hilfiger shoes and shirts over Campus Crew products, and dominantly purchase high-grade liquors are nearly useless tidbits of information when independent of one another, but when they are accumulated, it becomes possible to capture people's expressions of their identity through the products that they purchase. While we are not the products that we purchase, we do exhibit ourselves through them; this information can assist data collectors launch more effective marketing campaigns because aggregated data can make people vulnerable to marketing campaigns that target individuals with the accuracy of smart-bombs.

Digital dossiers are files that hold individuals' digitized information. Individuals may only be partially captured in their dossiers because many important facets of their lives are not, and perhaps cannot, be easily entered into an algorithmically searchable database. While it is possible to categorize the religious denomination a person identifies with, the reasons motivating that identification and their critical evaluations of the denomination's teachings are more challenging to capture. Given the (present) challenges to collecting this uniquely identifiable contextualized information, individuals are often classified according to standardized biographies or categories that are "based on stereotypes about their values, lifestyle, and purchasing habits."[78] These biographies

[78] Daniel J. Solove (2004) *DP*, 46.

are reductive, unauthorized, and are at best only partially true. People's digital dossiers routinely possess false information – when a marketer accidentally enters an extra letter in a person's name, that error is often transcribed across the entire database and any that it cascades information to. While whether or not Adidas spells your name correctly on marketing information is a trivial matter for most people, when your Social Insurance Number is mistakenly entered as being that of a convicted rapist, the matter can be of grave importance. As an example, if you were incorrectly identified as a rapist, some localities would distribute your name throughout the community, alerting its members that a sexual predator was in their midst. Even if the problem was remedied (assuming that the person discovered the mischaracterization), database errors are commonly pervasive and regenerative – fixing an incorrect record may only temporarily resolve the problem; a master database may impose its (incorrect) information over the corrected information days, weeks, or months later and provoke the same problems that prompted fixing the record in the first place. Without knowing the relationships between databases, it can be challenging, if not impossible, to confidently correct database errors. As digital dossiers and computer algorithms are increasingly used to automate decision-making about and for us, the errors in our dossiers will likely only escalate in frequency and magnitude.

The ease of generating and populating these databases must also be noted. Whereas in previous eras it was extremely time consuming to gather vast quantities of information from a diverse set of sources because of records' spatial and technological distribution, their digitization simplifies the process of importing data into these giant

databases. Data exchanges are now incredibly common– corporations generate massive super-databases from the data their subsidiary businesses collect and then petition governments to access census data, which they correlate with their databases to further develop their dossiers on individuals without the individuals ever realizing or consenting to the aggregation. As Oscar H. Gandy Jr. notes when evaluating corporations' ability to leverage massive amounts of client information,

> Telecommunications firms like AT&T that are also in the business of granting credit, and which perhaps will soon be in the business of providing information and entertainment through subsidiaries or partnerships, will have a distinct advantage over smaller entities in fewer lines of business. That is, credit information, and the information derived from numerous transactions, is available to the multiproduct firm at a far lower cost than it might be acquired (if at all) by competitors. Most of my concerns, however, are not focused on the market or society, but on the consequences for individuals. . . at its best the panoptic sort is guided by a utilitarian, rather than an ethical standard . . .[79]

In addition to lowered costs of implementation, aggregating content in contemporary digital databases is less obviously invasive than prior analogue aggregation techniques. The United State's National Security Agency (NSA) recently demonstrated the ease of covertly surveying the digital communications of massive numbers of people. Whereas truly mass-surveillance would have historically required agents to listen to every phone conversation that took place, open each piece of mail,

---

[79] Oscar H. Gandy Jr. (1995) "It's Discrimination, Stupid!", *Resisting the Virtual Life*, 41

and monitor each photo and audio recording, the NSA presently just copies all the digital information that passes through major American telecommunications network hubs through their own computer systems. With the data on the NSA's systems, sophisticated computer algorithms can be used to determine what conversations should be investigated for being related to domestic and foreign terrorism.[80] Those subject to the surveillance (which, given the distributed and networked structure of the Internet, alongside with the amount of Internet traffic flowing through major American data hubs, likely means that a significant portion of *world* digital communications are being subject to this surveillance) are none the wiser – had the NSA's activities not been made public by a whistleblower, the American spy agency would have even fewer restrictions on their surveillance than they do today. Given the ability to engage in surveillance and data collection without the surveyed ever being aware of the surveillance, we can understand how digital surveillance significantly differs from its analogue predecessors, both in scope and secrecy.

In light of the digitization of information, the easy aggregation of digital records, and ease of mass surveillance in the digital era where the surveyed never realize they are being scrutinized, we should return to the privacy archetypes from the previous section to evaluate whether their guiding metrics can effectively protect individuals from illegitimate digital surveillance. Can they effectively guide lawmaking in the digital era so that citizens in Western nation-states can maintain their traditionally realized rights to privacy whilst using digital systems? If they cannot (as I will argue is the case), we will

[80] Ryan Singel (2006) "Whistle-Blower Outs NSA Spy Room," *Wired*.

have to find an alternate privacy archetype if we are to secure privacy rights and free speech in the digital millennium.

(A) The intrusion archetype

Recall that if information is not collected in an unreasonably intrusive fashion and what is collected is not confidential in nature, the collection does not violate the intrusion archetype's normative guidelines and no privacy breach is registered as having occurred. Much of the data that is digitally collected is either given willingly by individuals to data collectors or is secretly collected using either cookies or by harvesting information from public records. Cookies are small computer files that are automatically downloaded onto most computers when visiting websites. They can benefit end users by remembering personalized settings for websites they have visited, but they can also log the sites that their computer visits and, in some cases, the amount of time spent on each site. This information is useful to data collectors because it provides insight into particular online and offline interests, and this information could potentially be used to shame individuals were the information made public (for example, a celibate monk who was found spending extensive periods of time on Internet dating sites might experience considerable shame for actually, or nearly, breaking their vows if the information was disclosed). Despite the possibility of shame, because the collected information isn't confidential (it's no more invasive than watching someone walk into a brothel), laws formed using the intrusion archetype would need to establish that cookies and intentionally inputting personally identifiable information is "unreasonably intrusive." This doesn't seem to an effective translation of how these norms have been applied in

analogue situations, where intrusion is identified as being overt and/or evidently harmful. While appropriate translations of laws and normative archetypes involve abstractly accommodating their norms, they must also remain consistent with the basic structure of prior laws. Judges are hesitant to make judgments that appear to be political and, as a result, it is likely that they will "increasingly defer to the political branches: If the judgements are policy, they will be left to policy makers, not judges."[81] For the political branch to establish competent policies, they must have their decisions guided by privacy norms that simultaneously appreciate the challenges of digital environments and the legislators' constitutional histories. The intrusion archetype lacks this comprehensive environment and political awareness and, as such, is unsuitable to act as the legislators' guide for privacy legislation concerned with digital spaces.

(B) The market archetype

The market archetype's weaknesses are highlighted when turning to the Internet and information's digitization. Websites that people must visit in their daily lives are littered with privacy agreements that must be agreed to before gaining access to the site's resources. Before using online banking, ecommerce websites, or booking health appointments online, a person must first accept the website's (and its associated institution's) privacy policy. To use a VISA or MasterCard in economic transactions individuals must allow their purchases and credit information to be subject to intense algorithmic analysis. Receiving a job often depends on a criminal background check, which draws on police databases to determine the application's criminal history.

[81] Lawrence Lessig (2006) *CV2*, 317.

Accessing corporate or NGO email accounts require giving network administrators access to oftentimes private messages. In all of these cases, individuals must accept institutions' privacy policy to receive services and, consequently, must make themselves vulnerable to the possibility of being incorrectly categorized in a collector's database. This vulnerability is significant because digital records commonly hold inaccuracies that can lead to discrimination in people's daily lives: a person's credit request might be denied, someone might be given priority seating on a plane at the expense of other people's comfort because of their frequent flying preferences, or (more seriously) they might be denied employment for being incorrectly labelled a rapist. Without the ability to inspect their database record, or even the ability to selectively choose services based on a willingness to accept portions of privacy agreements, the market archetype's suggestion that privacy is simply another commodity demonstrates its failure to recognize the divergence in power relationships between consumers and corporations. Until consumers can retain (at least) a provisional role in how their data is used (letting them personally oversee and safeguard their informational privacy), they should not be expected to forfeit their constitutionally established privacy rights – market proponents must provide an argument for how they would avoid social injustices stemming from power inequalities and knowledge discrepancies. Moreover, their argument would have to address the normative (rather than empirical) reasons for *why* citizens should abandon discursively generated privacy norms for the market's strategic norms. Until market proponents adequately articulate an argument that responds to this criticism,

their model should be viewed with suspicion by those immersed in the digital revolution.

