Symposium: Firmin DeBrabander's *Life After Privacy: Reclaiming Democracy in a Surveillance Society*

Push Back Harder: Asymmetric Power and the Struggle for Privacy

Irfan Khawaja[1]

CorroHealth

1. Prècis of *Life After Privacy*

It is no secret that we live, as Firmin DeBrabander aptly puts it, in a world "after privacy." "Democracy," we have long been taught, "is unthinkable without privacy," but the task of his book, *Life After Privacy*, is precisely "to think it."[2] He writes:

> My aim is to understand the prospects and future of democracy without privacy, or very little of it—and with a citizenry that

[1] I am a Provider Support Associate with CorroHealth, a health care revenue-cycle management company based in Plano, Texas, with an affiliate in Iselin, New Jersey, where I work. I am in no way a spokesperson, official or otherwise, for CorroHealth or any of its affiliates. The claims I make in this essay are made exclusively in my own name, at my own initiative and responsibility.

[2] Firmin DeBrabander, *Life After Privacy: Reclaiming Democracy in a Surveillance Society* (New York: Cambridge University Press, 2020), p. ix.

Reason Papers 44, no. 1 (Spring 2024): 5-19.

> cares little about privacy, and does not know why to appreciate it, or protect it.[3]

DeBrabander begins with a well-documented fact that by now should be common knowledge: Big Data, meaning the data-mining and data-harvesting branches of the modern corporation and modern state, have within just a few decades subverted almost all of the norms of privacy that preceded the rise of the Internet, and have created a surveillance state of unprecedented scope and power.

I will not belabor the details of DeBrabander's story here, which relies on well-known work by Bruce Schneier, Michael Lynch, Cathy O'Neill, Zeynep Tufekci, and Shoshana Zuboff, among others.[4] The bottom line is that, through the (literal) devices of Big Data, your privacy is either a dead letter or on its way to getting there. Every move you make leaves a digital footprint that someone, somewhere, is harvesting and monetizing. It is tempting to regard yourself as benefited by the convenience you enjoy and opportunities for self-expression you get as a result, but it is also likely that you have no idea how many liberties Big Data has taken with your "private life" and how little privacy you now enjoy.

How did this happen? On DeBrabander's account, our predicament might be likened to that of the Biblical Esau: We sold our privacy for the digital equivalent of a mess of pottage. Big Data gave us an iterated series of trade-offs, over decades, of convenience or self-expression over privacy.[5] We cultivated societies of unbridled preference-satisfaction subject to the imperatives of immediate gratification. We thus chose convenience and self-expression over

[3] DeBrabander, *Life After Privacy*, p. ix.

[4] See, e.g., Bruce Schneier, *Data and Goliath* (New York: W.W. Norton, 2015); Michael Lynch, *The Internet of Us* (New York: W.W. Norton, 2016); Cathy O'Neill, *Weapons of Math Destruction* (New York: Broadway Books, 2016); Zeynep Tufekci, *Twitter and Tear Gas* (New Haven, CT: Yale University Press, 2017); and Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York: Public Affairs, 2019).

[5] The story of Esau and Jacob is told at Genesis 25:25–34.

privacy, iterated across billions of mouse clicks, and divested ourselves by our own hands of our birthright.

It might in a sober moment occur to us that that we have given too much away to entities that may well threaten our well-being. What to do? There are, essentially, two options: either we explicitly fight for privacy under that description or we surrender our privacy and learn to live without it. DeBrabander makes an extended, albeit reluctant, case for the latter option, one part pragmatic, the other part theoretical.

The pragmatic part of the argument tells us that resistance to Big Data has at this point become futile. For one thing, there's *nothing left to fight about*: Big Data already has our data and already has the means by which to acquire whatever is left, so there is really nothing left to defend. For another, *there are no weapons left with which to fight*; there is no plausible or viable mechanism by which to hold the line against Big Data, much less to get back the privacy we have lost. Individual hacks will not work. Government regulation moves too slowly to catch up to Big Data's workarounds, and network-based activism, heavily reliant on the Internet, is easily neutralized by the owners of the networks on which it relies. To paraphrase Jesus, you might as well put down your digital sword.[6]

The theoretical part of the argument questions the nature and value of privacy itself. Consider three fundamental problems.

