Article

Anonymity Versus Privacy in a Control Society

Rachel Melis

ABSTRACT

Society is becoming increasingly more securitized with surveillance technologies having entered a phase of ubiquity, with their components built into many of our daily digital devices. The default state of tracking, monitoring, and recording has fundamentally changed our social and communicative environments. Through the lens of surveillance, everything we do and say can be potentially categorized as a "threat." Our technological devices become the means by which social control becomes informationalized. A common tool of resistance against these pervasive surveillance practices takes the form of arguing for greater privacy protections to be implemented through information privacy and data protection laws. However, beyond the complexity of the privacy discourse itself, there are diverse information environments not easily parsed by law where the tension between transparency and secrecy complicates privacy practices.

The main purpose of this article is conceptual. I consider what the practice of anonymity can offer that privacy does not. From a legal perspective, highlighting the nuances between privacy and anonymity helps us to understand the extent to which our speech and behaviors are becoming increasingly more constrained in the digital environment. In cultural and social contexts, privacy and anonymity often connote differing values; privacy is commonly considered a moral virtue, while anonymity is often maligned and associated with criminal or deviant behavior. In contrast to this understanding, I argue that anonymity should be reconsidered in light of the deterioration of privacy considerations as privacy practices are reframed as contractual resources that are co-opted by both the market and the state. Anonymity, more broadly construed as a mode of resistance to surveillance practices, allows for a more flexible, consistent, and collective means of ensuring civil liberties remain intact.

Melis, Rachel. "Anonymity Versus Privacy in a Control Society," in "Information/Control: Control in the Age of Post-Truth," eds. Stacy E. Wood, James Lowry, and Andrew J Lau. Special issue, *Journal of Critical Library and Information Studies* 2, no.2 (2019). DOI: 10.24242/jclis.v2i2.75.

ISSN: 2572-1364

INTRODUCTION

Society is becoming increasingly more securitized with surveillance technologies having entered a phase of ubiquity; they are built-in components of many of our daily technological devices. The default of tracking, monitoring, and recording has fundamentally changed our social and communicative environments. Through the lens of surveillance, everything we do and say can be potentially categorized as "threat." Through the use of our technologies, our lives have become transparent to both market players and law enforcement. Some resistance to this state of surveillance has taken the form of privacy protections implemented through information privacy law.

The main purpose of this article is conceptual. I consider the means by which privacy has become a matter of informationalized debate which revolves around the tension between a need for security and the need for freedom. I argue that privacy advocacy has not been successful in effecting a balance in the asymmetrical power relations that would lead to an empowering of the citizen (or consumer). Further, after considering what the practice of anonymity can offer that privacy does not, I argue that anonymity should be broadly construed as its own form of resistance to surveillance practices.

Even though they are understood as complementary concepts, in the legal realm privacy and anonymity differ in terms of the way they are perceived as resisting dominant views of what our information environments mean. From a legal perspective, highlighting the nuances between privacy practice and anonymous practice helps us to understand the extent to which our speech and behaviors become constrained, especially in the digital environment. In cultural and social contexts, privacy and anonymity can be seen to connote differing values; privacy is commonly considered a moral virtue, while anonymity is often maligned and associated with criminal or deviant behavior.

Notions of privacy and anonymity are commonly discussed in reference to the individual. With only a few exceptions, privacy is rarely studied on a collective scale, and anonymity is often considered only in relation to privacy protections. As privacy increasingly becomes a resource that is co-opted by both the market and the political sphere, anonymity allows for a more flexible, consistent, and collective means of ensuring civil liberties remain intact. In a culture of surveillance, privacy as it has been understood thus far, can no longer be invoked as feasible protection against an increasingly datafied existence.[1]

The "information revolution" as Viktor Mayer-Schönberger and Kenneth Cukier understand it, is one whereby data becomes the new currency. They believe that the

[1] Datafication is the effect of putting information into a "quantified format so it can be tabulated and analysed." Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform the Way We Live, Work, and Think* (Boston, MA: Houghton Mifflin Harcourt, 2013), 78.

move towards data knowledge and investment is both a benign and necessary outcome of our digital environments, and that the quantification of everything is inevitable.[2] In this view, the individual exercises economic control over their data, supporting and propping up the (arbitrary) numerical systems of value and worth, quantifying the self. The increasingly popular viewpoint that more data is always better, even necessary, or that more data helps explain, helps to *know*, is a byproduct of particular information ecologies we inhabit, and it is influenced by a rhetoric of transparency whose logic marks a process of visibility. But as Barnard-Wills argues, this process is also marked by radical contingency and it can change; the outcome is not inevitable as some would like to believe.[3] The defense against the process of datafication in the social and cultural spheres, however, cannot be an individual response; resistance must take place collectively if we strive for autonomy in our digital environment.

TRANSPARENCY AS GOVERNMENTALITY: VISIBILITY, DISCIPLINE, CONTROL

As the critical study of transparency gains momentum in the wave of e-government initiatives in the U.S., Canada, and Europe,[4] transparency warrants special attention in examining the ways in which openness, sharing, and the erosion of privacy are linked. Many government initiatives mobilize transparency to invoke access to open, available, unfettered and free information flows.[5] Transparency is the means by which people become informed, responsible and democratically enabled citizens. Transparency, it would follow, keeps governments accountable to their people as state processes become easier to understand and therefore, presumably, easier to act on. In reality, however, the call for transparency takes many forms and both expectations and outcomes vary according to circumstances and context.

The media theorist Felix Stalder suggests that studying the forms of transparency in terms of the production of social relationships reveals a political dynamic of empowerment and control.[6] He recognizes two paradigms of transparency that he sees operating simultaneously. Whereas the first paradigm sees transparency directed at

---

[2] Mayer-Schönberger and Cukier, *Big Data*, 73-97.

[3] David Barnard-Wills, "The Non-Consensual Hallucination: The Politics of Online Privacy," in *Media, Surveillance, and Identity,* ed. Andre Jansson and Miyase Christensen (New York: Peter Lang, 2014), 165-82.

[4] See, for example, the special issue on "Transparency" in the *European Journal of Social Theory* 18, no. 2 (2015).

[5] Hans Krouse Hansen, "Numerical Operations, Transparency Illusions and the Datafication of Governance," *European Journal of Social Theory* 18, no. 2 (2015): 203-20.

[6] Felix Stalder, "The Fight over Transparency: From a Hierarchical to a Horizontal Organization," *Open* 22 (2011): 8-22.

government in order to create accountability to the public, there is a second demand for transparency which comes from within neoliberal theory, and has as its goal the reduction of uncertainty. As such, this form of transparency is directed towards market participants whose transactional behavior can be tracked, collected, aggregated, and mobilized to predict future behavior and expectations, with the goal to reduce economic risk in an increasingly unstable and unpredictable global marketplace.[7] Transparency for those in power leads to accountability; for the public, however, it tends to lead to privacy violations, where the reduction of uncertainty requires free and open data flows.

The current and growing obsession with big data analytics, and the enthusiastic adoption of automated services, open social networking and sharing lead to additional, more profound considerations for the state of society, such as the efficacy of online civic engagement and discourse.[8] In open governance transparency (in terms of communication) defines the default relationship between individual and state. Technological tools for transparency, such as online databases of decontextualized government data, promise the speed, immediacy, and availability of information, but not the possibility of a dialogue concerning the information being released. Data alone does not make meaning and is not enough to "inform" citizens. This form of transparency, instead of allowing for the exchange of information, reduces political relations to mere transmission and effects.[9] Data divorced from dialogue becomes the reasoning function of the relationship between the state and the people.