(C) The intimacy archetype

The intimacy archetype is remarkable because, were its norms used to guide digital lawmaking, it would oppose the accumulation of most voice conversations and emails on the basis that the content could be assumed to be intimate,[82] with the onus on the data collector to prove otherwise in a court of law before gaining access to message content. This legally imposed limitation would preclude the mining of personal information from instant message conversations and limit Voice over Internet Protocol (VoIP) chats from being admitted into databases on the basis that surveying these conversations intrudes on intimate activity that draws its meaning in the agent's love, liking, or care. This said, intimate information or activity under this definition does not include information about bank records, the news sites a person visits and the stories that they read, or the recipes they search for. While this archetype's norms would protect clearly private conversations, which arguably are the richest sources of personal information, this model would not register privacy breaches when marketers collected vast sums of non-intimate information that could be used to create a digital composite of an individual. Again, while atomistically what a person buys, reads, and listens to are not terribly helpful in decoding their habits, as the information is aggregated to develop complex digital dossiers, it is possible to target individuals with questions that they

[82] *Warshak vs. United States*, (6th Cir. June 18, 2007). Indeed, the United States 6th circuit judicial court has determined that the content of email can only be searched with a warrant, based on a reasonable expectation to privacy, though law enforcement is not required to get a warrant to determine the email's transit path.

should (according to their profiles) be willing to answer and increase the accuracy of the dossiers', databases', and algorithms' predictive powers. Without entirely redefining the range of 'intimate information' to establish a new normative boundary capable of registering the challenges to privacy arising with the digitization of information, – in effect redeveloping, rather than translating, our understood definition of 'intimacy' – we can set this model aside due to its inability to comprehensively entrench privacy rights in the digital era.

(D) The secrecy archetype

As we recall, the secrecy archetype "focuses on breached confidentiality, harmed reputation, and unwanted publicity."[83] Under this archetype, any disclosure of individuals' digital dossiers that violated the parties' privacy agreements would legitimize individuals' seeking legal recourse. Moreover, if the disclosure resulted in an individual's reputation being injured, such as if their children or co-workers learned about previous legal indiscretions, legal avenues could be legitimized to rectify the breach. Finally, if the information in the database was made public and subsequently led to a person's reputation being injured, this archetype would register a privacy breach and justify legal responses.

While the secrecy archetype is best suited for mitigating privacy violations of the four archetypes examined thus far, its underlying premise that data aggregators even remotely want their data made public mistakes the intended use of most digital dossiers or databases. Information in these mammoth data compilations is intended to remain

[83] Daniel J. Solove (2004) *DP*, 43.

secret – databases afford corporations and governments a (relatively) deep and secret degree of insight into a large body of individuals, letting data collectors craft policies and campaigns that are strategically calculated to resonate with individuals' particularities. The value of maintaining private databases emerges from the particular insights that are presented through the dossiers' data – market forces invest data collectors with strong interests to keep their databases secluded from public light because their publicity would reduce competitive advantages that arise with the accumulation of vast amounts of data. As a result, public disclosure of the information is a deviation from preferred business practice – while it is important to recognize that these deviations do sometimes occur, and that restitution is deserved when these breaches occur, it is perhaps more valuable to focus and regulate how the information is typically used.

In addition to missing the core purpose of databases, the secrecy archetype does not address the issue that an individual's reputation could be accidentally harmed if their record were seen by a person who personally knew the individual. Most databases capture only raw statistics and values without providing any texture, which may cause someone reading a digital dossier to arrive at misleading conclusions about the people associated with these dossiers. Databases may not, for example, identify why a person is on a sex offenders list: it might be that a woman displayed her breasts during a particular political protest and was convicted by a particularly conservative district attorney for being a threat to the public good, which led to a harsh punishment and her placement on a sex offender list. The presentation of this information to an associate of the offender does not constitute harming the offenders' reputation assuming that the

list is already publicly accessible; the dossier has only compressed the information available in public databases, rather than distorting the truth and using it for slanderous purposes.

Individuals are typically powerless to add data, or 'texture', to their files; the sex offender is unlikely to be able to add an explanation for why she is classified as an offender. This textured information could severely reshape the story told by particular data entries, but it is challenging to make textured information machine-readable, which prevents algorithms from effectively analyzing the 'texture'. Perhaps most significantly, many of the digital records that are generated about individuals are created without their ever knowing. With the example of the NSA's spying actions in mind, breeches of confidentiality are unlikely (collectors actively try to keep their databases private), publicity is unlikely because it would decrease the value of the data (imposing market-pressures to keep this data out of the public eye), and injuries to reputations are only as likely as it is that uniquely identifiable personal information is publicized. Thus, while the secrecy archetype can normatively identify privacy breaches that arise with the *disclosure* of personal information, it fails to wholly recognize the challenges that arise as data is aggregated, secret profiles created, and information in compressed to be made machine-readable.

Lastly, but importantly, someone must be accountable when there is a privacy breach stemming from a digital data collection – it must be possible to identify who is responsible for the breach in order to apply coercion – and this archetype struggles with the fact that privacy breaches occur beyond the initial broadcasting of personal

information. Even when individuals can be held accountable, punishment cannot reverse the harm already experienced. While this was true even in analogue situations, in digital environments where data transmissions can be sent to millions of recipients at the click of a button, it is nearly impossible to 'pull the plug' and prevent mass dissemination of private data. At its best, the secrecy archetype demands personal accountability for safeguarding databases and requires punishments for those responsible for privacy violations, but it does not inherently recognize the subsequent harms from retransmission of personal information as privacy breaches themselves. This failure occurs because the secondary breaches are just transmissions of publicly held information – while harms might result from the widening transmission of information, the secondary transmitters (so long as they cannot be seen to have a confidentiality agreement with the individual whose information they are publicizing) cannot be normatively identified as violating the individual's privacy. Our present digital environment is becoming Kafkaesque, where the bureaucratic process is careless, unconcerned, and dehumanizing in its reduction of people to numbers that people have little role in legitimizing or consciously shaping. With the challenges presented by the rapid development of digital dossiers in mind, we will proceed to investigate the relationship between privacy, discourse, and politics, and come to realize that it is important to establish a new privacy archetype if we are to preserve the citizen-solidarity presently found in Western societies.

5 The Political Impetus for a Digital Privacy Archetype

Nation-states develop their modes of political association on the basis of discursive citizen-solidarity that is oriented around shared participation in lawmaking. As a result, nation-states must deeply embed free-speech in their constitutions because citizens must be free to express their opinions, concerns, and arguments in the process of forming law so as to see themselves as both the authors and addressees of law. When citizens can speak with one another on the basis of their shared rights, they begin to recognize each others' dignity and value in the process of identifying and working to resolve common problems that transcend their particular localities. Their mutual appeal to shared rights operates as a field to delimit, and subsequently identify, just courses of action in particular situations. In the process of exercising free and open political discourse that is framed by the constitution they generate constitutional patriotism and citizen solidarity. When able to communicate with one another without fearing federal, state, municipal, or private oversight of intimate, confidential, or secluded conversations, citizens empower themselves through their legislators to discuss matters of politics, laws, sexuality, religion, and justice with their fellow citizens. As a result of discourse's central role in maintaining a functioning deliberative democracy, especially given the growing pluralism and growing potential for intended and accidental discrimination as the majority social culture conflicts with minority cultures, it is incredibly important that all citizens can raise their voices to challenge any and all perceived discrimination. If nation-states are to genuinely embrace the principle of free discourse that is necessary for their continued political stability and citizen-solidarity,

where any member of society can have a role in shaping the ethical-political discourse, all members of the society must be substantively capable of speaking openly.

In an environment where individuals cannot be certain that their private conversations will remain private, they are less likely to engage in contentious issues, associate with deviant groups, or visit areas of political contestation. Their sense of shame, or fear of being shamed, inhibits their actions, actions that if taken could lead to significant personal discoveries that could transform their attitudes and affect the strength and composition of the discourse that they subsequently participate in. For Habermas this potential self-censoring stemming from the possibility of experiencing public shaming means that the lifeworld, the environment where individuals gather to communicate with one another and reach mutual consensus over contested issues, is endangered. Without certainty that the rules of discourse, especially the rule that coercion will not to be deployed against participants, are being approximated, citizens are less likely to openly participate in the discourse responsible for framing their prospective life-projects. Fearing the consequences of appearing as a social deviant, citizens turn to non-inclusive discussions that are either held in extreme secret or that stridently adopt public norms and resist norm-deviating contributions from taking hold in ongoing discourse. Without a full range of discourse, the ethical-political narrative fails to account for the full range of social diversity, leading citizens to decreasingly feel or experience themselves as involved in the law's legislation. Unable to recognize the constitution's core principles of free speech and inclusivity in the legal and political domains, citizens perceive themselves as mere subjects of, rather than equal discursive

participants in, the nation-state. As free speech, the lifeblood of the democratic nation-state, is replaced with the possibility of all-encompassing surveillance the central principle of democracy itself may slip away.

In light of the grim challenges accompanying the digital millennium, most importantly the possibility of massive, unsanctioned, aggregations of personal data and a subsequent chilling of free and open discourse, it almost seems as though citizens might be best served by working to desperately slow, reverse, or banish altogether the digital communications technologies responsible for this possible denigration of free speech and to 'return to the good old days' of analogue technology, where previously asserted privacy archetypes could effectively protect citizens' communications. As Judith Wagner Decew and Lawrence Lessig both insist, however, there is no reason why technological architecture cannot be modified to preserve our long-standing traditions.[84] Adaptations can take the form of fundamentally restructuring the technology itself (as Lawrence Lessig suggests, and will be discussed later) or reshaping the norms and laws that guide the exercise and implementation of digital technology (which I will later suggest is the best way to approach this issue). Before evaluating these solutions, I want to briefly focus on why digital communications offer hope for extending the scope, range, and potency of citizen-solidarity – I want to reveal the positive political applications of digitization.