(1) First, it is not clear what harm is involved when privacy is "invaded." Much of the privacy we give away, after all, is relinquished voluntarily. Even apart from consent, it is unclear where the harm is supposed to be. Some authors (for example, Zuboff) seem to equate data harvesting with "invasion" and Big Data with totalitarianism or imperialism, but that seems overstated. Others (for example, Lynch) seem to insist that the Self is harmed in the sheer act of unwanted scrutiny by others, but surely that depends on the aims and context of the scrutiny. There is, it seems, no entirely general or generalizable account of the harm involved in "the invasion of privacy." The

[6] From the King James Version of the Gospel of St. Matthew (26:52): "Then said Jesus unto him, Put up again thy sword into his place: for all they that take the sword shall perish with the sword."

uncomfortable question thus arises: How can data privacy matter so much if we have no account of the wrongness of violating it?[7]

(2) Second, beyond the preceding theoretical lacunae, it might well be argued that privacy is a pernicious and self-subverting normative ideal, neither capable of inspiring a fight nor worth the candle. By its nature, the quest for privacy privatizes life. It atomizes us, separates us, and drives us into cocoon-like enclaves of comfort designed to filter out the unpleasant facts of life that constitute the subject-matter of politics. In doing so, it systematically unfits us for political life by an insidious logic of its own. Given our Esau-like proclivities, it is not as though we are inclined to resist either their blandishments or their takings. To paraphrase Karl Marx, the ethos of privacy becomes its own gravedigger.[8] It may well deserve it.[9]

(3) Third, at the deepest level, however, privacy is problematic because it presupposes an indefensible conception of the self—a private self that enjoys its privacy by retreating away from the social realm to commune with itself, by itself. DeBrabander traces this idea to a strand of peculiarly modern thought in the Western tradition, from Michel de Montaigne to Henry David Thoreau and through Anglo-American jurisprudence of the past century or so. Essential to this conception of privacy is the asocial atom of social contract theory: the utterly self-determining, self-forming, rigidly bordered Self that must be *left* alone, like some Leibnizian monad, the better to realize itself.[10]

---

[7] For problem (1), see DeBrabander, *Life After Privacy*, chap. 2. Though not discussed in DeBrabander's book, it might have been worth engaging on issue (1) with the work of Adam Moore, *Privacy Rights: Moral and Legal Foundations* (University Park, PA: Penn State University Press, 2010).

[8] "What the bourgeoisie, therefore, produces, above all, is its own grave-diggers. Its fall and the victory of the proletariat are equally inevitable." See Karl Marx, *The Communist Manifesto*, in Karl Marx, *Selected Writings*, ed. Lawrence H. Simon (Indianapolis, IN: Hackett Publishing, 1994), p. 169.

[9] For problem (2), see DeBrabander, *Life After Privacy*, chaps. 5, 7, 8, and Conclusion.

[10] For problem (3), see DeBrabander, *Life After Privacy*, chap. 6.

However, there is (DeBrabander suggests) no good philosophical reason to believe in such a Self or the realization it needs. If there is not (an issue beyond my scope in this essay), there is no need for the extreme sort of privacy it demands. We ought perhaps to replace that atomistic conception of privacy with a more moderate one of the kind we find in Stoic, religious, and otherwise non-individualist conceptions of interiority, whose less romantic conceptions of privacy found expression in political regimes radically different from those that prevail in individualist Britain or America. The point is not to oscillate from, say, wild Thoreauvian freedom to theocratic repression, but to find the mean between them.

Given this, it is perhaps misleading of me to have described DeBrabander as counseling "surrender" to Big Data, full stop. What he wants is surrender on the *privacy* front, combined with an opening on a different front, the political. We should, on his view, replace our crusade for and valorization of privacy with a turn to a properly political conception of public life inspired by (a version of) Aristotle, John Dewey, and Hannah Arendt. The practical models here are the American civil rights and labor movements.[11] Neither movement aimed at or relied heavily for the effectuation of its aims on privacy. Freedom, equality, and justice are essentially public in character; they were won not by a retreat into the private sphere, much less by privatization, but by publicity, exposure, and the values of collective action in the service of a common good. Unlike digital activism, these movements were incontestable success stories (at least on their own terms, as far as achieving their own immediate and most pressing political aims), so we would do well to follow their lead. Doing so might win back some of our privacy without explicitly aiming at it, but more importantly, would

[11] On the civil rights movement, DeBrabander cites Taylor Branch's *Parting the Waters: America in the King Years 1954–63* (New York: Simon and Schuster, 1988); on the labor movement, he cites Philip Dray's *There Is Power in a Union* (New York: Anchor Books, 2010), and Erik Loomis, *A History of America in Ten Strikes* (New York: The New Press, 2018). See DeBrabander, *Life After Privacy*, pp. 99–104.

