

Re-reading Westin

*Lisa M. Austin**

*Alan Westin's work *Privacy and Freedom* remains foundational to the field of privacy, and Westin is frequently cited for his definition of privacy as control over personal information. However, Westin's full definition of privacy is much more complex than this statement, describing four states of privacy (solitude, intimacy, anonymity, and reserve) that one achieves through physical or psychological means. The "claim" of privacy involves negotiating a balance between a desire for disclosure and social participation and a desire for withdrawal into one of the "states" of privacy. Influencing this adjustment process are social norms (and surveillance to enforce social norms), environmental conditions, and the curiosity of others. In this Article, I draw upon this complexity in order to reread Westin's definition of privacy as a claim of control over personal information and use this rereading to understand how the law should protect and promote privacy in the twenty-first century. I argue that the law should focus on securing meaningful privacy choices rather than on individual control over personal information. Meaningful choice requires that our informational infrastructure, and the social practices that it enables, make states of privacy available for choice along with the means of attaining them. To enable such meaningful individual choice, we need to shift our attention from a focus on individuals to a more systemic focus on our public norms and built infrastructure. Otherwise we risk protecting a narrow understanding of individual control, while ignoring a more general and systematic erosion of privacy.*

* Professor and Chair in Law and Technology, University of Toronto Faculty of Law. This article benefited greatly from being presented at the Cegla Conference on The Problem of Theorizing Privacy (TAU January 2018). I would like to thank my commentator, Talia Fisher, the other participants, and the editors of this volume for their many helpful comments on an earlier version of this work. Cite as: Lisa M. Austin, *Re-Reading Westin*, 20 THEORETICAL INQUIRIES L. 53 (2019).

INTRODUCTION

Alan Westin's work *Privacy and Freedom* remains foundational to the field of privacy, and Westin is frequently cited for his definition of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."¹ This definition of privacy as control over personal information has deeply influenced the development of data protection law and its underlying Fair Information Practice Principles (FIPPs). However, Westin's full definition of privacy is much more complex than this statement, and the text that defends his full definition is very rich. In addition to defining privacy as a claim, Westin also describes four states of privacy (solitude, intimacy, anonymity, and reserve) that one achieves through physical or psychological means. The "claim" of privacy involves negotiating a balance between a desire for disclosure and social participation and a desire for withdrawal into one of the "states" of privacy. Influencing this adjustment process are social norms (and surveillance to enforce social norms), environmental conditions, and the curiosity of others. In this Article, I draw upon this rich context in order to reread Westin's definition of privacy as a claim of control over personal information and use this rereading to understand how the law should protect and promote privacy in the twenty-first century. I argue that the law should focus on securing meaningful privacy choices rather than on individual control over personal information. Meaningful choice requires that our informational infrastructure, and the social practices that it enables, make states of privacy available for choice along with the means of attaining them. To enable such meaningful individual choice, we need to shift our attention from a focus on individuals to a more systemic focus on our public norms and built infrastructure. Otherwise we risk protecting a narrow understanding of individual control while ignoring a more general and systematic erosion of privacy.

Westin wrote *Privacy and Freedom* in the 1960s, in response to public alarm and distress over "a revolution in the techniques by which public and private authorities can conduct scientific surveillance over the individual."² He saw his task as not providing "further ringing denunciations" but as opening a discussion of what could be done.³ The new challenges of surveillance are different from those that motivated Westin's work. The current revolution that must be accounted for is the digital revolution that is creating an unprecedented

1 ALAN WESTIN, *PRIVACY AND FREEDOM* 5 (1967) (This book was out of print for years. All references are to the 2015 Ig Publishing reprint).

2 *Id.* at 1.

3 *Id.* at 1-2.

infrastructure of surveillance. Digital platforms and information intermediaries increasingly dominate our online existence, enabling various forms of information collection. Sensors, cameras, GPS, the internet-of-things, and their bundling into “smart city” initiatives increasingly add an informational dimension to our navigation of the physical world. This data dimension that characterizes our “onlife” world doesn’t just provide an informational map, but also shapes the ways in which we interact with one another and increasingly involves intelligent systems and automated agents.⁴ Moreover, this dimension is largely being built by the private sector in pursuit of new data-driven business models.

My argument is that addressing this infrastructure of surveillance requires rereading Westin to shift away from an emphasis on individual control and instead focus on meaningful choice. Two analogies are helpful in understanding what is at stake in this shift.

Imagine living in an urban neighborhood with only three small grocery stores within walking distance and no access to other modes of transportation by which you could travel to another neighborhood. In that environment, you could have a variety of choices in relation to your food — choices within each store and choices between the stores. But suppose that none of those stores carried fresh fruits or vegetables. Geographers and public health scholars refer to such areas as “food deserts.”⁵ The fact that fresh fruits and vegetables are not *available* as a choice does not mean that your actual food choices are not your own, it just means that the environment within which you choose is not ideal because it does not offer *healthy* choices. We understand the failings of such environments through reference to ideas of healthy food and the need to be able to choose healthy food as important to individual wellbeing and public health. We would misunderstand the problem if instead of seeking to secure access to fresh fruits and vegetables, we campaigned for better nutritional labels for the existing food choices, on the theory that the problem is that people do not understand the choices they are making. To return to the privacy context, focusing on individual control over personal information leads to a strong emphasis on issues like informed consent, which is a bit like arguing about nutritional labels in the middle of a food desert. Like the need for healthy food choices, individuals need meaningful privacy choices. Understanding what this means requires a richer normative discussion of the nature and value of privacy to individuals, and to society, than simply appealing to individual control.

4 MIREILLE HILDEBRANDT, *SMART TECHNOLOGIES AND THE END(S) OF LAW* (2015).

5 Steven Cummins & Sally Macintyre, “*Food Deserts*” – *Evidence and Assumption in Health Policy Making*, 325 *BRIT. MED. J.* 436 (2002).

Imagine now the different ways we might regulate driving. A private law model might use tools like tort law to regulate dangerous driving — for example, drivers who negligently cause accidents would pay damages to the victims, and the prospect of this would create incentives for everyone to drive with due care. But many liberal democracies have embraced a more public law idea of regulating driving through things like the public enforcement of speed limits. I do not wrong anyone when I speed, but my behavior is risky in relation to safety and we publicly regulate this risk in order to reduce it. Other risks associated with the infrastructure of driving (safe roads, safe cars) are also heavily regulated. In such a publicly regulated context, individuals still choose what to drive, where to drive, how often, etc., but they do so within an environment meant to promote their individual wellbeing and autonomy as well as the general public interest. To return again to the privacy context, focusing too strongly on individual control places emphasis on the question whether the actions of others have violated individual control over personal information rather than whether the environment sustains choices that promote our autonomy and wellbeing. Like our shift towards regulating risk in relation to driving, we could also shift to regulating risk in relation to information practices and the infrastructure that sustains these practices. As in the case of driving, we can regulate risky behavior before it crystalizes into an instance of individual harm or a violation of individual rights. However, understanding this question of risk and infrastructure requires a shift away from focusing on particular informational interactions between individuals and others and taking a more systemic view of the informational environment in order to ask whether it generally supports privacy. This is partly empirical, but it is normative as well, for we cannot assess the adequacy of the environment without understanding the nature and value of privacy to individuals, and to society more generally.