The features of digital communications, from their low costs of data transfer and translation, to their easy storage, and universal underlying language, provide the

[84] Judith Wagner Decew (1997), *IPP*, 161 and Lessig (2006) *CV2*.

possibility for citizens to connect and communicate with one another as never before. Not only can Canadians on opposite sides of the nation to talk with one another affordably as a result of the lattice of digital networks surrounding them, Canadians have the advantage of being able to communicate rapidly with one another and retain referential documents so that they can develop vibrant discourses where new participants can learn what has been said before their entry and can challenge the validity of asserted claims without losing the discourse's initial trajectory. Moreover, digital communications and the generation of conversational records can happen without hours of transcription; modern instant messaging and email technologies are adapted for instantaneous transcription to text, speech, or image. These communicative systems have the added advantage of not discriminating against the deaf, blind, or mute; digital technologies can draw historically disadvantaged members of society into the ethical-political discourse as equal participants. Moreover, Internet forums and chat sites let people test their arguments with citizens and aliens alike, few of whom have met face-to-face and with whom they would have been unlikely to have shared in discourse without digital communications. These discourses can extend citizens' awareness of the range of pluralistic attitudes and arguments that pervade the nation-state. The possibility of extending the range, depth, and quality of discourse can theoretically increase as more and more people can enter online environments.

Further, because digital networks are interoperable and lack a single point of control people can discuss taboo topics even when governments or corporations attempt to censor discourse. In Iran's case, the government has tried to prevent Iranian citizens

from accessing social networks such as orkut[85] because discussions on these networks conflict with ethical codes surrounding Islamic dating and relationship codes. Despite the Iranian government's best attempts, Iranian citizens continue to use social networking sites – the government's attempts to block the dataflows are simply routed around. Similarly, Chinese citizens have developed ways of conversing with each other about state-declared taboo or illegal topics by bypassing the 'Great Firewall of China', a digital content-filtering system that censors discussions and prevents citizens from disseminating or receiving 'unbalancing' or 'subversive' news and information.

While there are technological ways of avoiding digital blockades and making speech anonymous to bypass governmental and corporate censors, it cannot be assumed that all citizens will have either the technical knowledge or confidence to use these electronic countermeasures, especially when the price for failure can include torture, imprisonment, public shaming, or death. Thus, it must be noted that while digital networks technically enable citizens to communicate without relying on a central switchboard, which can reduce the likelihood that citizens can be prevented from talking to one another, the technical possibilities of evasion are not adequate responses to systemic legal or social injustices.

In addition, a transparent communications network that citizens trust to not survey their digital actions and words could lead to bridging the divide between domestic and foreign spheres of political action. Digital networks make it possible to affordably learn what issues are affecting individuals in other countries giving Canadians citizens, for

[85] orkut is a social networking service that is increasingly popular in South America and the Middle East, especially Brasil. The service's name is not capitalized.

example, insight into how Canadian foreign policy is detrimentally or positively affecting the Nepalese. Canadians can become aware of how their governments' political actions affect others in the world by speaking with those others rather than depending on corporate news reports or de-personalized government reports; a global communications network that can be trusted to not survey individuals' digitized actions and expressions can facilitate awareness of the commonalities between citizens of differing nation-states and allow citizens to craft ways of collaboratively exercising influence over their governments to remedy commonly experienced injustices. This transparency between the actions of domestic decisions and their consequences on foreign nations will likely improve as projects such as the One Laptop Per Child (OLPC) initiative are spearheaded across the world. OLPC is an MIT-based program that aims to put electronics notebooks in the hands of children throughout the developing world. These notebooks can autonomously create digital networks that do not, on their own, censor speech and can offer children a chance to communicate with the larger world. So long as one computer in the autonomous network has Internet access, all the computers it is associated with can send and receive instant messages and email with people around the world. With the ability to hear the situations of children in Kenya, Ethiopia, northern Brazil, and other areas of the globe that are persistently affected by Western actions, it becomes increasingly possible for citizens, once aware of how their government's decisions affect others, to motivate their governments to adopt policies that are sensitive to the areas of the world that domestic policies affect. Digital networks offer the possibility of extending the definition of domestic beyond the

borders of the nation-state to include those affected by the state's actions and who reside in foreign countries – these networks open a space to start a substantive debate about the possibilities of conjoining domestic and foreign politics into 'politics'.

In light of the positive possibilities that digital communications offer, in addition to their increasing prevalence in our daily lives, it is critical that we develop a privacy archetype that shields us from unwanted public intrusion on our private lives and actions. With this goal in mind, we turn to archetypes that are intended to confront some of the challenges to communicative privacy that have arisen in the digital millennium and that are intended to once again secure spaces where state-level, citizen-solidarity can develop alongside wider international discourse. Ultimately, I propose that my own reciprocal archetype of information responsibility provides a normative framework that can mitigate the challenges that arise alongside the possibility of unobtrusively surveying digital communications. By securing communications from undue oversight and coercion citizens' discursively generated solidarity can continue to thrive while simultaneously shielding the lifeworld from the discourse-stunting influences of coercion and shaming that arise with the possibility of comprehensive public surveillance.

CHAPTER THREE - DIGITAL PRIVACY ARCHETYPES AND CITIZEN-SOLIDARITY

In light of the difficulties that analogue privacy archetypes experience when thrust into digital environments, we turn to contemporary proposals that attempt to address the challenges that arise with digitizing communicative mediums. Technologists have developed two especially prominent ways of alleviating privacy breaches in digital environments. The first asserts that abstracted laws ought to be created that influence the design of computer code, which can then be written to safeguard citizens' communicative privacy. The other proposes that computers be programmed to automatically forget, that is, delete, information after specified periods of time. Unfortunately, these responses would distance citizens from the process of lawmaking and their cultural histories, which leaves these technologists' proposals as unsuitable for securing citizens privacy in digital environments given citizens' traditional democratic and cultural values. In light of technologists' deficiencies, I introduce the reciprocal archetype of informational privacy, which offers discursive possibilities that can theoretically shield digital communications from illegitimate surveillance and can be used to facilitate public discourse. This archetype has the benefits of contributing to the development and expansion of discursively realized civic-solidarity, as well as preserving the viability of the Habermasian political project in the digital era. Specifically, by protecting digital communications from surveillance, the Habermasian lifeworld is shielded from colonization because its discursive structures will resist being stunted by coercion or surveillance that citizens have not themselves approved. Ultimately, after

shielding citizens' communicative and informational privacy at a national level, citizens can safely communicate with each other and other members of the digital era to develop and maintain their discursively grounded citizen-solidarity.

1 Building Towards a Privacy Archetype for a Digital Era

While it has been made evident that past privacy archetypes are not wholly satisfactory for protecting citizens' privacy in digital era, it does not follow that an archetype for this new era should ignore past archetypes' strengths in the process of avoiding their deficiencies. Before advancing to technologists' or my own model's suggested resolutions to the challenges arising in digital landscapes, the privacy challenges past models overcame and failed to meet are summarized to establish a criteria that subsequent privacy archetypes can be evaluated against.

Turning first to the intrusion archetype, it is concerned with how information is collected – information cannot be collected in a manner that intrudes on individuals' accessibility privacy, or on their ability to exercise autonomy or liberty. This archetype's focus on accessibility privacy proves a problem in the digital era because information collection is rarely intrusive – information is carefully and quietly gathered, usually without disturbing citizens. This archetype reveals the clear need for digital privacy archetypes to be sensitive to non-intrusive violations of personal privacy.

The market archetype suggests that, after commoditizing information, individuals can protect their privacy according to their rational, self-interested market desires. It assumes that all individuals are equals and discounts power inequalities between individuals and their supposed information 'partners'. As a consequence of its focus on

monetizing privacy, this archetype fails to realize that customers' informational privacy plays a central role in how they develop their value structures and life projects – these are externalities to the market project, which focuses only on the 'property' understanding of privacy and personal information. A newly formed privacy archetype ought to address the issue of commoditizing privacy and recognize that an unduly burdensome set of norms will be challenging, if not impossible, to guide the strategic practice of lawmaking that must balance the preservation of constitutional norms alongside the market's vibrancy if the state is to collect taxes that are sufficient to maintain the its normatively driven welfare programs.

The intimacy archetype expresses norms that shield individuals' intimate activities from surveillance – though an action may occur in public, it is not necessarily motivated by public attitudes and, as a result, this archetype can register privacy breaches when recording private exchanges in public spaces. Unfortunately, while this archetype's norms protect the privacy of online conversations, it does not extend similar protections to digitized banking, tax, or property records. This archetype demonstrates that privacy norms can shield digital conversations from electronic oversight, as well as identifying the importance of focusing on the compilations of non-intimate data that are used to construct personally identifiable profiles.

The secrecy archetype registers privacy breaches when individuals' confidential information is publicly disclosed. At issue, however, is that such disclosures are failures on the part of data collectors to protect their own info-capital resources – these disclosures are exceptions to the rule of secrecy. Further, this archetype does not

include the need for individuals to be able to 'texture' their digital dossiers, which leaves individuals vulnerable to incorrect or misleading characterizations of their personal and public lives. Additionally, it does not recognize additional privacy breaches when illegitimately publicized private information is subsequently rebroadcast. Thus, this archetype reveals the need to appreciate the reality of data aggregation, as well as the need for individuals to have some control over information about them that is held in databases.