pay dividends in the restoration of our common public life, which is where the action is or ought to be.[12]

2. Blaming the Victims?

I should begin my remarks with a confession. Though I spent some twenty-six years as an academic philosopher, I now work in Big Data. That makes me a kind of Edward-Snowden-in-reverse vis-à-vis my former profession: Edward Snowden left his former profession to disclose the facts about Big Data; I have left mine to become a guardian of the asymmetric power and secrecy by which Big Data operates. Put another way, you've all met the enemy and it's me.[13] Given that, I want in my remarks here to focus on a narrowly pragmatic (rather than deeply philosophical) aspect of DeBrabander's overall argument: I am going to discuss at length the Esau-like diagnosis he gives of our predicament and then touch briefly on his proposal to surrender the privacy front while shifting focus to the political.

As I see it, DeBrabander overstates our culpability for our loss of privacy in a way that amounts to blaming the victims. In doing so, he understates Big Data's culpability for that loss. Given that, his proposal to direct our attention away from privacy as such ends up giving Big Data a pass and averting our eyes from its culpability. In fact, it seems to me that he gets much of the story backwards. We should be pinning the blame for the loss of our privacy squarely on Big Data, and only there, and, as a society, pushing back on Big Data much harder than we have. That is a precondition of any restoration of the political, not an expected consequence.

---

[12] The suggestion is made throughout the book, but see in particular DeBrabander, *Life After Privacy*, chaps. 3, 4, 7, 8, and the Conclusion, e.g., pp. 72–74, and 157–63. I should emphasize that the paragraph as a whole is intended to capture DeBrabander's view, not my own.

[13] On my affiliation, see note 1. On Edward Snowden and related issues, see Edward Snowden, *Permanent Record* (New York: Metropolitan Books, 2019), and Barton Gellman, *Dark Mirror: Edward Snowden and the American Surveillance State* (New York: Penguin, 2021).

As a first approach, consider four explanatory models for understanding how Big Data managed to undermine privacy. The taxonomy is intended to be a rough, first approximation toward carving up logical space, neither mutually exclusive nor jointly exhaustive:

(1) *Unilateral seizure*: Big Data unilaterally acted to take our privacy; we played little or no voluntary role.

(2) *Voluntary relinquishment*: we voluntarily consented to give Big Data our privacy; it played little or no coercive role.

(3) *Symmetrical co-causation*: we acted in concert with Big Data, each party making co-equal contributions to the outcome.

(4) *Asymmetrical co-causation*: we acted in concert with Big Data, each party making unequal contributions to the outcome.

As I read him, DeBrabander oscillates throughout his book between (2), (3), and (4). Sometimes, he writes as though our loss of privacy is all our doing (2). Sometimes, he writes as though our loss of privacy is partially our doing (3). Sometimes, he acknowledges that while we voluntarily and culpably gave our own privacy away, Big Data, being the asymmetric player, played the larger causal role in producing the privacy-diminishing outcome (4).

My own view is a variant on (1). As I see it, Big Data acted unilaterally and coercively to take our privacy; the role it played was sufficient to produce the outcome. It is no doubt true that through apathy, indifference, and self-indulgence, we, its victims, made our own little contribution to the outcome, but I regard this as *explanatorily* irrelevant. The role we played was over-determined by the role Big Data played. Our role was epiphenomenal. Given the asymmetries of power involved, the informational constraints placed on us, and the sheer technical sophistication of the techniques deployed, there is almost nothing we could have done to forestall the outcome and save our privacy. Once the Big Data juggernaut began, it was fated to win, at least as far as it *has* won. Even if you factor in our culpability (where "our" excludes the power brokers within Big Data itself), it plays no important explanatory role.

To understand the actions involved, we have to understand the nature of the actors—the *modern corporation* and the *modern state*. The essential feature of both—to understate things—is asymmetric power vis-à-vis the rest of us. Both the corporation and the state are, in slightly different ways, mutually reinforcing *monopolies*. Whatever the moral tone of the rhetoric they use, both are fundamentally amoral, unscrupulous agents of power, unconstrained by the sorts of norms that constrain the average person acting in something other than an *ex officio* role.