Transparency in the service of reducing uncertainty functions inversely in the relationship between the state and the people. Data gathering and processing, while necessary for the functioning of the bureaucratic state, and commonly accepted as the regular work of governing populations, renders citizens visible in ways beyond the initial "work" that information processing does;[10] namely streamlining data-subjects, homogenizing the "other," and storing, aggregating, and linking data fragments that can later masquerade as knowledge. And society, it would seem, accepts this without question. Indeed, the so-called "big data revolution," and the hype surrounding it, is

---

[7] Stalder, "The Fight Over Transparency." See also Mark Andrejevic, "We Are All 'Lab Rats' Online," Interview with PBS. February 18, 2014. http://www.pbs.org/wgbh/pages/frontline/media/generation-like/mark-andrejevic-we-are-all-lab-rats-online/

[8] Antoinette Rouvroy, "The End(s) of Critique: Data Behaviourism Versus Due Process," in *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*, ed. Mireille Hildebrandt and Katja de Vries (Abingdon, Oxon: Routledge, 2013): 143-167.

[9] Mark Fenster, "Transparency in Search of a Theory," *European Journal of Social Theory* 18, no. 2 (2015): 154.

[10] Julie Cohen, *Configuring the Networked Self* (New Haven, CT: Yale University Press, 2012). See Chapter 5. See also Rouvroy, "The End(s) of Critique."

testament to a general acceptance and even enthusiastic adoption and perpetuation of data primacy.[11]

One immediate effect of the primacy of data in governing populations is recognizable in the shift from a disciplinary mode of population control based on panoptic visibility to softer, elusive, less visible modes of control. Without superseding discipline[12] (or disciplinary power) the work that big data does is both insidious and coercive, and depends in many ways on the evolution of disciplinary regimes.

Gilles Deleuze, in his short but influential essay of 1982, "Postscript on the Societies of Control," describes the control society as an extension of disciplinary modes of governance; here modulation is one of the salient features of a database-oriented, networked society. Deleuze's critique considers the power relations and affective capacities of ICTs and how they order and control our informational environments and influence our relations. The control society thesis can be understood as a continuum of both disciplinary and modular flows.[13]

Influenced by Deleuze, and following Michel Foucault's study of the ways in which disciplinary power works on the subject, David Savat argues that contemporary modulatory power has grave consequences for personal privacy in service of identity formation.[14] As a product of the control society, the informationalized "subject" is a *de*-identification. Datafication is a result of modulatory flows which fragment the individual into code. Savat argues that through simulation, sorting, and sampling, modulatory power functions through the "recognition of patterns," "anticipation of activity," "organization of antithesis," and "programming of code." [15] Where disciplinary power aims at constructing an individual, modular power fractures and splits the individual.[16]

Even though Savat's analysis does not focus on surveillance, it is the *culture* of surveillance, as a mode of real-time transparency, that remains the mechanistic environment of modulation which has serious consequences for the person under the law. From a Deleuzian control perspective, transparency regimes are also surveillance regimes; being reciprocal concepts, transparency and surveillance as regimes, share the goal of visibility. What form visibility takes, however, is determined by the sociotechnical

---

[11] "[Data] is the oil of the information economy," Mayer-Schönberger and Cukier, *Big Data*, 16.

[12] Stephen J. Collier, "Topologies of Power: Foucault's Analysis of Political Government Beyond Governmentality," *Theory, Culture & Society* 26, no. 6 (2009): 78-108.

[13] David Savat, *Uncoding the Digital: Technology, Subjectivity and Action in the Control Society* (New York: Palgrave Macmillan, 2013).

[14] David Savat, "Deleuze's Objectile: From Discipline to Modulation," in *Deleuze and New Technology*, ed. Mark Poster and David Savat (Edinburgh: Edinburgh University Press, 2009), 45-62.

[15] Savat, *Uncoding the Digital*.

[16] Savat, *Uncoding the Digital*.

relations that determine the context of data disclosure.[17] Modulatory flows can "create" or "predict" certain kinds of subjects for whom it becomes impossible to guarantee minimal rights and autonomy.

Antoinette Rouvroy, in her analysis of the effects of what she calls "algorithmic governmentality," describes the consequences that excessive information processing can have on the autonomy of the person,

> Understanding that the target of algorithmic governmentality is the *inactual*, *potential* dimensions of human existence, its dimensions of virtuality, the conditional mode of what people 'could' do, their potency or agency, allows us to understand what is at stake here: a deprivation which does not have as its opposite the possession of oneself.[18]

Targeting one's potential to act is both restrictive and prescriptive. Algorithmic governmentality is thus both disciplinary and modulatory as it plays out in big data projections. It is disciplinary because it restricts present conduct; modulatory because it prescribes the future *conduct of conduct*.[19] These fits and starts of the modulatory mode of power also create an environment or condition of constant interpellation.[20] Calling subjects into *discrete data positions* aids in the increasing decentering of attention at the individual level, while at the algorithmic level these discrete data attention points remain *invisible* to human detection and calculation.[21]

PRIVACY MODELS

When conceptualizing privacy across disciplines, we see a loose division of theories of privacy into either "rights-based" or "interests-based" approaches.[22] Theorists who model privacy as a right, understand privacy as a form of secrecy (surveillance model). They invoke a traditional mode of privacy as it pertains to the physical body, and in terms

---

[17] Deborah G. Johnson and Kent A. Wayland, "Surveillance and Transparency as Sociotechnical Systems of Accountability," in *Surveillance and Democracy*, ed. Kevin D. Haggerty and Minas Samatas (New York: Routledge-Cavendish, 2010): 19-33.

[18] Rouvroy, "The End(s) of Critique," 159.

[19] See Michel Foucault, "Governmentality," in *The Foucault Effect: Studies in Governmentality,* ed. G. Burchell, C. Gordon, and D. Murphy (Chicago, IL: University of Chicago Press, 1991) 87-104.

[20] Mark Poster, *The Second Media Age* (Cambridge, UK: Polity Press, 1995). See the chapter on "Databases as Discourse, or Electronic Interpellations."

[21] Mark Poster, *The Second Media Age*.

[22] Herman T. Tavani, "Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy," *Metaphilosophy* 38, no. 1 (2007): 1-22.

of intimacy associated with *confidentiality*. Theorists approaching privacy in terms of interests, understand privacy as a form of control that is often exercised in situations that involve data about a person. This contemporary meaning of privacy as it pertains to individual data protection is associated with *choice* (the capture model).[23] When we understand privacy to be more closely associated with secrecy, we are concerned with passive freedoms; freedom *from* invasion. As a passive measure, privacy is the "right to be left alone."[24] When we understand privacy to be more closely associated with control, we are concerned with active freedoms; freedom *to* choose (who gets access to data about us) and freedom *to* be (who we decide to be as represented by our data). This active measure of privacy entails identity, the "right to *be* oneself."[25] The latter view is prevalent in contemporary informational privacy discourse where personal information is data protected as property.[26] In this article, the term privacy, unless otherwise qualified is understood as *informational* privacy.[27]

Understanding privacy as a mechanism of control has less to do with the idea of access to the physical person (of the body, in public) and more to do with individual data ownership and controlling access to the data. Control in this case has less to do with secrecy and solitude, aspects of a traditional physical approach to privacy, and more to do with transactions. These transactions can be social interactions as in publicity and exposure in social networking or financial transactions in terms of consumer behavior. Though the role of choice is central to an interests-based understanding of privacy, choice becomes a problematic assumption when questions arise around how to define the kinds of information we can control, and how to determine how much control we can have in different environments. These questions, among others, become central to critiques of

---

[23] Philip Agre, "Surveillance and Capture: Two Models of Privacy," *Information Society* 10, no. 2 (1994), 101-127.