We can thus say that a privacy archetype for the digital era must recognize and overcome the following challenges:

(1) It must be sensitive to the usually covert methods of data collection, distribution, and use.

(2) It must be sensitive to the unequal power held between individual citizens and the groups that develop digital dossiers.

(3) It must acknowledge intimate and (seemingly) mundane data as deserving protection from secretive aggregation, discrimination, and use.

(4) It must realize the need to grant citizens access to their digital dossiers and the ability to texture them.

(5) It must recognize that any archetype that would allow citizens to learn who has their data, why they have it, and how they are using it cannot involve a discovery process that is unduly burdensome on either the individual or the market.

A privacy archetype that is sensitive to digital environments will possess norms that can recognize and rise to meet the above-mentioned challenges. While they appear to be simple matters of jurisprudence, as Lawrence Lessig observes, judges are largely unwilling to 'translate' laws, or take laws created for analogue environments and technologies and reshape them for application in digital environments. Courts, he writes, will likely step away from such translations because they feel "that these are new questions that cyberspace has raised. Their newness will make them feel political, and when a question feels political, courts step away from resolving it."[86] Translating law has been essential to maintaining constitutional values across different technological eras – free speech has been protected using different privacy archetypes that were developed to reflect changes in modes of communication, commerce, and mobility. While analogue archetypes could be translated for digital environments, the laws following from these translated archetypes would at best provide a mosaic approach to registering privacy breaches, and they risk failing to comprehensively protect individuals' privacy. Specifically, mosaic solutions involve appealing to hosts of oftentimes conflicting norms to secure particular rights. The challenge that arises with this proposal is that without primacy between different archetypes' norms, there is no definitive reason to prefer one normative account over another, save as a way to (hopefully) realize an end goal of entrenching the personal right to privacy. Norms ought not to be guided by particular social ends or else they lose their critical appeal – they are intended to guide particularities (in this case law) and to objectively evaluate the

[86] Lawrence Lessig (2006) *CV2*, 167.

success of particularities in meeting normative criteria. Rather than being forced to develop law from a series of individually flawed archetypes, we should draw on a new archetype that captures the reality of the new technological landscape, just as previous archetypes captured the landscapes at the time of their inception.

A newly realized privacy archetype must recognize and be sensitive to the following issues in the course of asserting a normative criterion that can adjust the present flow and use of digital information to protect individuals' privacy:

(1) It must recognize that when individuals share information they make themselves more vulnerable to coercion and shaming and, as a result, must recognize that receiving individuals' personal information brings corresponding obligations and responsibilities concerning how that data is stored, used, and transmitted.

(2) It must enable individuals to legitimize information transfers before they can occur.

(3) It must recognize the need for establishing safeguards aimed at preventing data breaches, mistaken categorizations, and algorithmic discrimination.

(4) It must realize that information capital is increasingly important to the market and, consequently, to the material substratum underpinning the lifeworld. Thus, it must seek a peaceful coexistence between the lifeworld and systems.

(5) It must extend the range of "personal data" to include individually insignificant shards of information that can be used to develop a personally identifiable digital dossier.

2 Code as Digital Law

Lawrence Lessig has famously equated code with digital law.[87] What he means by this is that the rules encoded in software programs bear many characteristics of law, insofar as they identify what a person can and cannot do in particular digital environments. He calls digital computer programming code 'West Coast' code, whereas the traditional laws that govern the speed that people can drive their cars at and that regulate citizens' public interactions are termed 'East Coast' code. The distinction between west and east identifies distinct seats of law in the United States of America – the west coast is home to Silicon Valley, whereas the seats of America's political power call the east coast home. This distinction also identifies the divisions of non-legitimated law (which is asserted through privately-developed and owned programming code) and legitimized democratic law (which is crafted and authorized in a public process that is representative of the citizenry).

In addressing the digital revolution's challenges to informational privacy, Lessig recognizes four major elements as being involved in regulating individuals' actions in digital spaces – the market, architecture, law, and norms. Markets are involved in regulating actions by imposing personal costs for disobeying laws, and architecture identifies the way that things are coded, which inherently establishes limits on actions. Law refers to 'East Coast' rules and norms establish values instilled through socialization. To analogously elucidate on this quaternary distinction, we can turn to seatbelt regulations in Canada. In Canada, laws punish individuals who do not wear seat

[87] Lawrence Lessig (2006) *CV2*.

belts when motor vehicles are in motion, children are educated about the importance of wearing seatbelts and develop norms concerning seatbelts that reflect public attitudes, and the market penalizes individuals who do not wear seatbelts when they are in accidents. Moreover, law requires car manufacturers to install seatbelts in cars during the manufacturing process – cars must have seatbelts 'coded' into their physical design. It is possible for any of these factors to be different – cars might be 'coded' to detect the number of people that are in a car and require their seatbelts to be locked before the vehicle's ignition can activate. Moreover, laws could be made harsher or less burdensome, and education could be used to more or less stringently teach norms. Each of these four elements is relatively malleable.

When Lessig turns to digital environments, he considers the influence that computer code has on how individuals interact in and with their digital landscape. The options and functionality that programmers design into software creates the software's limitations – while it might be possible to 'hack' the software and alter its capacities, most computer users cannot be reasonably expected to know how or be inclined to do this. Most individuals have their actions limited by what programmers choose to include in their software – their liberty, autonomy, and speech are all limited by the digital code. Lessig argues that effective regulation of digital spaces requires a combination of East and West Coast law to safeguard privacy. He claims that East Coast law is largely inefficient in safeguarding digital privacy because of the significant period of time legislators need to read, consider, debate, and implement law – given the rapidity of technological change, legislators' laws oftentimes trail technological advances. In light of the disparity

between the democratic legitimization of law and the rate of technological change, Lessig proposes that East Coast code (i.e. democratic legislation) provide citizens with some control over their personal information and simply requires West Coast code to enforce East Coast code. In essence, legislative assemblies would be responsible for developing wide-ranging abstracted laws from traditional privacy archetypes' norms and programmers would then be responsible for independently coding software in accordance with legislated law.

While Lessig's solution may be practical, insofar as it acknowledges the empirical challenges facing the process of legislation, it would have a series of negative effects across society. First, while it recognizes the legislative difficulties in establishing laws that are sensitive to the challenges brought about by digitization (such as the challenge to limit the blinding speed at which citizens' data is transferred), his proposals would impose legislation that only broadly asserts that software architecture ought to protect personal information and would fail to address the particular safeguards that would have to be implemented. This could prevent safeguards that might provide individuals with the most protection from being implemented because these protections might run counter to market logics. While safeguards might be implemented if required by legislators, there would be no way of guaranteeing that the best safeguards were being deployed.

Second, Lessig's solution would necessitate the extra step of requiring East Coast lawmakers to establish regulations that limit the transfer of illegitimately publicized

information. Given his faith in the free market,[88] Lessig might suggest that the market could meet this responsibility by having software programs require users to configure their privacy settings before they could use the software. This suggestion could enable users to enter privacy contracts that limit the broadcasting of public information, and thus restrict the possibility of republication. For example, Microsoft's Internet Explorer and Mozilla Corporation's Firefox could be designed so that the browsers access only sites that met the users' privacy criterion. Given his focus on the value of automation and attitudes towards the value of code being machine-readable, Lessig would likely suggest that before information is broadcast, an automated script would have to confirm that the broadcasting was permitted according to a corporate contract server that was responsible for authenticating the legitimacy of information transfers. Any such solution makes two assumptions: (a) that software and the digital spaces in which it is used are mutually-standards compliant[89] and (b) that individuals hold a default stance, rather than a granular attitude, towards their privacy. To expand, it is possible that a person is comfortable having their information shared across government agencies that have different privacy policies, while they hold a uniform policy regarding American corporate data collection groups, and yet another policy when it comes to some, though not all, Canadian corporations – a one-size-fits-all privacy configuration would miss this. For any kind of market realized privacy solution to function effectively, it must be easily understood by citizens and relatively easy to configure – an unduly burdensome process

[88] This is demonstrated through his works, such as *Code Version 2.0*, *Free Culture*, and *the Future of Ideas: The Fate of the Commons in a Connected World*.

[89] Maintaining digital standards and expecting all groups to meet and be aware of these standards is unlikely, as is currently demonstrated in the current challenges for web browsers to properly render websites because few websites are designed to be standards compliant.

would likely reduce the adoption of the market's safeguards and limit the substantiative realization of democratically asserted laws that are intended to safeguard citizens' privacy.

Finally, and arguably most importantly, Lessig's proposal fails to recognize harm as occurring when citizens do not see themselves as entirely involved and reflected in the process of lawmaking. While citizens may see themselves as the authors and addressees of East Coast law, they cannot similarly recognize themselves as such towards West Coast law. This lack of recognition largely stems from the lack of openness in most software development (where code is typically a proprietary secret) that would distance citizens from their historical involvement with all aspects of a law's institution. This means that citizens' concerns might not be adequately addressed when corporations discover that implementing solutions to those concerns is not financially viable. While markets might adhere to the minimums established by law they are unlikely to engage in a consultation process with individuals and groups that would be affected by West Coast law unless such consultations would increase profits. Without the transparency of democratically legitimated law, citizens do not necessarily see themselves in or trust law. In the case of the digital privacy laws that emerge from Lessig's suggestions, citizens might refrain from participating in open discourse because they cannot be assured that corporations protect individuals' privacy using the most effective code.