The central claim of this Article is that although privacy law needs to move beyond a narrow focus on individual control over personal information, we need not jettison Westin in order to do so. *Privacy and Freedom* offers us many resources to understand the relationship between individual control and a broader set of normative concerns about the nature and value of privacy.

The first half of this argument outlines Westin's view in detail. In Part I of the Article I discuss the role of choice and control in theories of privacy and show that for Westin the individual chooses either a state of privacy or social disclosure. For individual choices to be meaningful, it must be possible to choose a state of privacy. Part II outlines how Westin understands the states of privacy. An individual withdraws to a state of privacy (solitude, intimacy, anonymity, or reserve) when that individual withdraws from observation or identification, or limits disclosures of personal information. States of privacy

and the means to achieve them are highly dependent on our environment, both physical and social, and because of this will vary according to our social and political cultures. Part III outlines how environmental factors and social and cultural norms affect how an individual engages in the balancing exercise involved in choosing social withdrawal over social disclosure, and how the *social* balance of privacy — the general balance between privacy and surveillance within a society — affects the availability of states of privacy to be chosen. Understanding whether individuals have meaningful choices ultimately requires a normative inquiry into the value of privacy and its place within the broader universe of public norms. As outlined in Part IV, Westin’s discussion of the functions of privacy provide a basis for this inquiry, although it is underdeveloped. For Westin, states of privacy insulate individuals from the pressure of social norms associated with various social roles and relationships, which is required for the development of individuality, emotional health, and the maintenance of relationships. These functions connect with a variety of broader social and political norms and help us evaluate, in a more systematic way, whether the choices available to individuals are adequate in relation to these public values.

The second half of the Article uses this rereading of Westin to analyze our existing legal models and emerging challenges. Part V shows how existing legal models like tort law and data protection law rely upon social norms that can shift in light of new information practices towards supporting information disclosure rather than states of privacy. I argue that we need to ensure that the private sector builds an infrastructure that supports meaningful choices with respect to states of privacy. This requires our legal models to incorporate a stronger systematic and normative account of the relationship between privacy interests, business interests, and broader public norms. Part VI takes up the question of the limits of this rereading of Westin in light of emerging data practices and argues that we need to ultimately move beyond Westin’s framework in order to address issues like algorithmic fairness.

I. PRIVACY AND CHOICE

Westin’s definition of privacy as a claim of control over personal information is popular because it captures a broadly held intuition about the relationship between privacy and choice. For many, it is intuitively difficult to make sense of the idea of privacy without incorporating some aspect of choice. As Charles Fried argues, “To refer for instance to the privacy of a lonely man on a desert island would be to engage in irony. The person who enjoys privacy is able to

grant or deny access to others.”⁶ Similarly, Beate Rössler has noted that the individual who falls into a crevice is alone and inaccessible, but few would say that she enjoys privacy.⁷

There are several ambiguities regarding privacy operating in these claims. The first is that although privacy is often listed alongside other interests one might claim a right to — like bodily integrity — it is quite different. One always has an interest in bodily integrity, but in relation to privacy both too little *and* too much privacy is seen as problematic. It is not just that too much privacy thwarts the interests of other people, or the state, but that it is problematic for the individual who experiences it. The *individual* interest in privacy involves seeking the right balance between too much and too little. This shifts attention to individual choice in seeking that balance, rather than having it imposed, and is the reason why so many definitions of privacy build on some aspect of control, choice, or consent.

But this leads to another ambiguity. Privacy as a claim of individual control suggests that we are exercising our right to privacy when we choose to *share* information with another: so long as I determine for myself what to communicate, how, and to whom, then there is no violation of privacy. A violation of privacy is a violation of my claim to control information about myself. Yet this has seemed wrong to many critics, who argue that in disclosing information individuals are choosing, but they are choosing to give up privacy. Or, to take Rössler’s crevice example, why do we not say that the person experiences privacy but has not chosen it and, in those circumstances, does not value it, rather than that they have privacy? But to understand the privacy that is to be given up, or that is to be experienced without being chosen, we need a definition of privacy that is independent of ideas of choice.

Despite the fact that Westin is associated with control-based accounts of privacy, his account actually displays these ambiguities regarding choice. This is Westin’s full definition:

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve. The individual’s desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually

6 Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968).

7 BEATE RÖSSLER, *THE VALUE OF PRIVACY* (2005).

engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives. The individual does so in the face of pressures from the curiosity of others and from the processes of surveillance that every society sets in order to enforce its social norms.⁸

We can see from this that, after stating that privacy is a claim of control, Westin goes on to write that privacy involves voluntary social withdrawal, not disclosure, and associates this withdrawal with states of privacy.

Westin understands privacy *both* in terms of a claim of control and in terms of the experience of a state or condition. Westin's full definition of privacy tries to put together the idea of privacy as a claim with the idea of privacy as a state and relate it to the need for seeking a balance between too much and too little privacy through the "adjustment process" that an individual engages in. When we make a *claim* of privacy, what we claim is that it is up to us to choose the balance between privacy and disclosure. But what we choose when we choose privacy is a *state* of privacy.

What this points to is not the irrelevance of choice to our understanding of privacy but the importance of understanding *meaningful* choice. The choice is up to the individual, but there must be the possibility of choosing a state of privacy or the individual will not actually experience privacy.

II. STATES OF PRIVACY

If we are concerned about meaningful choice, then we need to attend to what it means to be able to choose a state of privacy. As detailed below, Westin outlines four basic states of privacy. Although these all involve forms of withdrawal from society, I argue that they are also deeply social. As Valerie Steeves has argued, Westin's definition has many social elements that are often overlooked.⁹ Westin also indicates that an individual achieves this social withdrawal through "physical or psychological means." I will elaborate upon this and outline how the availability of these means is highly dependent on our social and physical environment.

Westin outlines four states of privacy: solitude, intimacy, anonymity, and reserve. Solitude and intimacy both involve freedom from the observation of

8 WESTIN, *supra* note 1, at 5-6.

9 See Valerie Steeves, *Reclaiming the Social Value of Privacy*, in LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED WORLD 191 (Ian Kerr, Valerie Steeves & Carole Lucock eds., 2009).

others, and differ in whether the state of privacy involves the individual alone or within a small group. Anonymity involves freedom from being identified by others. Reserve is about freedom from disclosing information about yourself to others. What connects these states so that we might say they are states of *privacy*? For Westin, these are all examples of social withdrawal, which is contrasted with social disclosure. An individual withdraws to a state of privacy when that individual withdraws from observation or identification, or limits disclosures of personal information.