[24] This comes to us from the seminal ruling of Warren and Brandeis, "The Right to Privacy," *Harvard Law Review* 193, no. 4 (1890): 193-220.

[25] Luciano Floridi, "Four Challenges for a Theory of Informational Privacy," *Ethics and Information Technology* 8 (2006): 109-19. See also Antoinette Rouvroy and Yves Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy," in *Reinventing Data Protection?* ed. Poullet Gutwirth, De Hert, de Terwangne and Nouwt (Dordecht: Springer, 2009), 45-76.

[26] Christian Fuchs, "Towards an Alternative Concept of Privacy," *Journal of Information, Communication & Ethics in Society* 9, no. 4 (2011): 220-37; Julie Cohen, *Configuring the Networked Self* (New Haven, CT: Yale University Press, 2012).

[27] Ronald J. Krotoszynski, *Privacy Revisited: A Global Perspective on the Right to Be Forgotten* (London: Oxford University Press, 2016): 48. There are three modes of privacy that are categorized for the purposes of legal and constitutional protection: personal, territorial, and informational.

privacy.[28] The prevailing view of personal information as property is responsible for the push towards greater data availability and collection, instrumentalized through privacy notices demanding consent.[29]

Privacy notices are generally ineffective in communicating the possible risks to individuals' privacy. A number of experiments conducted by Alessandro Acquisti and his colleagues have brought to light some of the prevailing reasons for the apparent privacy paradox.[30] In terms of decision-making, cognitive biases affect the interpretation and effective understanding of privacy notices and agreements and lead to actions that would otherwise contradict the beliefs or intentions of the participants. Furthermore, "notice and consent" systems are fraught with inconsistencies. Research studies have demonstrated that the system is a poor mechanism of controlled access if the goal is to empower the individual user in his or her decisional framework.[31] Rather, because these systems are incapable of addressing future uses of personal data, they cannot adequately adjust for potential consequences. As Mayer-Schönberger and Cukier argue, when the value of data is more likely in its secondary use and in perpetuity, this ostensible privacy control mechanism is no longer suited to the *potentiality* of data use, ownership, and sharing.[32] And as Solove believes, "consent is virtually meaningless in many contexts. When people give consent, they must often consent to a total surrender of control over their information."[33] In other words, consent equates to a loss of control, the complete inverse of the intended consequences of privacy enhancing policies. The ostensible effect of these types of systems regulating our online informational transactions is the illusion of power or control (we "willingly" agree to the terms of service) while real empowerment is undermined by the nature of the contractual form.

Studying the relationship between consumer attitudes towards privacy and data behavior further reveals a form of responsibilization determining the relationship

---

[28] Tavani, "Philosophical Theories," 7.

[29] This process has been accelerated with the European Union's General Data Protection Directive (GDPR) which requires that all websites collecting data or tracking users in the EU display a notice detailing the collection practice and subsequent use of the data. In most cases, if the user does not consent to the practices, there is no moving forward through the site.

[30] Allessandro Acquisti, Idris Adjerid, and Laura Brandimarte, "Gone in 15 Seconds: The Limits of Privacy Transparency and Control," *IEEE Security & Privacy* (July/August 2013): 72-74.

[31] Solon Barocas and Helen Nissenbaum, "On Notice: The Trouble with Notice and Consent," *Proceedings of the Engaging Data Forum on the Application and Management of Personal Information* (2009). http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf

[32] Mayer-Schönberger and Cukier, *Big Data*.

[33] Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy," *Stanford Law Review* 53, no. 6 (2001): 1427.

between the "data subject" or "data publics" and data disclosure practices.[34] Elements of control, whether illusory or real, fail to account for the dangers and risk of data disclosure which implicitly puts the onus of privacy expectations, protections, and accountability on the individual rather than on the organizations collecting the data.[35] In data gathering, the whole becomes greater than its parts. Information abuses are identifiable and take on greater importance when viewed from a collective perspective. The ownership of personal information and thus the right to control it, as in decide to whom and when one may sell or trade their own information, creates an artificially commodified value for personal information.

Modelling privacy is one way of getting at the discourse of power and issues of control. If privacy functions as a commodity, an interests-based model is responsible for the legislation of privacy as a data-driven positive freedom to control who owns the information and how it is used. In this case, the person trades or sells personal information in order to access a service more efficiently or to gain an advantage otherwise withheld from those who are less willing to sell their data. If privacy functions as a right to be "left alone" (or remain unseen), this leads to a secrecy or rights-based model for legislating privacy as a negative freedom where the burden of proof lies on defining or recognizing "harm."[36] Confidentiality and trust would figure prominently in this approach to privacy. Nevertheless, the above understandings of privacy take the individual as the level of analysis; neither of these regulatory approaches consider the benefits or effects of privacy breaches to society as a whole.

We must recognize the importance of a collective approach to the protection of privacy, instead of focusing on individual interests.[37] This requires us to concern ourselves with blanket data collection and processing to the extent that a breach or invasion constitutes not only a breach of individual privacy, but involves unlimited *other* individuals. Much commercial and publicly available social data collection exists in relation to multiple individuals.[38] In this context, one's privacy control settings do nothing to protect oneself from a friend's or another's more lax or open privacy settings.[39]

It is in this complexity that I would suggest anonymity as the mode of analysis in group information sharing, trust, control, and power relations. Not to replace the concept

---

[34] Clare Birchall, "'Data.gov-in-a-box': Delimiting Transparency," *European Journal of Social Theory* 18, no. 2 (2015): 190-91.

[35] Clare Birchall, "'Data.gov-in-a-box.'"

[36] Philip Agre calls these the "surveillance" and "capture" models of privacy.

[37] Cohen, *Configuring*, 8.

[38] Social networks such as Facebook are the obvious case in point.

[39] David Wills and Stuart Reeves, "Facebook as a Political Weapon: Information in Social Networks," *British Politics* 4, no. 2 (2009): 265-281. See also Felix Stadler, "Autonomy and Control in the Era of Post-Privacy," *Notes & Nodes* (blog), June 14, 2010, http://felix.openflows.com/node/143.

of privacy, nor to minimize the work that privacy advocacy does, but to reorient and shift the emphasis from the individual to the collective by focusing on the relational aspects of anonymity in order to demonstrate how personal data control is illusory, and to trouble the belief that privacy protection can control the flow of information.