In contrast with Lessig's relatively complicated East Coast/West Coast scheme, Viktor Mayer-Schöenberger proposes a less extravagant use of code to minimize privacy concerns. Mayer-Schöenberger, a professor concerned with public policy, argues that

the central issue facing digital privacy comes in the form of data retention. While Lessig's proposed privacy filters would let individuals limit what kinds of data-relationships they enter into, Mayer-Schöenberger suggests that all digital information should simply be tagged with an expiration date.[90] All digital data can have metadata attached to it.[91] By adding a metadata tag that sets an expiration point, data could be automatically deleted from a computer's hard drive or server's database at a certain time following its collection. In much the same way as humans forget bits and pieces of information throughout their lives, Mayer-Schöenberger suggests that we reproduce this element of human memory retention and recollection in digital collection systems. His proposal "aims to reintroduce the concept of forgetting over time into our digital realm. [The] goal is to shift the default from retaining forever to deleting after a certain time."[92]

His solution has the merits of being relatively easy to implement because metadata and automated deletion software already exists. Aligning the digital world's retention characteristics with human retention characteristics that would limit the individual's risk of being punished throughout their lives for relatively minor youthful indiscretions, and being less politically disruptive than Lessig's solution because Mayer-Schöenberger's is easily understood by politicians and their constituents. While Mayer-Schöenberger's solution would mitigate some of the concerns over data retention, it would not, as he

---

[90] Mayer-Schöenberger (2007) "Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing," 18. Hereafter referred to as "UV".

[91] Metadata is often used to search data by associating characteristics that extend beyond the data's explicit content, such as songs' publishing and recording dates, the owner of a digital document, or the kind of camera used to take a digital photograph.

[92] Mayer-Schöenberger (2007) "UV," 20.

admits, resolve all or even the majority of privacy concerns in the digital era.[93] It would not limit corporations' ability to transfer information to one another for profit, nor would it prevent the transcription of data from one data source to another, where both actions would effectively undermine the process of forgetting because any data's expiration date would be extended to one that is based on its transcription into new data repositories or formats. For example, if digital pictures taken in public were set to expire in five years, it would be possible to simply alter the picture with the effect that the expiration date would extend five years from the time the alteration was made. While one might be inclined to respond by saying that the intentional extension of expiry dates would be an unlikely situation and, even if it was possible, that reasonable law-abiding people would likely be incapable of or unwilling to subvert law this way, consider what would happen if people's personal digital photos were coded to delete themselves after a space of a few years. Software programs would be written and sold to alter metadata so that photos and documents never deleted themselves. Mayer-Schöenberger's solution, while it appreciates some of the particularities of the human condition, simultaneously fails to appreciate our desire to retain historical artefacts that document our lives and the lives of those who went before us. We have many texts and photographs that are centuries old and that are treasured for their historical and personal value. In an increasingly digitized society, such artefacts would be less and less likely to be available to later generations were this date expiration system implemented. Mayer-Schöenberger's proposal is too coarse. If his proposal is complicated to account

[93] Mayer-Schöenberger (2007) "UV," 22.

for the issues that I have noted, then it will quickly lose its simplicity and, in turn, fall prey to many of the challenges that faced Lessig's proposal. Moreover, while Mayer-Schöenberger's solution might alleviate long-term data retention in personal portfolios, it would not minimize the privacy invasions between the time when the data is collected and deleted. While this might reduce the likelihood of our liberty, autonomy, and speech being persistently inhibited by our youthful indiscretions, citizens would still bear the scars of digital violations long after the data was 'forgotten'.

Neither Lessig's nor Mayer Schöenberger's proposals exist in opposition to my proposed privacy archetype – Lessig's is concerned with informational privacy and Mayer Schöenberger's with long-term data retention. The difficulty is that neither of their proposals is expansive enough to establish norms that would give individuals a democratically legitimated way of retaining control over their digitized personal information nor do they address the complexities of modern data retention. Neither model necessarily mandates that individuals provide their consent before their data is transmitted to third parties, nor do they guarantee individuals the right to texture their dossiers. These models do not impose an openness or transparency on databases and, as a consequence, under these models databases remain closed and secretive so long as they are architecturally coded to meet legitimized law.

In these theorized situations, citizens either accept their relegation to second-order authors of law – authors that outline legal architectures but who do not enunciate their specifics of law – or, they adopt a policy that is out of harmony with how they live. In light of these difficulties, it is apparent that neither one of the two proposed solutions

adequately alleviates the challenges that arise when digitizing information. In light of their respective difficulties and the continuing need to articulate a privacy archetype capable of responding to the challenges that arise in the digital era, I introduce my reciprocal archetype of informational responsibility. Its norms overcome and avoid the deficiencies of past analogue archetypes when they are applied to digital environments while carrying their positive characteristics forward into the digital era.

3 The Reciprocal Archetype of Informational Responsibility

Information held in databases is usually either gathered through individuals directly inputting their data or as a consequence of data being transferred from one database to another. When individuals disclose information it is often for particular purposes – they might want to provide a digital portfolio for a particular service, submit information to gain access to particular services, or disclose information during a session in which they and data collectors are learning about each other. In each of these cases there is at least a presumed element of reciprocity to the exchange – individuals are sharing information based on their assumption that the exchange has benefits. This should not suggest that individuals necessarily exchange or provide information strategically, but that when dealing with corporations or government bodies, they assume that their information will be used for particular ends or purposes. For example, when signing up for a free Google email account, users provide Google Corporation with personal information in return for nearly unlimited email storage space. In this situation, there is arguably a strategic exchange of information taking place. However, when individuals enter search strings into the Google search engine that pertains to personal values, sexual orientations, or

medical concerns, they are not being strategic, though Google Corporation's intentions with the data most certainly are. Very often, there are discrepancies in how individuals and service providers characterize their relationship, but regardless of these differences, both parties must acknowledge that they are in some kind of relationship with one another. In both of the examples involving Google, the corporation has a responsibility to the person who is revealing their personal information – the information must be kept confidential and cannot be used for purposes that extend beyond the agreed reasons for collecting the data.[94] These aspects of the Google – user relationship can be generalized to include all relationships where citizens reveal aspects of themselves to others. As citizens reveal themselves to data collectors, they become increasingly vulnerable to the collection bodies, and this vulnerability demonstrates that trust and the corresponding, implicit, possibilities of harm and/or shame are an intimate part of this relationship. Effectively, because individuals are revealing their identity through their particularities, their data partners are obligated to be sensitive to the trust and subsequent duties and obligations that are involved in these disclosures.

These responsibilities manifest in the obligation of the collecting agencies to hold the information provided to them in at least as much confidence as is outlined in the original agreement between themselves and the people disclosing their information[95]

---

[94] Peter Fleischer, Privacy Officer for Google Corporation, points out that corporations depend on the trust between themselves and their customers, stating "...privacy is about more than legal compliance, it's fundamentally about user trust. Be transparent with your users about your privacy practices. If your users don't trust you, you're out of business." http://peterfleischer.blogspot.com/2007/05/some-rules-of-thumb-for-online-privacy.html

[95] End User License Agreements (EULAs) are currently how individuals consent to corporate use and dissemination of personal information, but the legalese of these documents combined with the prohibitive costs of legal consultation to explicate what is being agreed to in EULAs requires that the

and in the obligations of individuals to be truthful when disclosing information. Based on the information that is revealed, different degrees of secrecy and security must be applied to the information. Collection bodies have long-term responsibilities and obligations to individuals from whom they collect data; instead of personal information acting as information capital that is transferred in much the same way as currency is exchanged when purchasing a candy bar, personal information functions as a way for individuals to access particular services while simultaneously entering into a (potentially long-term) relationship with the data aggregation body for as long as that data is retained. Personal information capital is bound up with the individual's ability to recognize and pursue their life-projects; the information plays a role in guiding the individual's particular public and private attitudes. After this information is disclosed, it does not become any less valuable – revealing one's gender, religion, cultural affiliation, age, hometown, educational background, employment history, or sexual orientation do not make any of these facets of a person's life any less important in their personal development. On the basis of this information's significance, collection bodies ought to limit their use and transmission of individuals' information to ensure that individuals retain their personal dignity.

A core aspect of the relationship between citizens and data collectors is that citizens ought to have some control over the use of their information – just as they can reproach a friend for uttering false statements about their personal lives, they should be able to

---

documents be simplified so that regular consumers can be reasonably expected to understand them. Failing to do so would maintain gross power inequalities between citizens and the data collection agencies that can afford the costs of legal consultation to create the EULAs.

similarly correct data collectors. The control that individuals could exercise in relationships with data collectors might require that individuals receive clear explanations of how data will be used and require that they have the ability to correct and texture their dossiers. Moreover, since individuals enter into a relationship when disclosing their information to any particular collection group, before their information can be transferred to third-parties the individuals ought to be required to opt-into the disclosure and enter the corresponding relationship. The requirement for individuals to opt-in to data transfers would have (at least) a pair of particularly significant effects: (a) it would ensure that collection bodies would clearly disclose their use of individuals' personal information; (b) it would give individuals control of whether third-parties could receive their personal information and make those parties accountable for how that information was used. Thus, if a person provided their personal information to an online lingerie store, before that information could be sold or strategically transferred to another business or governmental body the person would be required to consent to the transfer and, if they did, would enter into a separate informational relationship with the new party with all accompanying rights and duties.