This description of the states of privacy is similar to Ruth Gavison's account of privacy as a state of limited access where "perfect" privacy is defined as when an individual "is completely inaccessible to others."¹⁰ Gavison defines three states of inaccessibility which closely track Westin's: secrecy (inaccessibility in terms of knowledge), anonymity (inaccessibility in terms of attention), and solitude (physical inaccessibility). But it is important to see that for Westin social withdrawal is not an issue of either access or amount. For Westin, the states of privacy are about information. We choose a state of privacy when we choose to not share information about ourselves, either through shielding ourselves from observation (solitude and intimacy), shielding ourselves from identification (anonymity), or shielding ourselves from disclosure (reserve). The social withdrawal involved in states of privacy is about limiting information, not access. But the privacy loss involved in sharing information is also not an idea of *amount* of information, where sharing information with ten people involves giving up more privacy than sharing information with one person, or sharing one hundred pages of personal information involves giving up more privacy than sharing ten. What Westin shows is that the issue is not about the quantitative nature of access to information, but about *who* has access to this information and the nature of their relationship with us.

The distinction between these two ways of understanding states of privacy is clearest in Gavison's and Westin's different accounts of anonymity. For Gavison, a violation of anonymity involves bringing attention to an individual, and becoming an object of attention involves a loss of privacy.¹¹ Westin's account of anonymity is inherently social. He refers to Simmel's understanding of the "phenomenon of the stranger" in order to explain that anonymity is not freedom from attention but freedom from identification. He argues:

In this aspect of anonymity the individual can express himself freely because he knows the stranger will not continue in his life and that, although the stranger will not continue in his life and that, although

10 Ruth Gavison, *Privacy and the Limits of the Law*, 89 *YALE L.J.* 421, 428 (1980).

11 *Id.* at 432.

the stranger may give an objective response to the questions put to him, he is able to exert no authority or restraint over the individual.¹²

Anonymity is a form of social withdrawal that allows people to be in public with others, but at the same time not have to conform to the social norms that accompany the roles they might play in other parts of their lives. Therefore, it is not the number of people you withdraw from but *who* you withdraw from, and their relationship to you, that is important.

This difference in respect of “amount” vs. “who” can also explain why Gavison names secrecy as a state of privacy, while Westin instead names reserve. Both involve limiting disclosure of information about oneself, but secrecy involves an idea of quantity (how many people know this information) whereas reserve is deeply intersubjective. As Westin describes it:

Reserve, the fourth and most subtle state of privacy, is the creation of a psychological barrier against unwanted intrusion; this occurs when the individual’s need to limit communication about himself is protected by the willing discretion of those surrounding him. ... The manner in which individuals claim reserve and the extent to which it is respected or disregarded by others is at the heart of securing meaningful privacy in the crowded, organization-dominated settings of modern industrial society and urban life, and varies considerably from culture to culture.¹³

With reserve the issue is not keeping information secret but limiting communication of self to others in different ways — we can be known in some ways to the people with whom we interact, and be observed by them, but still withhold some aspects of our self. My large circle of friends might know something about me (so it is not a secret), but I still might want to hold back this information from my much smaller circle of work colleagues. The number of people to whom one discloses is not the issue; rather, it is the *who* to whom one discloses, and one’s relationship to them. Moreover, reserve requires the active participation of others — through their “willing discretion.” There are many forms of tact and discretion that involve people pretending not to see what they saw, or not mentioning what they know, for the sake of maintaining a particular relationship.

Westin points out that the means through which we enter a state of privacy are either physical or psychological. If we want individuals to have the possibility of choosing to be in a state of privacy, then we need to ensure that they have the means to do so. If we try to unpack what this might entail, what

12 WESTIN, *supra* note 1, at 34.

13 *Id.* at 35.

we find is that states of privacy and the means to achieve them are highly dependent on our environment, both physical and social.

Consider the state of solitude, which for Westin is a state in which one experiences freedom from the observation of others. It is difficult to choose solitude in an environment where there are no places where an individual can go and be free from observation, whether this is to a room where one can close the door, a building where one can keep others out, or a natural area where one is not likely to meet others. Intimacy is also a form of seclusion, but it involves the seclusion of a group from others in order to facilitate the kind of frank disclosure that is part of important relationships. It is traditionally protected through places where one might go to be away from others. Anonymity, which involves freedom from identification, also depends upon the choices available in one's environment. Urban life makes anonymity in public easier than small town life, because of the size of the population and lower likelihood that the people you interact with while on public transit or walking through a mall are people who will know your identity. We can remain anonymous in our commercial transactions if we can use cash rather than forms of payment, like credit cards, that are intrinsically connected to our identity.

But whether these options are available in one's physical environment is connected to social norms in multiple ways. If a culture values solitude, then its built environment will likely reflect this, with more doors and separate rooms than open spaces, for example. Sometimes the built environment reflects other choices and constraints, and this too will have an effect on social norms. For example, if one's physical environment is crowded, then it might be that individuals withdraw in different ways. As Westin argues, "[t]he English accomplish with reserve what Germans require doors, walls, and trespass rules to enforce."¹⁴

Social norms are central to states of privacy like reserve. Reserve is created through practices of "psychological distance" that are deeply intersubjective. It is used in close relationships to create forms of mental distance that can be important to those particular relationships. Westin argues that it is also used in crowded groups and public settings where

a complex but well-understood etiquette of privacy is part of our social scenario. Bates remarked that 'we request or recognize withdrawal into privacy in facial expressions, bodily gestures, conventions like changing the subject, and by exchanging meaning in ways which exclude others present, such as private words, jokes, winks, and grimaces.' We learn to ignore people and to be ignored by them as a way of achieving

14 *Id.* at 32.

privacy in subways, on streets, and in the ‘non-presence’ of servants or children. There are also social conventions within various sub-groups in the population establishing fairly clearly the proper and improper matters for discussion among intimates, workmates, persons on a bus, and other groups.¹⁵

Reserve is not just an individual achievement, but requires that others follow complex social norms of tact and discretion. Instead of physical walls protecting an individual from observation, reserve is constructed intersubjectively through norms of social interaction.

The influence of social norms on states of privacy also indicates that although these states can be described in general terms, their contours will vary depending on differences in social and legal/political culture. Westin writes at length of different “sensory cultures” that affect how individuals “relate to one another in space, in matters ranging from their concepts of architecture and furniture arrangement to their setting of social distance in interpersonal contact.”¹⁶

This discussion of the states of privacy shifts our attention away from focusing on particular individual choices. If it is important that it is the individual who decides between a state of privacy or social disclosure, then it is important that it is possible to choose a state of privacy. But the availability of a state of privacy requires the presence of multiple environmental and social factors to support it.

III. THE PRIVACY BALANCE

The informational self-determination that Westin seems to endorse in defining privacy as a claim of control is, on closer inspection, a “process” through which an individual balances a desire for privacy with a desire for disclosure and communication. An individual’s choices in the face of those desires are shaped by environmental conditions, social norms, the curiosity of others, and “the processes of surveillance that every society sets in order to enforce its social norms.”¹⁷ This Part outlines the relationship between an individual’s choice regarding states of privacy and these other aspects of social and contextual norms that influence that choice. It then contrasts this individual balancing process with Westin’s idea of the “social” balance of privacy.

15 *Id.* at 42-43.

16 *Id.* at 31.

17 *Id.* at 5-6.