PHILOSOPHY OF ANONYMITY

Anonymity is generally understood on a spectrum of controlled visibility from one end of identifiability to the other end of unknowability. Although in common parlance, anonymity closely aligns with secrecy and privacy,[40] anonymity can be understood as a means of undermining the transparency imperative more effectively when exercised and mobilized collectively. Anonymity is a tool of resistance to visibility and trackability, without compromising participatory communication, because it can allow for a form of presence that may be seen but not datafied. As such, anonymity is politicized because it reverses data responsibilization by deliberately denying the preemptive expectation to *share* (here as an active role) data. Anonymity plays a subtle but differentiating role in the struggle for privacy against data mining and tracking. Anonymity abides by the dictum "information wants to be free," by respecting access *and* rejecting the information market; through practices of anonymity, the tension between making information available and protecting one's privacy is alleviated and the incentive to commodify personal information is reduced, if not wholly eliminated.

Data exists. As soon as we do anything digitally, we generate data. These data traces we generate can be intentional or unintentional. They can be personally identifiable or anonymous. However, we can approach this anonymity in various ways. It is useful to consider anonymous practices in terms of the relations established between bodies and machines. Anonymity can mean nonidentifiability, approached as the "noncoordinatability of traits,"[41] untraceability,[42] or unreachability.[43] Depending on the approach, civil liberties can be impacted in different ways.

---

[40] Julie Ponesse, "Navigating the Unknown: Towards a Positive Conception of Anonymity," *The Southern Journal of Philosophy* 51, no. 3 (2013): 324.

[41] Kathleen A. Wallace, "Anonymity," *Ethics and Information Technology* 1 (1999): 23-35.

[42] Michael A. Froomkin, "Anonymity in the Balance," in *Digital Anonymity and the Law: Tensions and Dimensions,* ed. C. Nicoll, J.E.J. Prins, and M.J.M. van Dellen (The Hague: T.M.C. Asser Press, 2003).

[43] Helen Nissenbaum, "The Meaning of Anonymity in an Information Age," *The Information Society* 15, no. 2 (1999): 141-144.

Anonymity is variously associated with privacy as its enabler[44] or as its nemesis,[45] but often the two are conceived of in synonymous ways. In some cases, when the discourse surrounds freedom of speech and liberties online, they are used interchangeably. Anonymity can either be understood as a means of enabling privacy or as a means of undermining it; the former if anonymity is mobilized in a technological form, and the latter if privacy is understood in its ontological sense as identity.[46]

But anonymity is not equal to privacy. While privacy is about connections and the rules of conduct that oversee those connections, anonymity is about disconnecting.[47] According to Julie Ponesse, anonymity does not require complete unknowability, but only levels of dissociation. It is dissociability that Ponesse argues defines anonymity relations. She suggests, "What distinguishes anonymity relations from privacy relations, therefore, is a difference in *the way* information about a person fails to be known."[48] Thus, anonymity can regulate the circulation of information in a digital environment despite control (or consent) mechanisms that are put into place by contractual privacy agreements.

The economics of privacy demonstrate that interests and rewards are enough to ensure that people give up their data. From this starting point, anonymizing technologies such as Tor, Tails, and Signal[49] would interfere with the prevailing economic logic. They take as their conceptual starting point that data *need not* be tracked and collected,[50] and the continuing debates surrounding the efficacy of their design and the social value of their use is a smoke screen intended to distract away from the real threat to information stake-holders and those who would stand to benefit financially from the absence of these technologies. Nevertheless, the recent rising popularity of anonymizing technologies

---

[44] Robert Bodle, "The Ethics of Online Anonymity or Zuckerberg vs. 'Moot','' *ACM SIGCAS Computers and Society* 43, no. 1 (2013): 22-35. See also Ian Kerr and Jennifer Barrigar, "Privacy, Identity, Anonymity," in *Routledge Handbook of Surveillance Studies*, ed. Kirstie Ball, Kevin D. Haggerty, and David Lyon (London; New York: Routledge, 2012), 386-94.

[45] Anonymity must be separated from privacy in this case if privacy is the right to *be* as Floridi argues, for example.

[46] Floridi, "Four Challenges."

[47] Ponesse, "Navigating the Unknown."

[48] Ponesse, "Navigating the Unknown," 330.

[49] The Tor Project: https://www.torproject.org/; Tails: https://tails.boum.org/; Signal: https://signal.org/.

[50] Herbert Burkert, "Privacy-Enhancing Technologies: Typology, Critique, Vision," in *Technology and Privacy: The New Landscape*, ed. Philip Agre and Marc Rotenberg (Cambridge, MA: MIT Press, 1997), 125-142.

indicates that there is a changing cultural perception of anonymity online, and that it has become an aspect of online communication that is worth fighting to keep.[51]

However, the point to stress here is that there are dangers to normalizing the idea that personal data is a commodity, and a continued focus on privacy as a means of controlling access to personal data does very little in addressing the collective concerns of data disclosure. Practicing anonymity even on an individual basis addresses these concerns more generally and thus works towards a collective solution.

In summary, the access and control approach in informational privacy discourse is a common, but insufficient strategy to respond to the state of personal data collection and use today. The access-and-control approach begins with the assumption that there is information about us always already circulating with or without our consent or awareness, and that as consumers we should be able to control who accesses it and under what conditions. If, however, we want to critique the mechanisms of information circulation online we have to begin with the opposite assumption, the unavailability of personal information, and reconsider how the value of privacy can be seen as a public good for which we can be collectively responsible.[52] With few exceptions, questioning the necessity of personal data collection as an inevitability itself is rare within the literature; the initial collection of data, and the assumption to default tracking and recording of online movement and behavior seems not to be challenged by many privacy advocates.[53]

ANONYMITY AND LAW

In the early days of the Internet, anonymity was hard-wired into the network architecture and protocols.[54] By the end of the twentieth century, growing market pressures to identify Internet users in order to target them with advertising created an environment whereby anonymous participation was no longer acceptable in an economic framework.

---

[51] Angus Bancroft and Peter Scott Reid, "Challenging the Techno-Politics of Anonymity: The Case of Cryptomarket Users," *Information, Communication & Society* 20, no. 4 (2017): 497-512.

[52] Zbigniew Kwecka, William Buchanan, Burkhard Schafer, and Judith Rauhofer, "'I Am Spartacus': Privacy Enhancing Technologies, Collaborative Obfuscation and Privacy as A Public Good," *Artificial Intelligence Law* 22 (2014): 113-139.

[53] As long as Policies and Terms and Conditions are present and intact. Some exceptions to this trend can be found in Daniel J. Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," *San Diego Law Review* 44, no. 4 (2007): 745-72. See also: Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill, NC: The University of North Carolina Press, 2009) and Paul M. Schwartz, "Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices," *Wisconsin Law Review* 743 (2000): 744–788.

[54] Cole Stryker, *Hacking the Future: Privacy, Identity, and Anonymity on the Web* (New York, London: Overlook Duckworth, 2012).

Therefore, anonymity became more closely associated with deviance, and came to represent the harmful elements of the Internet in the form of the Dark Web.[55] The shift in associating anonymity with criminality, rather than with Internet freedoms, both in design and in execution, has served to marginalize anonymous technologies and obscure the positive aspects of anonymity previously associated with free speech. Today, however, anonymity is quickly becoming more and more difficult, if not impossible, for pretty much everyone. The reasons for this are social, economic, and political.