From the discussion of the reciprocal archetype of informational responsibility, we can identify a series of normative characteristics in this archetype:

(1) Data collection cannot be covert or involve coercion – individuals must have a substantive opportunity to refuse to provide their information to other groups.

(2) Data collection must be transparent, insofar as individuals must reasonably expect to understand the terms and conditions of information disclosures.

(3) Individuals must have access to their records and be able to correct falsities.

(4) 'Personal information' must be understood expansively, insofar as it must capture all data shards that could contribute to an individual's digital portfolio.

These norms have the aggregate effect of overcoming many of the challenges encountered in the process of digitization and still allow for the realization of digital networks' positive attributes. By requiring data collection bodies to transparently ask individuals to disclose their personal information and openly reveal who it will be exchanged with, the present covert collection, retention, and use of information to target and discriminate against citizens would decrease, if only because of strategic market logics; if citizens realized that their information was being used to injure them they could appeal to authorities to punish data collectors for the injustices they were causing. Instituting a norm that allows for granular disclosedness of personal information would let citizens share information with their bank without subsequently requiring them to give up their right to limit further access to the information – banks could not require individuals to agree to contracts that necessarily allowed the disclosure of citizens' information. Moreover, the expansiveness of these norms would shield intimate exchanges from publicity – intimate information could be shared according to explicit or tacit agreements between the intimate parties.[96] By broadly shielding digitized personal information, this archetype avoids limiting its purview to confidential, intimate, financial, or other data types. Moreover, by recognizing that

[96] Obviously, the agreements between lovers will differ from those between citizens and their banks. By 'tacit consent,' I am suggesting that revealing pictures, movies, and/or writings that were motivated by a person's love or caring would be expected to remain secret, despite the lack of an explicit agreement.

individuals have relationships with data aggregators, individuals ought to retain the capacity to review and correct the records about them, just as they might correct a friend's mischaracterization of their personal attributes. The ability to correct records, in particular, should be appealing both to the individuals who contribute their data to strategic databases and to those maintaining them – individuals can reduce the likelihood of being pervasively 'tagged' incorrectly across cascading databases, and value of data collectors' databases would increase alongside their records' increased accuracy.

This archetype's pervasive transparency norm would limit individuals' exposure to penalties or accidents following from incorrect information inputs. Moreover, it would alleviate the difficulties arising from regenerative databases. Oftentimes databases are interlinked, where one database holds a superior influence over the other. For example, database A may be a 'master' database, and databases B through K are 'slave' databases that draw information from database A into their own structures. In an environment where individuals do not have to validate their personal information when it is transferred, it is possible for database A to hold incorrect data and disseminate its inaccuracies across the slave databases. Thus, if database A holds incorrect information, it would replicate the errors across databases B through K. If a correction were made to database C the change would be undone as soon as data cascaded from the master to slave databases, re-imposing the error over database C. This exact problem causes individuals significant problems when they attempt to correct credit reports and

criminal records[97] – without an awareness of databases' interrelated structures, individuals are subject to bureaucratic speed to have their data corrected. When a falsely attributed record prevents a single mother from working for months, being told "sorry" for a mischaracterization resulting from a database error is of little consolation, especially if the error caused significant reputational or emotional harm. If individuals must opt-into informational transfers between databases and can validate information being exchanged, databases are less likely to replicate errors because they cannot spontaneously transfer information. The reduction of the number of errors and resulting inconveniences makes databases more valuable for the groups owning them while providing individuals a modicum of control over their disclosed information.

This archetype for digital privacy recognizes the inequalities of power between original information-content owners and those who collect information by requiring citizens to consent to the information transfer. This requirement of consent allows them to prevent the transfers should they desire to. After empowering citizens in this way, collection groups would have to develop detailed outlines for how and why they use the data to assuage individuals' concerns – market logics will lead to clarifications of usage policies because, without such clarifications, citizens will provide their information to the competitors who provide clear, understandable outlines of data use, security measures, and retention policies.

By asserting a shared responsibility for maintaining the privacy of personal information, with the majority of that responsibility falling on the shoulders of collection

[97] Judith Wagner Decew (1997) *IPP*, 150-1.

bodies, there would be an inversion of the current relationship between data collection groups and citizens who disclose personal information. Whereas individuals are currently responsible for investigating who has their personal data and how it is being used before they can attempt to correct inaccuracies or limit uses, this archetype would affirm individuals as critical nodes in information distribution webs – individuals would be empowered, quite simply, to direct the passage of their data from one junction to another. Moreover, this archetype would let markets more effectively target groups and individuals based on who made information available, restricting those who are targeted by market segments to interested participants. This archetype lets me provide Amazon.ca with a great deal of information about me so that they can target new books to my interests, but I can refuse to have Amazon.ca transfer that information to EBay so that it can target me with items or services. To enforce this relationship positive law that draws inspiration from this archetype's norms must be established. These laws would give individuals access to their digital dossiers, allowing them to monitor what information was collected about them and remedy inaccuracies. Moreover, these laws would let citizens renegotiate or exit contracts if the individual becomes reasonably uncomfortable with how the information is being used diverges from the permitted uses stated in the data collection policy/contract.

Ultimately, the reciprocal archetype for informational responsibility can accommodate the challenges facing the intrusion, market, intimacy, and secrecy archetypes while engaging with the current digital landscape. Because of its conservative approach to data sharing, even as the landscape changes by making data

sharing more efficient, individuals could direct how those networks could be used to transmit information. Individuals could retain control over their information regardless of increased efficiencies in transferring and storing data. After citizens can control how their information is shared, they do not have to fear being surveyed secretly– surveillance would require individuals to first opt-in to the observation or recognize themselves as the authors and addressees of a law authorizing the surveillance. Whereas a panoptic-sort environment involves the imposition of unknown and illegitimate categorizations and discriminations, this hidden sorting is made public under this archetype – the wizards responsible for secretly ordering society have their respective curtains pulled aside. When citizens empower themselves to control what is publicly visible and have the definition of personal information extended to the minutiae of information that could be used to develop and assess an individual's digital portfolio, they can expose themselves in digital environments as they determine is appropriate. Consequently, after adopting the reciprocal archetype of informational responsibility, citizens can associate with 'deviant' members of society, express personal opinions that diverge from public norms, and visit places in digital environments without fearing that they will experience illegitimate coercion or shame resulting from unwanted publicity about their choices of expression, association, or digital habitation. As we will see in the next section, this facilitates the continued persistence of political legitimacy in Western nation-states that have been swept up in the tidal wave of digitization.

4 Political Legitimacy in Digitized Environment

The reciprocal archetype of informational responsibility would recognize data-collection groups as being in relationships with citizens and would require these groups to treat citizens' information with respect and to avoid releasing it to other parties without receiving express consent from citizens. This would limit the unwanted publicity of personal information because when providing personal information to receive (or potentially receive) a particular good or service, the data would become a shared 'property' rather than becoming exclusively owned by the data collector. This archetype's norms enable individuals to determine the degree to which they will allow their information be publicized and enable them to participate in digitized ethical-political discourse without having to stunt their discourse out of fear of unauthorized digital surveillance. Moreover, this archetype elevates citizens' interests as the primary guiding factors for determining whether or not their information is transmitted across digital databases – individuals, rather than data collection bodies, would determine what information could be shared – and replaces the present system of opaque unilateral distributions with legitimated, consensual, and transparent transmissions.

Being able to prevent or slow the movement of info-capital has the effect of limiting the illegitimate or overzealous collection and distribution of personal information that flows throughout digital networks. Of course, for this slowing to occur, laws that are guided by the reciprocal archetype of informational privacy's norms would first need to be actualized. Citizens' awareness of how routinely their personal information is distributed would lead them to demand justifications for why data-collectors should be

allowed to maintain a high, unregulated, flow of information, just as citizens have when other private interests have appeared to be working against the public's interests and in opposition to constitutionally enshrined values. These demands would have the effect of requiring information collectors to explain their use of the data and, in the process, would educate the public about digital dossiers and surveillance tools as information aggregators attempt to preserve and legitimize the tools they currently use in their market operations. Citizens could then develop informed arguments for how digital information ought to be transferred, with their discourse revolving around their constitutionally entrenched liberties as well as their particular experiences and values. With an expanded awareness of their digital environment, citizens could work towards envisioning how their constitution's values should be translated into this new environment, values that revolve around the maintenance free speech, due processes under the law, and freedom of association. Citizens, rather than courts or private corporations, could continue to steer the direction of their democratic nation-state if this archetype was adopted to guide the discourse surrounding privacy in digital environments.