The state has a monopoly on the initiation, use, distribution, and authorization of force; it decides when force is to be used, what force is to be used, against whom, to what degree, and with what consequences.[14] In part for this very reason, it enjoys immunity for abuses of its authority. Formally, the state enjoys *sovereign immunity*; informally, it enjoys a sense of practical impunity.[15] What this means is that states are authorized, both *de jure* and *de facto*, to lie, cheat, steal, trespass, assault, torture, and murder without having to answer for it in any way that compares to the accountability demanded of the governed. Their doing so is the exception, not the rule. Paradoxically, the state enjoys a presumption of moral authority on top of all of this: regardless of its actual moral status, states demand that the governed acknowledge their legitimacy and go to remarkable lengths to ensure that they do. Being a state actor not only means almost never having to say "sorry," but by the terms of conventional moral and legal logic, means almost never having anything to say "sorry" for.

One implication of the state's monopoly on force is its exclusive prerogative to define, through the rule of law, how force is to be used. A further, nearly trivial implication is that it gets to define the nature of property and contract rights and their enforcement, including how, where, and when resources are legitimately to be extracted from the sources of initial appropriation and how they are to be transferred from

[14] See, e.g., the entry for "State (polity)" on Wikipedia: https://en.wikipedia.org/wiki/State_(polity).

[15] On sovereign immunity, see the entry for "Sovereign immunity" on Wikipedia: https://en.wikipedia.org/wiki/Sovereign_immunity.

there on. Because it enjoys this monopoly, the state has the option either to regulate appropriation and transfer directly or to outsource the task to others.

The modern corporation is in essence the relevant outsourcing operation.[16] The state grants to the corporation a permission—once upon a time a charter, now a permit, license, or registration—to exercise a mini-monopoly on resource extraction, defined by the state, including limitations on liability for torts and guarantees of protection and favored treatment. Where the state concerns itself with the governance of territory, the corporation concerns itself with the extraction of resources from those territories, protected by state authority. In doing so, the state rigs the rules so as to facilitate corporate resource-extraction at the expense of nonstate and noncorporate actors: the tax code, property law, contract law, tort law, and criminal law are all structured to corporate advantage. The state has the incentive to do this because the revenue stream generated by the corporation is ultimately the revenue stream that pays for the state itself. The employment it generates serves to regulate the population, usually without the need for direct state intervention.

Given this setup, the two institutions both mirror each other and exist in a symbiotic relationship with each other. The state monopolizes force; the corporation monopolizes resource extraction, protected by the state's monopoly on force. The state enjoys immunity from prosecution for the way it deploys force; the corporation enjoys near-immunity from accountability for how it extracts resources from the commons. The state protects the corporation; the corporation feeds the state.

In short, the modern corporation governs us at precisely the point at which the state relinquishes control and precisely because it

[16] For a general account, see the entry for "Corporation" on Wikipedia: https://en.wikipedia.org/wiki/Corporation. For a more worked-out account, see Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Public Affairs, 2019). For a more libertarian-friendly take on the same theme, see Brink Lindsey and Steven M. Teles, *The Captured Economy: How the Powerful Enrich Themselves, Slow Down Growth, and Increase Inequality* (New York: Oxford University Press, 2017).

does. Counterintuitive as this may seem to some, the modern corporation, like the state, wields the power of life and death over us. This should be obvious in the case of the health care corporation, the private prison, or the mercenary security outfit, but as many experts have persuasively argued, it is increasingly true of the rest of the world as well. Just as the state outsources its power to corporations, the corporation, in turn, outsources its power to the computer-driven algorithm. Everything nowadays either is, or is driven by, such algorithms, so computerization becomes an expression of corporate power. While the corporation's main concern is the monetization of the world, not its destruction, its risk calculus is its own, not ours. It does not wantonly have to kill us to possess the right to impose its risk calculus on us, however ultimately lethal.[17] Thanks to limited liability, it does not have to apologize when it is wrong, either.

That brings us more directly to Big Data. Personal data is a resource to be extracted from the circumstances of private life. To understand how it is extracted, we have to focus on the right or relevant circumstances. The relevant ones are not (*pace* DeBrabander) those of retail commerce or private self-expression, but of genuine human necessity, those junctures in our lives where we appear to face options,

[17] On lethal threats arising from computer algorithms, see Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World* (New York: W.W. Norton, 2018). It's worth remembering that foreign threats and underworld actors—partly governmental, partly corporate—are as much part of "Big Data" as anything else. For useful discussion, see John P. Carlin and Garrett Graf, *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat* (New York: Public Affairs, 2018).