In a social context, a compulsion to interact is altering subjectivity. Constant participation on social platforms begins to replace more introspective and self-reflexive methods of identity creation. Felix Stalder argues that the postmodern subjectivity is based on interaction instead of introspection. In his interpretation, privacy entails a form of disconnection in a context in which "sociability is tenuous and needs to be actively maintained all of the time."[56] In my view, this kind of sociability sounds more like a threat than a promise. Though Stalder's analysis is convincing and sound, his conclusion lacks a critical understanding of sociality as something more than just the default of our technological communicative capacities. In his view, privacy reduces to non-participation which then signals disconnection, isolation, and loneliness; even worse, irrelevance. This is not the first time we have been warned of the "danger" of disconnecting.[57] Threats of becoming untethered from the network demonstrate exactly the rhetoric of both markets and states whose interests remain dependent on the connectivity of subjectivities whose continued belief, or acceptance that participation determines identity animates the control society thesis.

In terms of economics, anonymity gets in the way of profit. The move towards Persistent User Identities (PUIs), spearheaded by Google and Facebook, is indicative of the progressive and aggressive demand for continuous uninterrupted data flows as a means of generating revenue. The "identity" which follows you online (your "data double") and which connects your various browsing sessions and access accounts, stands in for all of your behavior and activities online. Naming and persistent identities online translate into great financial gain through personalization and target marketing, loyalty

---

[55] Eric Jardine, "The Dark Web Dilemma: Tor, Anonymity, and Online Policing," Global Commission on Internet Governance Paper Series (Waterloo, Canada and London, UK: CIGI and Chatham House, September 2015).

[56] Felix Stadler, "Autonomy and Control in the Era of Post-Privacy," *Notes & Nodes* (blog), June 14, 2010, http://felix.openflows.com/node/143.

[57] Laura Portwood-Stacer, "Media Refusal and Conspicuous Non-Consumption: The Performative and Political Dimensions of Facebook Abstention," *New Media & Society* 15, no. 7 (2012): 1041-1057.

accounts, and user product reviews. “Synergistic technologies” make online and offline links for tracking by both government and the private sector.[58]

Seen through the lens of cyber-security, anonymity does not fare well. The political argument here is in order to keep a country’s information infrastructure safe, there must be total control over access points and communications. What the Snowden files revealed was not only the general security in place to safeguard against the threats of terrorist activities, but also the indiscriminate tracking and capture of swaths of citizen data without warrant or other legal sanctions.[59] The discourse of security makes it dangerous to pursue anonymity as all levels of the law work towards identifying and profiling individuals in a preemptive strategy to secure future data requirements. Connected to market-based incentives, identification and profiling not only makes money, but ostensibly increases the feeling of security. In Canada, though there is no equivalent blanket provision for government eavesdropping, there are growing concerns with cross-border information sharing, and data legislation is slow in progressing beyond market-centered contract-law.[60]

Transactional data accounts for most of the relational transactions online between consumer and organization. Indeed, it would not be a difficult argument to mount that any information exchanged for service involves a transactional expectation. Because of this, much privacy legislation is geared towards business and consumer relations. In Canada, transactional data are covered by PIPEDA, and in Europe under the General Data Protection Regulation (GDPR).[61] That it involves in many cases, egregious amounts of information extraction completely unnecessary to the validity and verity of the transaction at hand, is rarely analyzed or challenged.

Definitionally, anonymity and privacy are complementary concepts. However, in terms of information policy, the two concepts function very differently. Privacy legislation in Canada and in the United States in particular, has been slow to adapt to the increase in data collection, processing, storage, and sharing.[62] In some cases, as in the European response, modified policies have been enacted to deal with personal information, data directives and protections in an attempt to legislate the use of information after it has

---

[58] Michael A. Froomkin, “From Anonymity to Identification,” *Journal of Self-Regulation and Regulation* 1 (2015): 120-138.

[59] Via the U.S Patriot Act (2001).

[60] In Canada, Bill C-51, The Anti-terrorism Act (2015) was superseded by Bill C-59 The Canadian National Security Act with some of the more privacy-reducing clauses amended. See Michael Geist’s critique online, http://www.michaelgeist.ca/2017/06/billc59/.

[61] See also https://epic.org/ for the United States. For Europe, https://www.eugdpr.org/; The GDPR became law in 2016, but only just came into effect in May 2018.

[62] Dörr, Dieter and Russell L. Weaver, eds. *The Right to Privacy in the Light of Media Convergence: Perspectives from Three Continents* (Berlin and Boston, MA: DeGruyter, 2012), 1-30.

already been collected. So it is data protection legislation in Europe which governs personal data use and storage, though it does not address the context surrounding the appropriateness of data collection to begin with.[63] In Canada, while PIPEDA and the Privacy Act cover different modes of data and information use, they do not address or question the presumption of initial data collection itself.[64]

In the United States, anonymity is generally dealt with under the existing privacy legislation which is determined under the First Amendment and the Fourth Amendment.[65] In Canada, there is no general right to anonymity,[66] though the Supreme Court of Canada has recognized the importance of anonymity as a manifestation of informational privacy especially as it relates to online activity.[67] In the European Union, privacy and data protection rights are covered under the European Convention of Human Rights and the Charter of Fundamental Rights of the European Union.[68] Importantly, in 2006 the European Union instituted the "right to be forgotten" which gives citizens the ability to contest the existence of information about themselves and demand the removal and deletion of pictures, videos, and other information from the Web so that search engines will no longer be able to find it.[69]

---

[63] Antoinette Rouvroy and Yves Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy," in *Reinventing Data Protection?* eds. Poullet Gutwirth, De Hert, de Terwangne and Nouwt (Dordecht, Netherlands: Springer, 2009), 45-76. The GDPR does now include some regulation concerning "data minimization" outlined in Article 23.

[64] European Commission data protection reform: "The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business. The data protection reform is a key enabler of the Digital Single Market which the Commission has prioritised. The reform will allow European citizens and businesses to fully benefit from the digital economy." (http://ec.europa.eu/justice/data-protection/index_en.htm); In the United States: http://www.informationshield.com/usprivacylaws.html; In Canada: "Office of the Privacy Commissioner of Canada" http://www.priv.gc.ca

[65] Anita L. Allen, "First Amendment Privacy and the Battle for Progressively Liberal Social Change," *University of Pennsylvania Journal of Constitutional Law*, Symposium: Privacy Jurisprudence as an Instrument of Social Change, 14, no. 4 (March 2012): 885–927.

[66] Carole Lucock and Katie Black, "Anonymity and the Law in Canada," in *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*, ed. Ian Kerr, Carole Lucock, and Valerie Steeves (Oxford, UK: Oxford University Press, 2009), 465-484.

[67] See Krotoszynski, *Privacy Revisited*, on page 41 referring to the 2012 case of *R. v. Spencer.*

[68] Antoinette Rouvroy, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence," *Studies in Ethics, Law, and Technology* 2, no. 1 (2008): Article 3.