In entertaining arguments about a new set of laws to oversee digital interactions, citizens would realize that the relationships they hold with one another and with information aggregators is dramatically different in digital spaces than in analogue environments. Databases threaten to segregate citizens; as citizens are assigned to particular data groups, they are blanketed with a similar series of messages as other

citizens who are associated with that particular data category.[98] This information segregation risks establishing data cocoons, insulating citizens from the wider spectrum of events and actions occurring inside and outside of their locality – certain events or discourse may not be brought to their attention because they do not correlate with the citizens' historical preferences. These cocoons threaten to diminish, and ultimately disintegrate, substantial ranges of citizens' discourse because the shared repertoire of meaning that grounds their ethical-political discourse drops away – issues are not seen as common in a segregated society but as belonging to specific subsets of the population. These cocoons were more challenging to establish subtly in analogue environments because it was not practical (or feasibly possible) to develop the digital era's elaborate digital dossiers and sorting techniques. Without full disclosure concerning how data-groups are established, citizens cannot be certain of the extent that other members affect their collective data streams and, in an environment where it is (relative to analogue environments) inexpensive to establish and reinforce the data cocoons, citizens cannot be certain that they are not persistently experiencing information discrimination.

The reciprocal archetype of informational responsibility is aimed at preserving the discourse that is needed to maintain citizen-solidarity as Habermas envisions it, and it is diametrically opposed to secret impositions of these cocoons. After becoming aware of the possible challenges that might face the nation-state as a result of unmitigated data transfers, citizens can engage in public discourse to establish ethical-political norms that

[98] Cass R. Sunstein (2006) *I:HMMPK*, 97-8.

preserve their right to privacy and, as a result, shield their rights to autonomy, liberty, and secrecy. Born of these norms, citizens can craft laws to affect the architecture and implementation of digital technologies. By approaching technology and law from a normative perspective, the elements of digital technology that relate to digital informational privacy can be democratized – the structure, use, and implementation of digital technologies must conform to the citizenry's democratic will before being made available to the market.

After law shields digital communications from illegitimate oversight, citizens can use digital communications to effectively generate citizen-solidarity. No longer concerned that their conversations will be disclosed at a later time to injure their reputations, unless they first permit such disclosures, members of the nation-state can freely participate in online associations and communications. They can expose themselves to ideas, arguments, and values that they were previously unaware of and that could subsequently alter their own perspectives, values, and arguments in the process of realizing the nation-state's increasing plurality. Moreover, given that citizens are increasingly distributed across vast geographic distances, establishing clear national data privacy laws allows for open communications between distant citizens and could even be extended beyond traditionally understood state borders. It is possible that international arrangements could lead friendly foreign nations to develop 'friendly foreign alien' privacy policies, where foreign aliens are protected by their national

privacy laws when in friendly nations.[99] As with all democratic law, the digital privacy laws born of ethical-political discussions could be modified over time as new participants enter the discourse, which would ensure that the laws could be refined and extended to respond to, as yet undiscovered, privacy concerns and social injustices. Further, given the transmission rate of digital communications, new participants could (theoretically) collaborate with other citizens using near-instantaneous digital transmissions to reshape public attitudes towards privacy when unforeseen challenges to privacy rights arise. The speed of digital networks and the ability of private citizens to monitor for and report on their illegitimate use to other citizens *en masse* would also facilitate rapid legal responses if information collection groups were discovered breaching privacy laws. Ultimately, the reciprocal archetype of informational responsibility offers citizens a way of developing privacy laws that would correlate their ethical-political discourse concerning digital communicative privacy with the nation-state's laws and enable them to rapidly direct the nation-state and its coercive force towards those found to be violating laws surrounding information aggregation and dissemination. This would, as a result of safeguarding free speech, preserve discursively generated citizen-solidarity.

5 From Digital Privacy to Regenerating the Lifeworld

The Habermasian lifeworld is a domain of discourse, wherein individuals recognize the plurality of values that found theirs and others' life-projects. It is a space intended

[99] This is meant expansively, insofar as it can apply when physically in different geographies and in foreign-controlled areas of cyberspace.

for mutual understanding and is non-competitive insofar as discursive participants are interested in arriving at consensual agreements rather than with winning arguments. When communications are negatively structured by fear of shame or coercion individuals strategically assert limited, particular, aspects of their discourse to try to protect themselves from persecution. After their communicative mediums are secured from illegitimate oversight, these participants can speak with one another without needing to strategize their conversations, opening them to the full possible horizons of the discourse. Digital communications, as they actually exist now, are largely subject to invasion and, as such, are an unsuitable medium for free and open communication. Adopting the reciprocal archetype of informational responsibility and using its norms to guide subsequent digital laws to stem the dissemination of personal information would provide a way of overcoming the digital era's colonization of the lifeworld.

Personal information is currently traded for profit – data aggregators maximize their investments by developing the most comprehensive and unique databases along with powerful search algorithms to target consumers with spectacular accuracy. In limiting the flow of information by requiring individuals to consent to its flow, citizens could again communicate without fearing that their conversations or personal information will be secretively sucked into systemic domains and used to possibly discriminate against or embarrass them in the future. While it is true that nation-states' laws are limited to national jurisdictions and thus that data collected by companies in other nations is subject to different laws, large nation-states can set rules for trade that punish or entirely prevent foreign companies from participating in the nation's market unless they

adopt or respect the privacy rights that the nation-state guarantees. Additionally, nation-states can require that local internet providers encrypt personal information so that only data collectors who comply with the nation-state's data protection laws can decrypt individuals' personal information, which would cause data collectors to accommodate that nation-state's laws and data architecture on the basis of market logics. These steps would not entirely curtail digital privacy breaches, but the likelihood of breaches would be mitigated and offenders would be subject to punishment.

The European Union's data protection laws in particular have demonstrated the ability of localized geographic areas to significantly affect how data protection and confidentiality are honoured around the world. In 1995 the European Union instituted its initial data privacy laws, which have subsequently led to the creation of the Safe Harbour Provisions that businesses must obey to legally hold information about EU citizens. If a corporation is found holding information on EU citizens in violation of Safe Harbour Provisions, the corporation can be subjected to trade restrictions and legal challenges from the EU, as well as by nation-states that have imposed legal obligations on 'their' international corporations to honour the Safe Harbour Provisions. Consequently, while the United States of America might not have created the Safe Harbour Provisions and while American corporations are typically only responsive to American law, all American data aggregation groups must honour these provisions or be subject to legal punishments directed by the American government. The United States government is compelled to apply these punishments because, if it does not, its exports to the European Union could be limited or subject to tariffs – international market

pressures are responsible for long-term compliance to Safe Harbour Provisions. While the EU is in some ways a unique case, insofar as its economic mass provides it with a great deal of international influence, its unique situation should not lead others to abandon the hope of protecting their own constitutional rights. While a similar degree of influence and compliance would be less likely were Chad to impose provisions similar to the EU's, Chad could possibly work with the EU to have Safe Harbour extend beyond just EU citizens.

Extending privacy laws across state borders aligns with the possibility of establishing a post-national attitude. As individuals become aware that their actions are not constrained to their localities as in prior centuries, they can become increasingly open to shared international collaboration. The ability to communicate with individuals in other areas of the world and to learn about common issues that stretch across localities can lead to the realization that humans possess a common moral value. No one should be forced to experience sexual violence in order to secure the basic necessities for life, for example. As the nation-state's citizens realize the interrelations between domestic policies and foreign consequences on specific others, citizens can have their notions of who should be protected by and from national actions extended to include those foreign to the nation-state. These realizations would necessitate extending legal norms beyond national borders and actualizing them in a manner that is sensitive to all who are affected by the nation-state's actions. While I do not claim here that a post-national political body would develop necessarily or soon after adopting the reciprocal archetype of informational responsibility, it would be helpful in establishing a zone of

communicative action within which individuals could develop and play with these ideas in their legally defined localities. As citizens learn of others' experiences and subsequently evaluate the nation-state's role in those experiences, they could reward politicians who take the courageous steps to shift the domestic political boundaries to become more sensitive to those in foreign parts of the world. Politicians who make moves to extend legally binding discourse beyond the nation-state to address citizens' concerns for humans in other nations would need to be rewarded by citizens, which could manifest in citizens re-electing them. Such rewards would provide politicians with a strategic reason to continue extending the domestic to the foreign. As politics, a systemic domain, is realigned towards securing the lifeworld's zone of discourse, it could secure other communities' values on the basis of citizens' recognition that both those within and outside the nation-state deserve similar basic dignities. The rebalancing of the lifeworld and systems would return citizens to the role of guiding politics instead of watching as market logics drive political actions. This said, before citizens can reassume the role of guiding politics, they must be able to freely communicate with one another, which requires the imposition of a new digital privacy archetype. After adopting the reciprocal archetype of informational responsibility, laws that effectively translate constitutional values onto digital environments and that safeguard communicative rights can be established. This would allow citizens to maintain their discursively generated solidarity, and thus maintain the integrity of the nation-state. Simultaneously, the scale of the lifeworld and systemic domains would be rebalanced.

CONCLUSION

Over the course of this thesis, I have asserted that there is a need to maintain communicative privacy if citizens are to generate solidarity and establish norms that adapt to their changing and technological environments. The groundwork for this argument was established while examining the role of discourse in Habermas' political theory. Openness of speech is fundamental to establishing a constitution that citizens recognize themselves as being the authors of and is critical to developing and maintaining citizen-solidarity. The nation-state's constitution lets citizens develop common understandings about the ethical-political narrative based on their shared public normative framework, a framework that persists across the plurality of values and life-projects in the nation-state. This common ethical-political narrative is structured by citizens' constitutionally recognized rights, which operate as a central validating force in discourse.