Since I first presented an earlier version of this essay, six of my company's hospital clients have been hit by major computer hacks, leading in at least two cases to extended suspensions on hospital admissions. See, e.g., Michael L. Diamond, "CentraState Healthcare Hack Stole Data from 617,000, Including Some Social Security Numbers," *Asbury Park Press* (New Jersey), February 11, 2023, accessed online at: https://www.app.com/story/money/business/consumer/2023/02/10/freehold-nj-centrastate-hacker-stole-625k-social-security-numbers/69892194007/.

but where one option bears down on our needs, crowding out the possibility or feasibility of choosing any of the others.[18]

Birth is the unchosen point of entry into data harvesting, followed in (very) roughly chronological order by health care, education, employment, finance, housing, insurance, and law. There is little or no way of avoiding these institutions in modern life and no way to avoid the relevant institutions' demands for personal data. Once engaged with them, and typically at the first encounter, an individual is deprived of any choice about whether to surrender her data, the purposes for which that data will be used, the methods that will be used in mining it, or the risks involved at any point in the process of harvesting, mining, sale, or exploitation of it.

The same mechanism is deployed in every case. An asymmetrically powerful actor, often a corporation but sometimes the state, exploits the necessity of a weaker actor, a person, demanding data as the price of meeting the weaker party's unavoidable human needs. Nominal consent is obtained for the transaction, but the consent in no plausible way qualifies as informed and is often given (for instance, in health care or law enforcement) under duress, even extreme, terrifying duress.

The transaction itself has no defined boundaries. The terms of service keep changing. The terms are often themselves incomprehensible and incoherent. Many uses of the data are not captured by the terms of the "contract" at all: they are simply *faits accompli*. Beyond this, the stronger parties to any interaction enjoy almost complete immunity in cases of breach. Indeed, most cases of breach go undetected. Contracts today are breached so often by the stronger party that the phenomenon becomes a kind of parody of Immanuel Kant's example of the lying promise in his *Grounding*: the world literally *becomes* the one in which the maxim of the lying promise

[18] I rely here partly on my personal experience of working in Big Data (see note 1 above) and partly on the work of O'Neill and Zuboff (cited in note 4 above).

has become universalized—and universalized by the most powerful agents in the world.[19]

Beyond *this*, the socio-political world is organized so as to reward innovation at getting around the terms of a contract, because the terms are themselves conceived as irritating side-constraints on the imperatives of unbounded optimization (think HIPAA in health care or FERPA in higher education).[20] In many contexts, "innovation" just *means* finding ways to maximize revenue by exploiting the ambiguities of contract or regulation. Innovation so conceived is rewarded with far greater enthusiasm than adherence to humdrum moral norms.

The surrender of personal data is part of the price of the ticket for just about anything we want in the modern world, be it a necessity, a luxury, or anything in between. Once surrendered, the data enters a cycle of mining, monetization, regulation, and punishment—in short, external control—far beyond the control of the individual consumer. Your personal sense of decorum, prudence, or reserve are utterly beside the point in this context. Even the dead are harvested, catalogued, investigated, and administered.

Given this, DeBrabander's focus on voluntary disclosure via the frivolities of online commerce and online acts of self-expression strikes me as misplaced. Even if we took those things entirely out of the equation, we would be left with a Data Leviathan staring down its subjects.

While your moral mileage may vary here, it is beside the *explanatory* point that we are all shopping online until we drop; posting our selfies, nudes, and private confessions on social media; or a little of both. Private self-indulgence does not really explain much about

---

[19] See Immanuel Kant, *Grounding for the Metaphysics of Morals*, 3rd ed., trans. James W. Ellington (Indianapolis, IN: Hackett Publishing, 1993), pp. 14–15, Ak. 402–3.

[20] HIPAA is the law that governs protected health information in the United States: the Health Insurance Accountability and Portability Act of 1996. FERPA is the law that governs educational records in the United States: the Family Educational Rights and Privacy Act of 1974.

our collective loss of privacy, which is another way of saying that contrary to DeBrabander, the desire for individual privacy (or self-expression) is—and never was—the problem.

3. Pushing Back Harder

I have, admittedly, focused on the *least* philosophical part of DeBrabander's argument. It might justifiably be wondered what turns on my doing so. Haven't I ignored what's more central to the book? In some ways, I have. However, the relevance of these initial explanatory concerns becomes clear if we now fast-forward past the philosophical arguments to DeBrabander's practical proposals.