[69] Rolf Weber, "The Right to Be Forgotten: More Than a Pandora's Box?" *Journal of Intellectual Property, Information Technology and E-Commerce Law* 2 (2011): 120-130. See also David Lindsay, "The 'Right to be Forgotten' in European Data Protection Law," in *Emerging*

PRIVACY VERSUS ANONYMITY

My contention in this article has been that neither privacy notices nor data-protection legislation alone adequately address the impelling forces at work in the system of data collection, processing, storage and reuse. Beyond policy, privacy and anonymity, when considered from sociological and cultural perspectives, are represented differently dependent on the context. The choice to reveal or to conceal personal information sometimes is a false choice. If the choice is not to reveal, and not to share, that is, if the preference is to withhold requested information, this may result in a block to services that would otherwise be construed as "free." To *choose* to reveal information under these circumstances amounts to a kind of "illusion of voluntariness."[70]

The main difference between privacy and anonymity is this: Privacy presumes an element of secrecy; Anonymity does not. This might not be immediately obvious, but let me attempt an explanation by way of example. X's communication in order to be private must be altered in such a way that something is withheld, most often a name or ID that would otherwise link that communication back to something or someone in real life. This communication is not meant for everyone. It is not meant to be "public" or publicized. A private communication implies trust, secrecy, and control (as confidentiality). X's communication in order to be anonymous does not presume any of the above (agent-enhancing) requirements. For example, to be anonymous, X does not necessarily *withhold* anything. Rather, there is an absence of something active around X's communication (ie: there are no identifying trackers, monitors, or surveillors, beacons, cookies, etc.) Without an ecosystem of watchability and trackability, we find ourselves back in the early days of the Internet.

Anonymous practices are dangerous to those in power. They are threatening to the state because they undermine the state's ability to control its population. They are threatening to law enforcement because they impede their ability to manage risk and criminality. Anonymous technologies may impede policing's ability to recognize and name potential criminals; to categorize and control minority populations such as the poor, and the deviants, the ones who find themselves on the fringes of the information marketplace. Conceptually, anonymity extends the privilege of invisibility beyond the domain of the elite and the powerful by democratizing identity protections. But anonymity adds additional measures of freedom; the freedom of mobility, of speech, of association—basic liberties that Western democracies profess to make available to all.

Challenges in Privacy Law: Comparative Perspectives, eds. Normann Witzleb, David Lindsay, Moira Paterson, and Sharon (Cambridge, UK: Cambridge University Press, 2014), 290-337. The EU's expanded GDPR has this now firmly entrenched in its legislation.

[70] Simon Davies, "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity," in *Technology and Privacy: The New Landscape,* eds. Philip E. Agre and Marc Rotenberg (Cambridge, MA: MIT Press, 1997), 143-165.

Opting for anonymity means understanding what visibility can and cannot accomplish. This involves accepting that some contexts make us data vulnerable and some contexts make us data powerful,[71] but what determines these contexts are frequently beyond the scope of individual users' ability to identify.

SUMMARY

In this section, I summarize the discussion above by highlighting two considerations that arise from the privacy defense which ultimately prove to be ineffective in responding to surveillance culture. The first consideration has to do with the conflation of privacy with data protection, the second has to do with the dependence on notice and consent to resist datafication practices.

1) Privacy is not the same as data-protection

Despite the fact that many privacy theorists tend to conceptualize informational privacy in terms of data protection, the two need to be kept discrete if we are to envision a revaluation of privacy in the networked age.[72] Informational privacy, as we have understood it thus far in the digital age *already* entails giving up control of your personal information, whether it is through voluntary institutional trust relationships, or as commodified transactions.

Traditionally, privacy has been understood as harm reduction and, therefore, defined in terms of negative freedoms (to be left alone). Before the extension of ICTs into every facet of our daily lives, there was no universal access that was generally assumed through the use of our technologies. Surveillance technologies both enable access to services and communication networks, and disable or block access to users from outside visibility. Anonymous technologies do not presume, or give the illusion, that your personal information is *not there*. What they do is make it very difficult or impossible to identify or trace you. This may be the best means of resistance unless we collectively decide to actively *stop* collecting and storing data. But as we understand in the era of Big Data, this seems to be precisely what has captured the attention of both government and the private sector. It seems an impossible request.

---

[71] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, CA: Stanford Law Books, 2009). See also Robert Bodle, "Regimes of Sharing: Open APIs, Interoperability, and Facebook," *Information, Communication & Society* 14, no. 3 (2011): 320-337.

[72] Raphaël Gellert and Serge Gutwirth, "Beyond Accountability, the Return to Privacy?" in *Managing Privacy through Accountability*, ed. Daniel Guagnin et al. (London, UK: Palgrave Macmillan UK, 2012), 261–283, https://doi.org/10.1057/9781137032225_13. See also Rouvroy and Poullet, "The Right to Informational Self-Determination."

2) Privacy cannot be a control technology

In our constant interactions online, consent cannot be said to be truly freely given as a consequence of choice. Despite what many privacy advocates argue, control does not describe the relationship that we have with data. Data is produced, generated (leaves traces), mixed, and mobile; wherever we are, wherever we go, we leave digital traces. Data is the offspring of our relationship with digital technologies. It is not our property, and we do not control access to it. Viewing personal information as property to be controlled by the individual allows for the commodification of information and a continued illusory view that we can ultimately decide who has access on an individual and case by case basis. The flaw in this position becomes clear when considering the outcome of this mindset will affect society collectively, and those who otherwise cannot afford to be in control of their data would be disadvantaged in other aspects of our social and cultural existence.[73]

There are also ethical and social implications to consider. The choice of whether or not to share personal information affects not just the individual but those associated with and informationally tethered to her through the various networks of which she is a part. One's personal choice becomes extended to one's choosing *for another* by virtue of the network. In other contexts, such as service contracts, one's choice becomes a false choice; an "illusion of voluntariness."[74] Once a critical mass of participation is reached, there is no opting out of the system for those who choose not to participate.

The legal protection of a "reasonable expectation" of privacy has been eroded by surveillance technologies, being slowly replaced by a spectrum of general discomfort with constant visibility. This normalization of surveillance has allowed for the continuing encroachment on public space by surveillance technologies in the interests of security and safety. The promises of safety and security make it difficult to argue for the right not to be watched.

The culture of transparency affects certain behaviors and represents a shift in thinking that living in an entirely open society is both welcome and desirable. In order to sustain this argument, the privacy debate is simplified by reducing complex social, market, and state power dynamics to a struggle between the figure of the "citizen" and the bureaucratic apparatus in an effort to strike a balance between autonomy and control.

Ideally, transparency in this context will lead to the power to contest the information that is connected to us. The information presented reflects us as individuals

---

[73] Schwartz, "Beyond Lessig's Code."

[74] Davies, "Re-Engineering." See also the recent privacy studies that have been conducted by Queens University and by Ipsis whose findings point to the wide acceptance that choice is effectively eliminated. Elia Zureik, Lynda Harling Stalker, Emily Smith, David Lyon, and Yolande Chan, *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons* (Montreal & Kingston, Canada: McGill-Queen's University Press, 2010).

in a social network of communication that must be understood as relational and therefore not subject to one's individual control. In some ways this demand has been partially met in the "right to be forgotten" legislation, part of the European GDPR.[75]

CONCLUSION

Theories of privacy which take into consideration the psychological, behavioral, legal, and philosophical aspects of sociality will reflect the challenges mounted by the individualistic responses to privacy harms. A collective understanding of privacy as anonymous relations may provoke a more nuanced debate about the nature of informational transactions both online and offline.

It is too soon yet to do away with the legal framework that upholds at least some understanding of personal privacy. I am inclined to argue for the "rule of law" as a general guide in terms of data collection, use, and storage, with the balanced use of anonymizing technologies. This practice must be implemented with restrictions on second use, as well as confidentiality, in consumer business transactions and health transactions. The problem with teasing out all of these informational levels is that right now, they are all for the most part equally treated as types of data informing types of transactions. Arguing for more anonymity does not preclude a strong commitment to privacy. The balance to be sought is not between individual autonomy and control—but between the power to collect personal information and the power to withhold personal information.