First, Westin points to “environmental conditions and social norms” as shaping the decision space.¹⁸ By this, Westin seems to contemplate factors that have an impact on an individual’s choice but are not directly about the specific actions of others. For example, there might be a social norm that suggests that an individual who is a guest in another’s home should not spend too much of their time alone in the guestroom but should socialize with the hosts. An individual might, for a variety of personal reasons, desire solitude while visiting another’s home and would have to decide whether to act on this desire or to conform to the social norm regarding socialization. The choices available to the individual would also depend upon environmental conditions — the fact of having a separate room with a door, for example. These environmental conditions themselves are sometimes, albeit not entirely, the product of social norms — if it is desirable to both have houseguests and to provide them with a place of personal retreat, then people will have separate guestrooms.¹⁹ The individual’s choice therefore is affected by norms regarding what is appropriate within that context. However, the individual still has a choice regarding whether to follow those norms or choose more or less privacy than those social norms dictate. The ease of any particular individual choice depends in part on the degree to which an individual’s desires regarding the balance between privacy and disclosure conform to social norms.

This distance between individual desires and social norms are why “we” (the judging public) can say that some individuals may desire too much or too little privacy. That distance can also help highlight the way in which individual choice feeds back into social norm creation. If there is a social norm against sharing a particular kind of information, and enough individuals decide to share it anyway, then the social norm can shift. This then changes the decision-making space of others who will find it more difficult to decline such sharing given the pressures of the new social norm.

Second, Westin points to the pressures from the “curiosity” of others and “processes of surveillance” for enforcing social norms. By these, Westin points to a different set of pressures faced by an individual while engaged in this “personal adjustment process.” Unlike general social norms or environmental conditions, these seem to recognize that particular others have interests in finding out things about you. The activities of others in prying in various ways is also governed by social norms. It might be that social norms dictate that it is generally rude to pry into another’s financial details, but it is allowed

18 *Id.* at 6.

19 This is obviously not entirely a function of social norms regarding the desired balance between privacy and social interaction — in expensive cities the ability to have such space is also a function of economics.

in some particular contexts. This is different from social norms that dictate that it is generally acceptable to pry into another's financial details. In the second, "reserve" in relation to finances will be very difficult for an individual to maintain, whereas in the first it is generally possible and will only admit of some exceptions. Another way to put this is that social norms that suggest that an individual should engage in social disclosure are also likely to support another's curiosity or social surveillance in the same context. This shows that norms of tact and discretion that help sustain states of privacy like reserve are also norms that push against the curiosity of others or processes of surveillance and, conversely, where curiosity and surveillance track social norms it will be difficult for individuals to choose a state of privacy, for the state of privacy will be less supported.

Although the *individual* adjustment process that Westin describes is fundamentally about an individual seeking balance, Westin also talks about "balance" in a different sense. This second sense of balance is the "social balance" between privacy and surveillance.²⁰ In the context of an individual seeking balance, surveillance is a pressure that exists in the decision-making space of the individual. By "social balance," Westin takes a more systematic perspective. Westin argues that the social balance is fundamentally shaped by the political system of a society. Totalitarian systems display a different balance than liberal democracies, and even within the category of liberal democracies there are multiple variations.²¹ This social balance also involves social norms, but they are different from the interpersonal norms that Westin often discusses when he discusses how curiosity or limited disclosure between individuals operates. These are norms that underpin our political and legal institutions and structure the relationship between individual and state.²²

What is the relationship between the individual balancing and the social balancing? Although Westin does not give a clear account of this, his descriptions of the different social balances in different societies show that surveillance does not just add pressure to an individual who is trying to decide on the right individual balance between privacy and disclosure, but also fundamentally shapes the availability of states of privacy in a society. If individual balancing is about the ability of an individual to choose a state of privacy, then this ability is deeply affected by a society's political and legal system and the extent to which privacy is protected in relation to other values. The meaningful

20 WESTIN, *supra* note 1, at 25-26.

21 *Id.* at 25.

22 See PRISCILLA REGAN, LEGISLATING PRIVACY: TECHNOLOGY RLP: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995).

choices of individuals can only be secured in the context of political and legal institutions that ensure an appropriate social balance of privacy.

IV. TOWARDS A NORMATIVE ACCOUNT OF PRIVACY

The argument so far is that privacy as a claim of individual control over personal information provides an inadequate account of privacy, even in terms of Westin's own exegesis. Instead, we need to understand privacy in terms of the ability of individuals to choose a state of privacy. This, in turn, shifts us away from questions of individual choice to instead focus on the social norms, environmental conditions, and broader political and legal norms that influence whether a state of privacy is available to be chosen and whether an individual has the means to choose it. If we are worried about the erosion of privacy, then instead of only strengthening individual control, we need to support meaningful choices. Understanding Westin's states of privacy, as discussed in the previous parts, starts to provide the normative basis for this discussion, although it is not sufficient.

Evaluating "meaningful" is not simply a descriptive project where we look at our society and ask whether there are in fact states of privacy available to be chosen. It is partly this, but it is also deeply normative. Westin's individual balancing is an ongoing process that individuals continuously engage in. The important issue is not whether at any given point in time an individual can make a particular choice, but whether they are provided with adequate choices in a more systematic manner. Answering this question requires understanding the role that privacy plays in an individual's life across multiple domains and over time, not just within interpersonal relationships but also in terms of the broader social and political context.

We can understand these normative dimensions better in relation to what Westin writes regarding the functions of privacy. Westin points to four main functions of privacy: personal autonomy, emotional release, self-evaluation, and limited and protected communication. The idea of personal autonomy at issue is the "sheltered" development of individuality and the protection of individual choice in relation to how an individual chooses to present herself to others.²³ Westin talks of a "core self" where an individual chooses to reveal information that is closer or further to this core and share it with people according to different levels of intimacy. However, we do not have to follow Westin on this point — people can have multiple roles and relationships and share different information across a rich diversity of relationships without

23 *Id.* at 36-37.

thinking that there is a “core” or essential identity, let alone a set of “concentric circles” regarding information that becomes less and less sensitive as one gets to the outer circle.²⁴ What is important is that this idea of autonomy is really about the protection of identity within social relations.

The function of “emotional release” is closely related. Here Westin points to the need for release and respite from social roles and their attendant pressures, as well as from the emotional stimulation of sociality.²⁵ This insulation from pressure and stimulation also helps with the function of “self-evaluation” — individuals need time and space to process and plan their activities. But this also has a moral component, for individuals need to be able to determine their own view of things and not just follow the view of others, a process that is difficult if one is never insulated from those pressures for social conformity.²⁶

Although Westin labels it this way, “limited and protected communication” is not really a “function” of privacy so much as another way of discussing the value of Westin’s state of privacy of reserve. Reserve is all about limiting communications about oneself to others and, as outlined previously, depends heavily on intersubjective norms of discretion and tact. The value of this is that it protects our ability to tell different people different things. In contrast, he describes the view of telling everything to everyone as “[t]he greatest threat to civilized social life.”²⁷ When Westin discusses limited and protected communication he discusses this in terms of both protecting the ability to share confidences within relationships of trust and protecting the ability to set boundaries through psychological distancing.²⁸ Both of these relate to protecting different aspects of relationship boundaries. So we might recast Westin’s function of privacy instead of “limited and protected communication” as “protecting relationship boundaries.”