In the process of examining the constitution and its role in developing common ethical-political narratives, it became apparent that we needed to consider the challenges towards free speech and association in digital environments. While informational privacy has persistently been recognized as an important issue and led to analogue privacy architectures being developed to guide lawmaking and stem privacy breaches, past archetypes cannot effectively be translated into the digitized environment to adequately safeguard citizens privacy. In light of this difficulty, and the subsequent threat to discursively generated citizen-solidarity, the reciprocal archetype of information responsibility was proposed to overcome these deficiencies and

safeguard citizens' right to private, free speech. This archetype addresses the challenges that have arisen with the growing prevalence of digital technologies and the decreased costs of transferring, copying, and combing through data and the possibility of nigh perpetual data retention. It focuses on empowering citizens by concentrating on the responsibilities and obligations that develop when sharing information with others; there must be a transition from the present stance that individuals give up all rights to their information after disclosing it to a stance where individuals retain some control over its disclosure. This shift offers a way to open digital spaces as places where individuals can communicate without fearing illegitimate surveillance while letting them pursue their life-projects and develop discursively founded solidarity.

In focussing on the national-scale, I have not attended to many of the wider consequences of this archetype nor have I significantly evaluated how influential it might be in contributing towards creating cosmopolitan or supranational attitudes or modes of political association. While I have tentatively begun to examine why and how national laws might be extended beyond a nation's traditionally held territorial borders, my account has not engaged with the question of whether or not my archetype could lead to international privacy laws based on legitimizing, rather than market, conditions. I have also not evaluated whether or not it is necessary to establish a reason for obedience to international law beyond strategic market reasons. Finally, while I have focused on digital technologies and digital privacy, in the process I have not addressed the matter of the 'digital divide', or the distinction between nations that are largely connected to the Internet and those who lack even widespread national telephone

networks or dependable postal systems. Mark Poster has noted that during the age of print an exclusive group of people was responsible for establishing the nation's composition and, while the nation-state's composition has changed over the centuries, its contemporary principles and attitudes resemble its historical antecedents. In writing a new set of norms and developing any new political apparatus based on the possibilities of a digitally networked society, we run the risk of developing an 'inclusive' metric that is insensitive to the substantive exclusion of the majority of the world's population. In light of this possible insensitivity digitization, far from leading to the enfranchisement of the least well off in society, may actually be forming a new fortress of the powerful that excludes all who cannot scale or penetrate the digital era's silicon walls.

BIBLIOGRAPHY

Balibar, Étienne, and Daniel Hahn. *Politics and the Other Scene*. New York: Verso US, 2002.

Brock, Gillian, and Harry Brighouse, Ed. *The Political Philosophy*. New York: Cambridge University Press, 2006.

De Greiff, Pablo. "Habermas on Nationalism and Cosmopolitanism," *Ratio Juris*, Vol. 15, No. 4, pp 418-38.

Finlayson, James Gordon. *Habermas: A Very Short Introduction*. New York: Oxford University Press, 2005.

Gandy Jr., Oscar H. "It's Discrimination, Stupid!" *Resisting the Virtual Life: The Culture and Politics of Information*. San Francisco: City Light Books, 1995.

Guerrina, Robert. *Europe: History, Ideas, Ideologies*. New York: Oxford University Press Inc., 2002.

Goldsmith, Jack and Tim Wu. *Who Controls the Internet?: Illusions of a Borderless World*. Toronto: Oxford University Press, 2006.

Habermas, Jürgen. *Moral Consciousness and Communicative Action*. Cambridge, Massachusetts: The MIT Press, 1990.

- *The Inclusion of the_Other: Studies on Political Theory*. Ed C. Cronin and P. De Greiff. Cambridge, Massachusetts: The MIT Press, 1998.
- "Lecture Two," *The Philosophical Discourse of Modernity: Twelve Lectures*. Trans. Fredrick g. Lawrence. Cambridge, Massachusetts: The MIT Press, 1990 (Pbk).
- *The Postnational Constellation*. Ed. and Trans. Max Pensky. Cambridge, Massachusetts: The MIT Press, 2001.
- *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Ed. and Trans. Thomas Burger and Frederick Lawrence. Cambridge, Massachusetts: The MIT Press, 1991 (Pbk.)

Hardt, Michael and Antonio Negri. *Empire*. Cambridge, Massachusetts: Harvard University Press, 2000.

Hegel, G.W.F. *Elements of the Philosophy of Right*. Ed. Allen W. Wood. New York: Cambridge University Press, 1991.

Held, David, Anthony McGrew, David Goldblatt, and Jonathan Perraton. *Global Transformations: Politics, Economics, and Culture*. Stanford: Stanford University Press, 1999.

Kant, Immanuel. *Groundwork of the Metaphysic of Morals*. Trans. H.J. Paton. New York: Harper and Row Publishers, 1964.

- "On the Common Saying: 'This May be True in Theory, but it does not Apply in Practice." Ed. H.S. Reiss. *Political Writings*. New York: Cambridge University Press, 2002.
- "Perpetual Peace: A Sketch." Ed. H.S. Reiss. *Political Writings*. New York: Cambridge University Press, 2002.
- "Introduction." Ed. H.S. Reiss. *Political Writings*. New York: Cambridge University Press, 2002.

Kymlicka, Will. *Multicultural Citizenship*. Toronto: Oxford University Press, 1995.

Laing, R.D. *The Politics of Experience*. New York: Ballantine Books: 1967.

- *The Politics of the Family*. Concord: House of Anasai Press Limited, 1993.

Lessig, Lawrence. *Code Version 2.0*. New York: Basic Books, 2006.

Locke, John. *Why We Don't Talk To Each Other Anymore : The De-Voicing of Society.* New York, NY: Simon & Schuster, 1999.

MacKinnon, Catharine. *Towards a Feminist Theory of State*. Cambridge: Harvard University Press, 1989.

Mayer-Schöenberger, Viktor. "Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing," *Harvard University Faculty Research Working Papers Series*, April 2007.

McCarthy, Thomas. "On Reconciling National Diversity and Cosmopolitan Unity," *Alternative Modernities*, Durham: Duke University Press, 2001. pp. 197-235.

Mosco, Vincent. *The Digital Sublime: Myth, Power, and Cyberspace*. Cambridge, Massachusetts: The MIT Press, 2004.

Müller, Jan-Werner. *Constitutional Patriotism*. Princeton: Princeton University Press, 2007.

Payrow Shabani, Omid. *Democracy, Power, and Legitimacy: The Critical Theory of Jürgen Habermas*. Toronto: University of Toronto Press Incorporated, 2003.

- "Constitutional patriotism as a model of postnational political association: The case of the EU," *Philosophy and Social Criticism*, vol. 32, no. 6, pp 699-718.
- "Cosmopolitan Justice and Immigration: A Critical Theory Perspective," *European Journal of Social Theory*, Vol. 10, No. 1, pp 87-98.

Poster, Mark. "National Identities and Communications Technologies," *Information Society*, Vol. 15, No. 4, pp 235-240.

Ontario. Information and Privacy Commissioner. An Internet Privacy Primer: Assume Nothing. Toronto: Office of the Information and Privacy Commissioner of Ontario, 2001.

Russon, John. *Human Experience: Philosophy, Neurosis and the Elements of Everyday Life*. Albany, NY: State University of New York Press, 2003.

Schmitt, Carl. *Legality and Legitimacy*. Trans and Ed. by John P. McCormick. Durham: Duke University Press, 2004.

Schiller, Herbert I. "The Global Information Highway: Project for an Ungovernable World." *Resisting the Virtual Life: The Culture and Politics of Information*. Ed. James Brook and Iain A. Boal. San Francisco: City Lights, 1995.

Schnapper, Dominique. "The European debate on citizenship," *Daedalus*, Vol. 126, No. 3, pp 199-222.

Single, Ryan. "Whistle-Blower Outs NSA Spy Room," *Wired*. Published July 4, 2006. URL accessed September 11, 2006. http://www.wired.com/science/discoveries/news/2006/04/70619

Solove, Daniel J. *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press, 2004.

Sunstein, Cass R. *Infotopia: How Many Minds Produce Knowledge*. Toronto: Oxford University Press, Inc., 2006.

von Berstoff, Jochen. "Democratic Global Internet Regulation? Governance Networks, International Law and the Shadow of Hegemony," *European Law Journal*, Vol. 9, No. 4, pp. 511-526.

Wagner Decew, Judith. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithica, New York: Cornell University Press, 1997.

Warshak vs. United States, No. 06-4092 (6th Cir. June 18, 2007) Martin, K. (20 pages) available at http://w2.eff.org/legal/cases/warshak_v_usa/6th_circuit_decision_upholding_injunction.pdf

Wellmer, Albrecht. "Ethics and Dialogue: Elements of Moral Judgement in Kant and Discourse Ethics." *The Persistence of Modernity*. Trans. David Midgley. Cambridge, Massachusetts: The MIT Press, 1991.

White, Stephen K., ed. *The Cambridge Guide to Habermas*. Cambridge: Cambridge University Press, 1995.

- Baynes, Kenneth. "Democracy and the *Rechtsstaat*: Habermas' *Faktizität und Geltung*."

- Chambers, Simone. "Discourses and democratic practices."
- Moon, Donald J. "Practical Discourse and Communicative Ethics."

Winnicott, Donald. *The Muturational Processes and the Facilitating Environment: Studies in the Theory of Emotional Development*. New York: International Universities Press, 1965.