The main purpose of this article was to illustrate the ways in which privacy has been distorted and misapplied in the discourse of Internet freedom and the culture of surveillance that is quickly normalizing constant visibility and trackability. In response, I have illustrated the ways in which anonymity can be conceptualized as a value in order to shift the perception that privacy is the only means of defense against surveillance enclosures. I argued that informational privacy within the context of surveillance as I outlined it in terms of practice, is not successful in effecting a balance in asymmetrical power relations if our goal is to empower citizens and consumers. If we believe that privacy is about power,[76] the current path to challenging the power of corporate and state datafication has been unsuccessful, and privacy in this context has arguably become yet another commodified resource for both the market and the state.

The privacy paradox and the expository nature of today's society seems to signal a reduced interest in the efficacy or utility of privacy except when considered as a method of controlling and capitalizing on one's data. If privacy is understood as the right to trade

---

[75] Weber, "The Right to be Forgotten;" Lindsay, "The 'Right to be Forgotten'."

[76] As Lisa Austin has insisted in "Enough About Me: Why Privacy is About Power, not Consent (or Harm)," in *A World Without Privacy: What Law Can and Should Do?* ed. Austin Sarat (Cambridge, UK: Cambridge University Press, 2015), 131-89.

personal information for goods and services, this individual right works against a social or collective benefit of equivalent consideration of informational privacy. This in turn perpetuates and strengthens the practices of corporate and commercial enterprises to withhold the same services and goods from those who would not give up, "trade," or "sell" their information.

By consenting we are presently sanctioning an environment where privilege and economic affluence continues to be rewarded, and non-participation is seen as deviant.[77] If we continue in this vein, we normalize the trading of information for goods, services, efficiency and social connectedness. Thus, the withholding or *not* sharing of information will come with an added cost either financially or socially to those who are underprivileged or willingly resistant to the transparency regime; either they end up paying too much for goods and services, or they lose the privilege to access what could be otherwise open and accessible to all. In this case, it is not a matter of infrastructure that gets in the way, but personal choice and autonomy that ultimately determines the course of the social response. Whereas infrastructure can be affected both by design[78] and legislation at the policy level, this form of social control can lead to more alarming and unexpected consequences.

The defense of privacy seems to be ill-equipped to protect the autonomous agent from an excess of data collection. Historically, privacy rights have been invoked to defend the individual (to a greater or lesser degree depending on the approach and rationale taken) by invoking, or affirming, the values of a neoliberal economic system grounded in ownership and control of data. However, a deepening and pervasive surveillance culture has made an individual approach untenable. In order to effectively respond to and critique the cultural and social acceptance of a post-privacy information ecosystem, I maintain that a shift in thinking away from the individual towards a collective understanding of the value of privacy will set the stage for a rethinking of the value of anonymity.

Anonymous relationships, whether human-to-human, human-to-machine, or machine-to-machine (in terms of algorithms and protocols), may be better suited to defend the individual and society against an increasingly controlling information ecosystem. In addition to strengthening privacy protections, presently in the form of data accountability, I have suggested that both a technical means of attaining anonymity and a legal means of protecting the right to anonymous expression is necessary for cascading protections of civil liberties. The social value of anonymity requires greater consideration

---

[77] Michalis Lianos, "Periopticon: Control Beyond Freedom and Coercion—And Two Possible Advancements in the Social Sciences," in *Surveillance and Democracy*, ed. Michael Haggerty and Georgos Samatas (New York: Routledge, 2010), 69-88.

[78] Anne Cavoukian, "Privacy by Design: The Definitive Workshop. A Foreword by Ann Cavoukian, Ph.D.," *Identity in the Information Society* 3, no. 2 (2010): 247-251.

as I believe a collective valuation of anonymity is one viable means of safeguarding autonomy and ensuring communicative freedoms, without becoming too transparent.

BIBLIOGRAPHY

Acquisti, Allessandro, Idris Adjerid, and Laura Brandimarte. "Gone in 15 Seconds: The Limits of Privacy Transparency and Control." *IEEE Security & Privacy* (July/August 2013): 72-74.

Agre, Philip. "Surveillance and Capture: Two Models of Privacy." *Information Society* 10, no. 2 (1994): 101-127.

Allen, Anita L. "First Amendment Privacy and the Battle for Progressively Liberal Social Change." *University of Pennsylvania Journal of Constitutional Law*, Symposium: Privacy Jurisprudence as an Instrument of Social Change, 14, no. 4 (March 2012): 885-927.

Andrejevic, Mark. "We Are All 'Lab Rats' Online." Interview with PBS. (February 18, 2014). http://www.pbs.org/wgbh/pages/frontline/media/generation-like/mark-andrejevic-we-are-all-lab-rats-online/.

Austin, Lisa. "Enough About Me: Why Privacy is About Power, not Consent (or Harm)." In *A World Without Privacy: What Law Can and Should Do?* edited by Austin Sarat, 131-189. Cambridge, UK: Cambridge University Press, 2015.

Bancroft, Angus and Peter Scott Reid. "Challenging the Techno-Politics of Anonymity: The Case of Cryptomarket Users." *Information, Communication & Society* 20, no. 4 (2017): 497-512.

Barnard-Wills, David. "The Non-Consensual Hallucination: The Politics of Online Privacy." In *Media, Surveillance, and Identity*, edited by Andre Jansson and Miyase Christensen, 165-182. New York: Peter Lang, 2014.

Barocas, Solon and Helen Nissenbaum. "On Notice: The Trouble with Notice and Consent," *Proceedings of the Engaging Data Forum on the Application and Management of Personal Information* (2009). Retrieved from http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf.

Birchall, Clare. "'Data.gov-in-a-box': Delimiting Transparency." *European Journal of Social Theory* 18, no. 2 (2015): 185-202.

Bodle, Robert. "Regimes of Sharing: Open APIs, Interoperability, and Facebook," *Information, Communication & Society* 14, no. 3 (2011): 320-337.

———. "The Ethics of Online Anonymity or Zuckerberg vs. 'Moot','' *ACM SIGCAS Computers and Society* 43, no. 1 (2013): 22-35.

Burkert, Herbert. "Privacy-Enhancing Technologies: Typology, Critique, Vision." In *Technology and Privacy: The New Landscape*, edited by Philip Agre and Marc Rotenberg, 125-142. Cambridge, MA: MIT Press, 1997.

Cavoukian, Ann. “Privacy by Design: The Definitive Workshop. A Foreword by Ann Cavoukian, Ph.D.” *Identity in the Information Society* 3, no. 2 (2010): 247–51. https://doi.org/10.1007/s12394-010-0062-y.

Cohen, Julie. *Configuring the Networked Self*. New Haven, CT: Yale University Press, 2012.

Collier, Stephen J. “Topologies of Power: Foucault’s Analysis of Political Government Beyond Governmentality.” *Theory, Culture & Society* 26, no. 6 (2009): 78-108.

Davies, Simon. “Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity.” In *Technology and Privacy: The New Landscape*, edited by Philip E. Agre and Marc Rotenberg. 143-165. Cambridge, MA: MIT Press, 1997.