How are these functions related to either the individual or social balance of privacy? Understanding the functions of privacy allows us to recast an individual’s desire for privacy in terms of navigating their social identity and role within social relationships with others. States of privacy insulate individuals from the pressure of social norms associated with various social roles and relationships, which is required for the development of individuality, emotional health, and the maintenance of relationships. Of course, too much privacy is also detrimental to many individual interests — it is easy for solitude

24 See Lisa M. Austin, *Control Yourself, or at Least Your Core Self*, 30 BULL. SCI. TECH. & SOC’Y 26 (2010).

25 *Id.* at 37-40.

26 *Id.* at 41.

27 *Id.*

28 *Id.* at 41-42.

to turn into social isolation. This is why it is individuals who navigate these relationships and seek the appropriate balance. However, that individuals have the ability to navigate their social identity in this way depends upon the availability of states of privacy and the means to choose them. This points towards the question whether we have the appropriate social balance of privacy. Many of the functions of privacy that Westin lists have broader social and political salience. For example, values like autonomy and the ability to engage in self-evaluation are central to liberal-democratic political systems. Answering the question of appropriate social balance requires providing an account of the relationship between the functions of privacy and these broader public norms.

V. NEW CHALLENGES AND THE LIMITS OF PRIVACY LAW

In the following Part, I want to show how this rereading of Westin's basic account of privacy can help us to understand the shortcomings of our legal models in the twenty-first century. The concern we should have is that the emerging infrastructure of surveillance will shift social practices in ways that undermine the availability of states of privacy and the means of attaining them, diminishing meaningful choices and altering the social balance of privacy. If we do not understand the role of social norms in our existing legal models, then we could end up in a situation where despite rigorously applying our existing laws we find ourselves facilitating the general erosion of privacy.

In what follows I will use my rereading of Westin's framework to analyze two existing models of privacy protection — private law (tort and property) and data protection law — for their shortcomings in this new context. I omit a discussion of public law models — such as data protection laws governing the public sector or constitutional protections — for several reasons. First, many new forms of state surveillance “piggyback” on top of private-sector data practices and so the latter should be our primary focus.²⁹ Second, many state practices are exceptions to the idea that an individual should have control over their information and so introduce a number of additional considerations, the discussion of which is beyond the scope of this Article.³⁰

29 See Lisa M. Austin, *Technological Tattletales and Constitutional Black Holes: Communications Intermediaries and Constitutional Constraints*, 17 THEORETICAL INQUIRIES L. 451 (2016).

30 See Lisa M. Austin, *Towards a Public Law of Privacy: Meeting the Big Data Challenge*, 71 SUP. CT. L. REV. 527 (2015).

A. Private Law

Consider first tort law. Although tort law falls within the realm of private law, and individuals bring tort actions in order to protect their individual interests, tort law does not protect an individual claim to privacy in Westin's sense of individual control. For example, the U.S. Restatement (Second) of Torts formulates the tort of intrusion upon seclusion in the following terms: One who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person.³¹

The tort protects individual choice only insofar as this choice aligns with the expectations of a reasonable person. As Robert Post describes, the privacy torts "safeguard[] rules of civility that in some significant measure constitute both individuals and community."³² By this, he means that individual personality is constituted in part through the civility rules that govern interpersonal interaction. The transgression of these social norms is an injury to social personality.³³ Another way to put this is that tort law constructs, and protects, states of privacy that depend for their definition upon social norms.

Other forms of private law can protect privacy in a manner that is not so dependent upon social norms. For example, in many Western liberal democracies property norms protect an individual's ability to choose solitude or to shelter intimate relationships from observation. As the owner of my home, I can keep people out for any reason I like or even no reason at all. I can choose solitude or intimacy to a degree that is quite out of keeping with social norms and the law will protect my choice — not because it endorses my choice of the balance between privacy and disclosure, but because it endorses my control over my home as an owner. Property functions as a kind of proxy for privacy, but property entitlements do not depend upon social norms regarding privacy.

Property norms are problematic if their role as privacy proxy is not well understood; they have done much damage in debates regarding privacy in public, where both "private" and "public" track property ideas. Courts were slow, but eventually have come to understand that just because something is no longer well-protected by property norms does not mean that there is no privacy interest worth protecting.³⁴ Courts are coming to also see that this

31 RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 2010).

32 Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 959 (1989).

33 *Id.* at 962.

34 *See, e.g.*, *Katz v. United States*, 389 U.S. 347 (1967) (the recognition that the U.S. 4th Amendment protects people, not places).

extends to observation in public places — just because property norms suggest that it is acceptable for other people to be in a location does not mean that all forms of privacy invasion are justified.³⁵ Property is an imperfect proxy for privacy. However, the loss of property as an effective means of achieving a state of privacy is also a serious loss. Property norms, at least in some circumstances, allow individuals to choose both more and less privacy than prevailing social norms might dictate is appropriate and without any need to examine social norms regarding those choices.

Our digital infrastructure is further eroding the usefulness of property norms as a useful proxy for privacy. In the online world these protections are irrelevant, and in the emerging onlife world — a world of cameras, sensors and the internet of things — the physical infrastructure is more often enlisted into projects of observation rather than the opposite. But it is not clear that tort can fill in this gap. As already outlined, tort law depends heavily on social norms of reasonableness and the infrastructure of surveillance is one that has profound effects on social norms. The various platforms that mediate this informational dimension of our physical world are also reshaping the ways in which we interact with one another. Platforms like Facebook have business models that depend upon the collection of as much information as possible, and so they build an architecture that is meant to nudge individuals towards disclosure.³⁶ If more and more individuals respond to these incentives by choosing social disclosure then the social norms will shift.

Westin was alive to a version of this problem from the 1960s. He argued that although individuals protect and respect the privacy of others through practices of discretion and tact, individuals are also curious about others; curiosity is a universal human trait. But Westin pointed to the rise of a dangerous form of curiosity that he labelled “voyeurism.”³⁷ He wrote:

As used in its social rather than its clinical sense, voyeurism refers to the tasteless pursuit and aggressive exposure of the privacies of personal life, especially sexual conduct among the socially prominent. Such invasion of privacy for its own sake as a stimulant to those who do not find direct social satisfactions is commonly seen in the mass circulation of confession and fan magazines; . . . The intimate relations that are captured and disclosed by wiretapping, camera surveillance, or

35 *Alberta v. United Food and Commercial Workers*, [2013] 3 S.C.R. 733 (Can.).

36 Zuboff calls this surveillance capitalism. See Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization IC*, 30 J. INFO. TECH. 75 (2015).

37 WESTIN, *supra* note 1, at 60.

personality testing find an avid market in the voyeuristically inclined segment of the public.³⁸

If the problem in the 1960s was the easy availability of technologies that encourage voyeurism, the problem of the twenty-first century is the creation of an entire social-technical infrastructure that is encouraging new forms of curiosity.