In making his argument, DeBrabander canvasses the philosophical and legal literature in search of a serviceable definition of privacy and a defensible account of its value. Finding neither, he reaches the conclusion that there is none to be had. That, in turn, becomes the rationale for his suggestion that we change the subject. Instead of focusing on privacy, we ought to focus elsewhere; instead of defending privacy, we ought to defend other things.

I do not think DeBrabander's survey of the literature is comprehensive or charitable enough to justify the dismissal he offers. I also happen to disagree with many, if not most, of the strictly philosophical criticisms he makes about the value of privacy,[21] but let me leave those issues for others to discuss.

Suppose that we have done the best we can as far as philosophical accounts of privacy and come up short. Regardless, if my account is right, we have ample reason to regard Big Data's infringements on our privacy as a threat to us and ample motivation to push back. All we need to know is *that* they are threatening infringements, not *why*. We do not need a deep philosophical account of privacy to come to this conclusion, valuable as that might be.

DeBrabander is doubtless right that we lack a fully worked-out account of privacy in all of its details and subtleties, but we have a

[21] See note 7 above.

commonsense notion of what privacy is and a thin, generic account of its value. Like private property (and in much the same way), privacy serves a need to preserve and safeguard the separateness of persons. The details are no doubt contestable, but the fact itself is clear enough. The threat to privacy posed by Big Data is equally clear. We now have ample documentation of the scale and depth of Big Data's intrusions into our lives, so it is difficult to say that we are safe enough to change the subject and move on. The threat we face is as big as any we are ever likely to face.

Unless we really *know* that Big Data has won the game, that we are entirely out of ammunition, that all attempts at resistance will certainly be futile, we have undeniable reason for pushing back on Big Data. We need only know that it has awesome powers, is constrained from abusing them only in a purely formal way, is run by morally flawed mortals with ordinary vices, puts us at substantial risk (which it then covers up), and adopts a God-like posture toward us without having God's omnibenevolence. None of the good it does us can entirely offset or explain away these harms. Yes, it would be nice to have a theory that conceptualizes all of this in a neat and tidy way, but more important is to have the right weapons that protect one's space or that drive intruders out of it. The question is how to fashion them, not whether we need to.

DeBrabander writes as though privacy was a lost cause and as though the construction of an Arendt-inspired collectivist political order was somehow more feasible than the defense of privacy against Big Data. I do not see why—and I say that as someone *inside* the Beast. No particular political goal that DeBrabander favors is any more or less utopian than the task of reining in Big Data. Indeed, I do not see how anyone could construct the Arendtian order DeBrabander favors until they had *first* secured a measure of privacy. Even collectivist groups have to exclude those hostile to their aspirations in order to have the space to deliberate and act in a productive way. No one can function in an atmosphere of indiscriminate inclusion and total exposure. Contrary to DeBrabander, unless we draw some lines against Big Data and defend them, all bets are off for any higher political aspirations, Arendtian or otherwise.[22]

[22] The details of an activist strategy are worth discussing, but beyond my scope here. DeBrabander and I had a fruitful initial exchange on the topic at the event

Let me double back a bit, however. I am still enough of a philosopher to appreciate the strictly theoretical challenges DeBrabander has laid out. The concept of privacy is, as he rightly suggests, protean, equivocal, elusive, and sometimes over-hyped. Some of its applications are, as he rightly suggests, problematic and even pernicious. I share many of his concerns about the privatization of public life, particularly in the United States, as well as his aspirations toward an Aristotle-influenced, Arendt-inspired civic order. Though I disagree with much of it, I find *Life After Privacy* a bracing, stimulating read, one that helped re-focus my attention in salutary ways on the role and value of privacy in my own personal and professional life. It is not obvious how to reclaim democracy in a surveillance society, but reflection on DeBrabander's arguments has forced me to think hard about how it should be done.[23]

.

that gave rise to this symposium. One disagreement arises from the very different lessons we take from Zeynep Tufekci's *Twitter and Teargas* (note 4 above), which DeBrabander reads more pessimistically than I do.

[23] This symposium began life as an Author-Meets-Critics session at the Central Division Meeting of the American Philosophical Association in Denver, Colorado (February 24, 2023). Many thanks to Celeste Harvey (College of St Mary) for initiating, organizing, and chairing the session, and to the North American Society for Social Philosophy for sponsoring it. Thanks also to Shawn Klein and *Reason Papers* for agreeing to publish the conference proceedings. And thanks, of course, to Firmin DeBrabander, Paul Showler, and Ethan Hallerman for a fruitful exchange at the session itself.