Dörr, Dieter and Russell L. Weaver, eds*. The Right to Privacy in the Light of Media Convergence: Perspectives from Three Continents.* Berlin and Boston, MA: DeGruyter, 2012.

Fenster, Mark. “Transparency in Search of a Theory.” *European Journal of Social Theory* 18, no. 2 (2015): 150-167.

Floridi, Luciano. “Four Challenges for a Theory of Informational Privacy.” *Ethics and Information Technology* 8 (2006): 109-119.

Foucault, Michel. “Governmentality.” In *The Foucault Effect: Studies in Governmentality*, edited by Graham Burchell, Colin Gordon, and Peter Miller, 87-104. Chicago, IL: University of Chicago Press, 1991.

Froomkin, Michael A. “Anonymity in the Balance.” In *Digital Anonymity and the Law: Tensions and Dimensions*, edited by C. Nicoll, J.E.J. Prins, and M.J.M. van Dellen, 5-46. The Hague: T.M.C. Asser Press, 2003.

———. “From Anonymity to Identification.” *Journal of Self-Regulation and Regulation* 1 (2015): 120-138.

Fuchs, Christian. “Towards an Alternative Concept of Privacy,” *Journal of Information, Communication & Ethics in Society* 9, no. 4 (2011): 220-37.

Gellert, Raphaël, and Serge Gutwirth. “Beyond Accountability, the Return to Privacy?” In *Managing Privacy through Accountability*, edited by Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland, and Hector Postigo, 261–83. London: Palgrave Macmillan UK, 2012. https://doi.org/10.1057/9781137032225_13.

Hansen, Hans Krouse. “Numerical Operations, Transparency Illusions and the Datafication of Governance.” *European Journal of Social Theory* 18, no. 2 (2015): 203-220.

Jardine, Eric. “The Dark Web Dilemma: Tor, Anonymity, and Online Policing.” Global Commission on Internet Governance Paper Series. Waterloo, Canada and London, UK: CIGI and Chatham House, September 2015.

Johnson, Deborah G. and Kent A. Wayland. “Surveillance and Transparency as Sociotechnical Systems of Accountability.” In *Surveillance and Democracy*, edited by Kevin D. Haggerty and Minas Samatas, 19-33. New York: Routledge-Cavendish, 2010.

Kerr, Ian and Jennifer Barrigar. “Privacy, Identity, Anonymity.” In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin D. Haggerty, and David Lyon, 386-394. London, UK; New York: Routledge, 2012.

Krotoszynski, Ronald J. *Privacy Revisited: A Global Perspective on the Right to Be Forgotten*. London, UK: Oxford University Press, 2016.

Kwecka, Zbigniew, William Buchanan, Burkhard Schafer, and Judith Rauhofer. “‘I Am Spartacus’: Privacy Enhancing Technologies, Collaborative Obfuscation and Privacy as A Public Good.” *Artificial Intelligence Law* 22 (2014): 113-139.

Lianos, Michalis. “Periopticon: Control Beyond Freedom and Coercion—And Two Possible Advancements in the Social Sciences.” In *Surveillance and Democracy*, edited by Michael Haggerty and Georgos Samatas, 69-88. New York: Routledge, 2010).

Lindsay, David. “The ‘Right to be Forgotten’ in European Data Protection Law.” In *Emerging Challenges in Privacy Law: Comparative Perspectives*, edited by Normann Witzleb, David Lindsay, Moira Paterson, and Sharon Rodrick, 290-337. Cambridge, UK: Cambridge University Press, 2014.

Lucock, Carole, and Katie Black. “Anonymity and the Law in Canada.” In *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*, edited by Ian Kerr, Carole Lucock, and Valerie Steeves, 465–84. Oxford, UK: Oxford University Press, 2009.

Mayer-Schönberger, Viktor and Kenneth Cukier. *Big Data: A Revolution That Will Transform the Way We Live, Work, and Think*. Boston, MA: Houghton Mifflin Harcourt, 2013.

Nissenbaum, Helen. “The Meaning of Anonymity in an Information Age.” *The Information Society* 15, no. 2 (1999): 141-144.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books, 2009.

Ponesse, Julie. "Navigating the Unknown: Towards a Positive Conception of Anonymity." *The Southern Journal of Philosophy* 51, no. 3 (2013): 320-344.

Portwood-Stacer, Laura. "Media Refusal and Conspicuous Non-Consumption: The Performative and Political Dimensions of Facebook Abstention." *New Media & Society* 15, no. 7 (2012): 1041-1057.

Poster, Mark. *The Second Media Age.* Cambridge, UK: Polity Press, 1995.

Regan, Priscilla M. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill, NC: The University of North Carolina Press, 2009.

Rouvroy, Antoinette. "The End(s) of Critique: Data Behaviourism Versus Due Process." In *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*, edited by Mireille Hildebrandt and Katja de Vries, 143-167. Abingdon, UK: Routledge, 2013.

———. "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence." *Studies in Ethics, Law, and Technology* 2, no. 1 (2008).

Rouvroy, Antoinette and Yves Poullet. "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy." In *Reinventing Data Protection?* edited by Poullet Gutwirth, De Hert, de Terwangne and Nouwt, 45-76. Dordecht, Netherlands: Springer, 2009.

Savat, David. "Deleuze's Objectile: From Discipline to Modulation." In *Deleuze and New Technology*, edited by Mark Poster and David Savat, 45-62. Edinburgh: Edinburgh University Press, 2009.

———. *Uncoding the Digital: Technology, Subjectivity and Action in the Control Society.* New York: Palgrave Macmillan, 2013.

———. "Autonomy and Control in the Era of Post-Privacy." *OPEN! Platform for Art, Culture & the Public Domain*. Retrieved from http://www.onlineopen.org/article.php?id=23.

Schwartz, Paul M. "Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices." *Wisconsin Law Review* 743 (2000): 744–788.

Solove, Daniel J. "Privacy and Power: Computer Databases and Metaphors for Information Privacy." *Stanford Law Review* 53, no. 6 (2001): 1393-1462.

———. "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," San Diego Law Review 44, no. 4 (2007): 745-772.

Stalder, Felix. “The Fight Over Transparency: From a Hierarchical to a Horizontal Organization.” *Open* 22 (2011): 8-22.

Stryker, Cole. *Hacking the Future: Privacy, Identity, and Anonymity on the Web.* New York, London: Overlook Duckworth, 2012.

Tavani, Herman T. “Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy,” *Metaphilosophy* 38, no. 1 (2007): 1-22.

Wallace, Kathleen A. “Anonymity,” *Ethics and Information Technology* 1 (1999): 23-35.

Warren, Samuel D. and Louis D. Brandeis. “The Right to Privacy.” *Harvard Law Review* 193, no. 4 (1890): 193-220.

Weber, Rolf. “The Right to Be Forgotten: More Than a Pandora’s Box?” *Journal of Intellectual Property, Information Technology and E-Commerce Law* 2 (2011): 120-130.

Wills, David and Stuart Reeves. “Facebook as a Political Weapon: Information in Social Networks.” *British Politics* 4, no. 2 (2009): 265-281.

Zureik, Elia, Lynda Harling Stalker, Emily Smith, David Lyon, and Yolande Chan. *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*. Montreal & Kingston, Canada: McGill-Queen’s University Press, 2010.