If legally protected states of privacy are so deeply dependent on social norms, then these states are vulnerable to erosion by shifting social norms that favor prying and disclosure. The worry is that we are increasingly inhabiting a digital world created to facilitate such a shift in social norms. But they will shift in the context of a world where there are no longer any obvious means for individuals to choose a privacy balance that is more privacy-protective than these social norms dictate.

All of this orients us towards the need to develop a more robust normative understanding of the states of privacy that should be protected in a free and democratic society and ensure that individuals have the means to choose such states even when this runs against the current of the prevailing preferences of others. Otherwise our laws will be helpless in the face of a built environment where identification and observation is the essence of the architecture and the practices that it facilitates.

B. Data Protection Law

In contrast to tort law, data protection law models modelled on fair information practice principles (FIPPs) are more closely aligned with Westin's understanding of privacy as a claim of individual control over personal information. This is especially true if we look at data protection law models that emphasize informed consent. If the collection, use and disclosure of personal information requires my consent then I have the ability to determine for myself "when, how, and to what extent, information about [me] is communicated to others."³⁹ This form of legal protection appears to offer individuals a means through which to choose either more or less privacy than prevailing social norms might dictate because it is so strongly focused on individual choice. However, as I will outline, data protection law models are not immune to the problem of shifting social norms.

Consider a strong consent-focused regime like Canada's *Personal Information and Protection of Electronic Documents Act* (PIPEDA), which

38 *Id.* at 61.

39 WESTIN, *supra* note 1, at 5.

regulates private-sector data practices.⁴⁰ Experience with this legislation shows that even where informed consent is required decisions need to be made regarding whether consent is explicit or implied, opt-in or opt-out. Under PIPEDA, these issues are determined through reference to how “sensitive” the information is and “reasonable expectations.”⁴¹ This is where prevailing social norms can heavily influence the robustness of the consent regime. For example, the Office of the Privacy Commissioner of Canada (OPC) held that Facebook’s privacy default settings needed to be “reasonable” and that this meant that they had to reflect “the reasonable expectations of Facebook users.”⁴² Given that the point of Facebook is to share information, a preselected default of sharing with friends and networks is acceptable.⁴³ The social norms that informed this analysis were the social norms created by Facebook users with the considerable influence of Facebook. In this way, platforms can create architectures that nudge people towards information disclosure, and their success in doing this can then undermine the actual strength of the provisions meant to operationalize individual control.

There are other options for thinking about defaults than the route taken by the OPC in its Facebook decision. One is to take seriously the “privacy paradox” and note that the actual choices of individuals do not always conform to their stated preferences, and that the practices of businesses like Facebook are often optimized to induce maximum information disclosure. Given this, we should not look to the practices of Facebook users to discern reasonable expectations but find other methods to understand their preferences in a manner that is independent of choices made within surveillance architectures.⁴⁴ Another option is to require “privacy by default,” or that the default option be the most privacy-protective so that individuals must actively opt-in to broader information sharing.⁴⁵ In the Facebook context, this could mean that the default answer to “who can see your friends list” should be “only me”

40 Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.).

41 *Id.* at Schedule 1, Principle 4.3.

42 ELIZABETH DENHAM, REPORT OF THE FINDINGS INTO THE COMPLAINT FILES BY THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC) AGAINST FACEBOOK INC. UNDER THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT 89 (2009).

43 The OPC did take issue with the default of “everyone” for the sharing of photos.

44 See, e.g., Ron Hirschprung et al., *Analyzing and Optimizing Access Control Choice Architectures in Online Social Networks*, 8 ACM TRANSACTIONS INTELLIGENT SYS. TECH. 57 (2017).

45 See generally Ian Kerr, *The Devil is in the Defaults*, 4 CRITICAL ANALYSIS L. 91 (2017).

rather than “public.” This would be an architecture that nudges individuals towards choosing nondisclosure over disclosure. Justifying this approach to defaults requires a more strongly normative interpretation of “reasonable expectations” that embraces the considerations I have outlined in the previous Parts regarding meaningful choice. If “reasonable” simply tracks an idea of general social norms, then we might need better methods of identifying those norms independently of their revealed choices within platforms like Facebook, but we do not have grounds to require a default that is more privacy-protective than what most people would choose. To do the latter requires an account of how such a default better maintains the general availability of states of privacy and the means of choosing them, and why this is important within a liberal-democratic society.

The *lack* of social norms in relation to some data practices can also erode privacy on the data protection law model. When I choose to share personal information with a corporation in exchange for services of some kind, I do not do so within a rich context of intersubjective norms that govern other relationships. As Robert Post argues, “relationships between individuals and large organizations like credit rating agencies are not sufficiently textured or dense to sustain vital rules of civility.”⁴⁶ Yet recall that Westin’s state of privacy as reserve dealt with disclosures of personal information and limited communications, and was sustained through these norms of civility that involve the tact and discretion of others. If we take this away, then an individual who chooses to disclose personal information to another (now an organization) does not know from the social context and the relationship whether she is engaged in a limited communication or not. Requiring that organization to tell the individual what purposes her information will be used for and then requiring it to only use and disclose that information for those purposes provides that individual with the missing information about the context of disclosure. But this does not necessarily reproduce a state of privacy like reserve — the options provided are not created through a rich social world of norms, but through the transactional logics of organizational relationships where organizations have a lot of power to define these norms. It also places an additional burden on individuals to understand the implications of their choices in these contexts because they can no longer rely upon shared social understandings to help them navigate their disclosures. This burden is one of the reasons why choice models are thought to be failing.⁴⁷

46 Post, *supra* note 32, at 1009.

47 Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013).

We need to move beyond an emphasis on consent as the key to privacy protection. Even theorists who embrace the individual control model, like Birnhack, caution that we should not conflate individual control with ideas of consent. FIPPs provide a more robust set of principles that enable control over personal information than simply notice and choice.⁴⁸ One such crucial principle is the data minimization principle.

Consider the following example: If I desire to purchase a widget from a bricks-and-mortar store then I can enter the store, pay with cash, and leave. Nobody needs to learn my identity or anything about me except, at the time of checkout, that I have the required amount of money for the purchase. If I desire to purchase a widget online, then I need to provide more information in order to both pay for the widget and have it delivered. Data minimization is the basic principle that the online widget store should only ask me for the amount of information necessary to complete the transaction and no more. This protects meaningful choice in the sense that if I choose disclosure (of payment and shipping information, for example) over social withdrawal then I should only have to disclose the information that is needed in order to achieve my objective (purchase the widget).

However, there are ambiguities here that are increasingly important. For example, should the online widget store be required to provide me with an option for anonymous payment? Should it be required to provide me with an option for anonymous pickup? In general, data protection legislation has provided few levers for requiring such choices. If we think in terms of individuals choosing for themselves how to balance privacy and disclosure, and then focus on specific individual choices, data minimization would just seem to mean that we take it for granted that an individual has chosen disclosure and we limit the amount of disclosure to the minimum needed. If an individual had wanted a different balance between privacy and disclosure, in the example of the widget, she could choose to shop in person and pay cash. But it is also not the case that our laws should require the ability to purchase all things anonymously at all times. Whether or not this is desirable depends upon the values and practices at stake in purchasing widgets anonymously and also the overall balance between privacy and disclosure across a range of activities and relationships that make up our lives.

If we take a more systemic approach, and are concerned with the nature of the choices offered in a more systematic fashion, then we would interpret data minimization to also sometimes require offering the ability to engage in transactions without sharing personal information — so we would not start

48 Michael Birnhack, *A Process-Based Approach to Informational Privacy and the Case of Big Medical Data*, 20 THEORETICAL INQUIRIES L. 257 (2019).

from the assumption that an individual is choosing disclosure, but by placing a burden on the organization to show that they require disclosure.

In Canada, this has not been the approach. Part of the issue is the fact that PIPEDA's very purpose is to balance the right of privacy with the needs of organizations.⁴⁹ When these organizations adopt data-intensive business models that create incentives for organizations to collect as much information as they can from individuals, then this introduces a very serious tension with privacy that gets "baked in" to privacy law at the outset. For example, in its Facebook decision, the OPC held that individuals *had* to consent to the use of their personal information to deliver Facebook Ads because Facebook's business model relies upon advertising revenue.⁵⁰ Nor would the online widget store face an obligation to provide anonymous payments.⁵¹ This shows that interpreting the demands of data minimization is not simply a technical inquiry (do you need this data to do X) but has important normative dimensions regarding the interpretation of business needs and the place of privacy in relation to those needs.

Part of the problem with the Canadian approach is that PIPEDA is interpreted as consumer protection legislation, rather than human rights legislation. The Supreme Court of Canada has clearly stated that even private-sector data protection law is "quasi-constitutional," but this has not yet made an impact on its interpretation.⁵² A human rights approach to balancing privacy and business interests would place a more significant burden on businesses to offer meaningful choices. Human rights legislation places burdens on organizations to accommodate things like disabilities up to the point of "undue hardship." While a consumer approach to interpreting data minimization requires organizations to offer disclosure-minimizing options consistent with a balance between consumer and business interests, a human rights approach to interpreting data minimization would require organizations to offer privacy-preserving options up to the point of undue hardship. In other words, a robust data minimization framework will come from a more robust understanding of the need to offer individuals meaningful choices with respect to states of privacy, and this in turn requires a stronger normative account of the relationship between privacy interests, business interests, and broader public norms.

49 Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5, § 3 (Can.).

50 DENHAM, *supra* note 41.

51 *See, e.g., PIPEDA Case Summary #2002-48*, OFF. PRIVACY COMM'R CAN. (Apr. 29, 2002), <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2002/pipeda-2002-048/>.

52 *Alberta v. United Food and Commercial Workers*, [2013] 3 S.C.R. 733 (Can.).

This inquiry requires a broad systematic perspective with empirical dimensions as well. Whether anonymous payment options are required depends upon how one views the importance of freedom from identification in commercial transactions in relation to the broader social and political dimensions of privacy.⁵³ But it also depends on whether, in general, individuals have other viable options to purchase similar items in person using cash and therefore can choose anonymous commerce in many instances even if not in every instance online. This systemic view can also involve understanding the relationship between privacy and other important values such as equality. Anonymous payment options for transportation systems like subways and buses might be more important where a greater proportion of the population relies on transit than where walking or driving are viable options. But it also might be that without anonymous payment options we create a system where the poor are denied anonymous travel choices because they must take the bus, whereas the wealthy are provided anonymous travel choices because they can drive. This systemic perspective is also needed to address issues that arise with companies like Facebook. When platforms achieve a certain level of social dominance, it is very difficult for individuals to refuse all participation. They should be given the choice of a privacy-protective form of participation.

It is not clear that more robust legal rules for “privacy by design” (PbD) will help achieve this infrastructure of privacy unless this broader normative and systematic account of privacy is provided. There is a rich literature on PbD but the details are not important for this discussion.⁵⁴ The main issue is that what is demanded by PbD will depend upon what is demanded by privacy law obligations in the first place. If data minimization is interpreted so that it does not require making anonymous payment options available, for example, then PbD is not going to provide these either. We need to build our infrastructure to support the availability of states of privacy, and the means through which to choose them, but the robustness of this infrastructure will depend upon the robustness of our normative account of meaningful privacy choices.

One way that data protection models sometimes deal with the need to maintain the possibility of states of privacy is to prohibit the collection, use or disclosure of certain categories of “sensitive” information.⁵⁵ In some

53 There are additional complications if we add the question of when an individual can remain anonymous in relation to the state.

54 See Michael Birnhack, Eron Toch & Irit Hadar, *Privacy Mindset, Technological Mindset*, 55 JURIMETRICS J.L. SCI. & TECH. 55 (2014).

55 For example, the Office of the Privacy Commissioner of Canada has recently indicated that it will “draft new guidance for businesses on no-go zones where

ways this appears to be consistent with the account I've been providing, for it creates a state of privacy in terms of freedom from disclosure of sensitive information. The difficulty with this is that it takes us outside of the paradigm of meaningful *choice* since individuals are not given a choice. We coerce privacy choices, which is at odds with Westin's view that, even from the perspective of an individual's interests, one can have both too much and too little privacy and the individual is best placed to make this decision.⁵⁶ If we think that an individual will not make informed decisions about their own self-interest, then the way to address this is to strengthen transparency and provide strong defaults in relation to sensitive categories of information rather than "no-go zones." If we think that an individual will make decisions that lead to less privacy for others by shifting social norms in the ways I have been describing, then the way to address this is by ensuring more privacy-meaningful choices for individuals who want a balance that is different from these shifting social norms. And this involves placing a positive obligation on private-sector platforms to create the means through which individuals can choose states of privacy.

The place for "no-go zones" is not in relation to individual choice but in relation to creating barriers to some forms of nonconsensual collection, use and disclosure of personal information. All data protection law permits exceptions to consent for purposes such as law enforcement. And constitutional law permits law enforcement access to information that attracts a reasonable expectation of privacy — this access just needs to be governed by protective processes such as obtaining a warrant. But the new infrastructure of surveillance potentially places such a vast amount of information in the hands of the state that it might be time to rethink the terms of this private/public nexus of surveillance and replace a permeable boundary with some firm walls, at least in some cases. We already do this in some contexts. For example, in Canada the census form is treated as privileged and cannot be used as evidence in any kind of proceeding.⁵⁷ The nonconsensual use of data collected through private-sector mechanisms is an area worth much greater attention.

the use of personal information, even with consent, should be prohibited as inappropriate." See *2016-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act*, OFF. PRIVACY COMM'R CAN. (Sep. 21, 2017), https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1.

56 *But see* Anita Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723 (1999).

57 Statistics Act, R.S.C. 1985, c S-19, § 18 (Can.).

VI. THE LIMITS OF MEANINGFUL CHOICE

I have proposed a rereading of Westin's definition of privacy that focuses on meaningful choice rather than individual control. Meaningful choice contemplates the availability of states of privacy for individuals to choose, and the availability of the means to choose them. Where an individual control account emphasizes the role of the individual in choosing privacy, a meaningful choice account emphasizes the role of public norms and built environment to create an infrastructure to enable privacy-protective choices.

There are, of course, other approaches that also emphasize the importance of infrastructure.⁵⁸ This Westin-inspired account of meaningful choice has both benefits and limits. The main benefit is that it provides a clear way of engaging with the many regulators and technologists who remain inspired by Westin's control-based account. By showing the complexities of Westin's own view, it can help dislodge some of the hyper-individualized versions of control-based approaches and help reconcile an emphasis on individual choice with the broader considerations I have been outlining. This centrality of individual choice is, for those not so enthusiastic about control-based accounts, the main weakness of a meaningful choice approach. And although I have pointed to the many social dimensions acknowledged in Westin's text, there is much there in terms of his understanding of individuality and its construction that remains open to critique, and much about the broader public norms at issue that remains underdeveloped. I do not undertake such critique or development here but only acknowledge that this is where I think the main limits of the rereading are to be found.

There are other potential limits of a different kind. One general question that all privacy theories have to face is whether or not to embrace all concerns regarding informational practices under the rubric of "privacy." Westin discusses some interesting examples that indicate that some forms of data analysis that get raised in privacy discussions are not, on his account, privacy issues. If they are nonetheless concerning then we need a different label for them.

For example, Westin points to self-disclosure as a threat to privacy — that an individual can reveal so much about herself that she no longer has a "private life."⁵⁹ This loss of individual reserve can then affect the discretion of others, as "if enough individuals lose their reserve, the sense of discretion in others

58 See, e.g., Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES L. 1 (2019); Mireille Hildebrandt, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, 20 THEORETICAL INQUIRIES L. 83 (2019).

59 WESTIN, *supra* note 1, at 57.

would be affected; those who tell all prompt others to ask all.” For examples of this kind of “self-invasion,” Westin points to the practices at the time of public-opinion pollsters and behavioral researchers. But what is fascinating is that Westin draws back from ultimately criticizing these practices. He found that Americans were willing to engage in such self-disclosure and argued that the reserve that is appropriate in interpersonal relationships with intimates is different than that for anonymous disclosures to strangers:

Reputable polling and survey organizations, it must be remembered, always tell their subjects that all information will be treated as confidential and that the subject’s identity will never be disclosed; this guarantee of anonymity has been respected. Furthermore, the interviewer and the polling agency he represents are strangers to the respondent and will remain so; this is not the surveillance of government, the boss, neighbours, friends, or intimates. The respondent knows that he will not be hurt by disclosing his private thoughts, his past conduct, or his future intentions; nothing will be used against him. Indeed, not only will he not be influenced by self-disclosure, but the interview offers him as well an unusual opportunity to influence others — the manufacturers, television programmers, advertisers, government agencies, and others who will read and study what the respondent says.⁶⁰

Westin suggests here that some forms of self-disclosure, and the practices that encourage this, are not ultimately a threat to privacy if they do not come back to affect an individual in terms of harm or influence. In the example he gives about polling organizations, there would also be no obvious way in which the self-disclosure would affect interpersonal norms of discretion and thereby erode the social norms we need to protect our practices of reserve. This would suggest that not all “platforms” that encourage self-disclosure are a threat to privacy, and that this could include some forms of data collection and use that help us to gain social insights.⁶¹

Westin was also deeply interested in the use of personality testing. Some of the concerns about such testing echo more contemporary concerns regarding algorithmic decision-making in that the technology can be used to find out information about an individual that they would not otherwise choose to disclose (and might not even know themselves). But his deeper concern regarding this

60 *Id.* at 58-59.

61 This might open a discussion on the relationship between privacy questions and the benefits of machine learning. See Ryan Calo, *Technology, Law, and Affordance: A Review of Smart Technologies and the End(s) of Law*, 4 CRITICAL ANALYSIS L. 72 (2017); Hildebrandt, *supra* note 58.

technology does not seem to be privacy. Consider the following discussion of the use of personality testing for personnel selection:

In all these situations the assertion of privacy serves to say to those in power: “If you make evaluative decisions openly, questioning me directly and justifying your decisions openly, I can fight out publicly your right to judge me in a certain way, and American society will decide our conflicting claims. But if you invoice ‘science’ and ‘expertise’ and evaluate me through personality tests, the issue becomes masked and the public cannot judge the validity and morality of these evaluative decisions. Thus, where such basic issues as political ideology, religion, and race are at stake, the selection process must be objective and public, and I assert my right of privacy to close my emotions, beliefs, and attitudes to the process of job evaluation in a free society.”⁶²

The privacy claim in relation to personality testing is one that is really at base a transparency claim: the real issue is the lack of transparency in evaluative decisions when they are made on the basis of personality testing. Claiming privacy is a way of stopping this practice and forcing public transparency. Similarly, there are many contemporary questions of fairness and transparency surrounding algorithmic decision-making. However, the language of privacy becomes an even more awkward fit than Westin’s use of it here.

There are at least three main types of responses one might have to these examples. The first is to argue that because there is no privacy problem on Westin’s account that there is no problem generally. The second is to argue that this just shows that Westin’s account of privacy, being so deeply rooted in interpersonal norms, is too narrow to account for the kinds of informational contexts we must now navigate. The third is to argue that even if there is no privacy problem, there might be other kinds of problems with these practices and we should seek a broader account of data governance than the language of privacy permits. Evaluating and developing these options requires moving beyond Westin’s account in *Privacy and Freedom*.

CONCLUSION

As Daniel Solove argues in his introduction to the new edition of *Privacy and Freedom*, Westin’s work “remains one of the most comprehensive and electrifying accounts of the concept and value of privacy yet written.”⁶³ One of

62 WESTIN, *supra* note 1, at 66.

63 *Id.* at viii.

the reasons for its comprehensive nature is that it came out of a larger project associated with the Special Committee on Science and the Law, which was part of the Association of the Bar of the City of New York. The role of the committee was purposefully broad: to study “the interrelationships between man, science, and society and the concessions which each sought to exact from the others,” and to do so through collaboration between lawyers and scientists.⁶⁴ In 1962 the committee launched a formal study on privacy, with Alan Westin as the director of research, and which was conducted over a four-year period. The richness of the resulting text is often overlooked and yet it still contains much that is instructive.

In this Article, I have offered a rereading of Westin to show that his account is much more complex than the definition of individual control over personal information that he is most often associated with. Moreover, these complexities are helpful in relation to our current context. What is helpful is also what is most ambiguous in Westin — his acknowledgement that privacy is both a claim and a state. The best way to reconcile this is to embrace a view of privacy as involving individual choice in relation to states of privacy. Instead of individual control we need to focus on meaningful choice — are states of privacy available to be chosen and do individuals have the means to choose them? This requires that we attend to the way in which the private sector is building an infrastructure of surveillance and that we impose obligations on the private sector to provide individuals with the effective means to choose states of privacy. Some of this involves attention to the technical — how this world should be built. But some of this requires more attention to the normative — the functions of privacy and its role in our political and legal frameworks — so that shifting social norms do not subvert the social balance between privacy and surveillance most supportive of a free and democratic society.

64 *Id.* at xii-xiii

