mediastudies.press • Social Media & the Self: An Open Reader

Personal Panopticons

L. M. Sacasas

Published on: Nov 05, 2018

License: Copyright © All rights reserved. (COPYRIGHT)

EVERY NOW AND then, due to some egregious blunder or blatant overreach on the part of government agencies or tech companies, concerns about surveillance and technology break out beyond the confines of academic specialists and into the public consciousness: the Snowden leaks about the NSA in 2013, the Facebook emotional manipulation study in 2014, the Cambridge Analytica scandal in the wake of the 2016 election. These moments seem to elicit a vague anxiety that ultimately dissipates as quickly as it materialized. Concerns about the NSA are now rarely heard, and while Facebook has experienced notable turbulence, it is not at all clear that meaningful regulation will follow or that a significant number of users will abandon the platform. Indeed, the chief effect of these fleeting moments of surveillance anxiety may be a gradual inoculation to them. In my experience, most people are not only untroubled by journalistic critiques of exploitative surveillance practices; they may even be prepared to defend them: There are trade-offs, yes, but privacy appears to be a reasonable price to pay for convenience or security.

This attitude is not new. In the late 1960s, researcher Alan Westin divided the population into three groups according to their attitudes toward privacy: *fundamentalists*, who are generally reluctant to share personal information; *the unconcerned*, who are untroubled and unreflective about privacy; and *pragmatists*, who report some concern about privacy but are also willing to weigh the benefits they might receive in exchange for disclosing personal information. He found then that the majority of Americans were privacy pragmatists, and subsequent studies have tended to confirm those findings. When Westin [updated](#) his research in 2000, he concluded that privacy pragmatists amounted to 55 percent of the population, while 25 percent were fundamentalists and 20 percent were unconcerned.

In a more [recent study](#) of attitudes toward privacy among older adults, Isioma Elueze and Anabel Quan-Haase expanded upon Westin's taxonomy to include a category for what they termed the "cynical expert." These individuals were better informed about privacy concerns than their peers but also tended to be more likely to share personal information. The findings corroborated a 2016 [study](#) of privacy attitudes and social media platforms by Eszter Hargittai and Alice Marwick that sought to better understand what they called the "privacy paradox": the gap between reported privacy attitudes and actual privacy practices. Hargittai and Marwick suggested that the rise of privacy "cynicism" (or "apathy" or "fatigue") was in part a function of the opacity of how social media platforms structure privacy settings and what users perceived to be the inevitable dynamics of what Marwick and danah boyd had, in a [previous paper](#),

termed “networked privacy.” In a network, they contended, the individual invariably cedes a measure of control over privacy to others within the network who have the power to share and publicize information about them without their consent.

That picture has been [further complicated](#) by the widespread adoption of the accouterments of the “smart home,” including internet-connected devices like Nest and AI assistants such as Amazon Echo or Google Home. Perhaps this development has been enough to push people from privacy cynicism toward what media scholar Ian Bogost, [writing in the *Atlantic*](#), has described as full-blown “privacy nihilism,” which presumes an omnipresent regime of surveillance that we can no longer resist and may as well not bother to try. He points to experiences of what we might call the data uncanny—“someone shouts down the aisle to a companion to pick up some Red Bull; on the ride home, Instagram serves a sponsored post for the beverage” or “two friends are talking about recent trips to Japan, and soon after one gets hawked cheap flights there”—that have led users to erroneously conclude that their phones are listening in on their conversations.

As Bogost observes, this is not yet technically feasible, but the fact that this belief persists is itself revealing. Having surrounded ourselves with cameras, microphones, and a panoply of sensors, we now find ourselves enclosed in our own personal panopticon. It doesn’t matter whether anyone is actually watching or listening as long as we can’t be *sure* that they aren’t. Once the apparatus of surveillance is considered a *fait accompli*, then some measure of cynicism, apathy, or nihilism may present itself as the only reasonable response. It’s worth emphasizing, too, that this panopticon is experienced as *personal*: one whose boundaries are drawn close to the self and whose structures derive chiefly from consumer choices rather than government injunctions. The panoptic bubble we inhabit overlaps with what we have traditionally thought of as the private sphere, the sphere of the body and the home. In this way, it reinforces the sense that privacy is a private rather than public concern.

This all suggests the broader possibility that the pervasive presence of surveillance helps produce people who are more at ease with it—people who no longer know what privacy is for, or what socio-moral milieu could give it value. We may retain some memory of how the word is used, but we don’t know what it names. This development is, in part, an effect of habitually experiencing the self as mediated through the apparatus of surveillance. The subjective experience of operating within the field of surveillance has more bearing on our attitudes than detached theorizing about the capacities of the surveillance apparatus or the abstract ideal of privacy.

The older understanding of privacy that arose in conjunction with the material culture of early modernity is no longer adequate, in part, because it is no longer plausible or even altogether desirable. The techno-social order that was its habitat no longer exists. The degree to which we have preferred the more visible self mediated through social media, the quantified self mediated through personal tracking technologies, and the smarter household mediated through the internet of things, is the degree to which we have also, unwittingly perhaps, embraced the apparatus of surveillance. Older accounts of privacy, deriving their force from an ideal of the self whose appeal has faded, have lost their coherence and thus their usefulness.

The consumer surveillance business did not start with contemporary tech companies. “Google and Facebook,” as Bogost notes, “are just the tip of an old, hardened iceberg.” He traces the history of marketing data collection from its mid-19th century origins through the emergence of relational databases in the 1970s to the later rise of data brokers. This long history, as far as Bogost is concerned, suggests that it has become “the machinery of actual life” from which there is no escape, “no matter how many brows get furrowed over or tweets get sent about it.” He concludes that “your data is everywhere, and nowhere, and you cannot escape it, or what it might yet do to you.”

In good dialectic fashion, then, the erosion of the earlier norms surrounding privacy facilitate the further encroachments of surveillance technology. But we will misunderstand our situation if we conceive of the resulting “privacy nihilism” as merely the unintended consequences of this history. From the perspective of what has helpfully been termed surveillance capitalism, such resignation is, to borrow a phrase, a feature not a bug. For the consumer surveillance industry, privacy expectations are obstacles, and one way to overcome them has been to gradually erode their plausibility.

Not everyone, of course, has the same privacy expectations. Privacy pragmatism, for instance, is plausible chiefly for those not already conditioned by the hard experience of discrimination and bias. But attitudes about privacy derive not only from experience of surveillance but perceptions of its potential and many social media platforms—along with the tools of personal tracking, personal AI assistants, and the data gathering nodes of the smart home—have, deliberately or not, made its potential seem limitless, generating the indifference that abets its further expansion.

The appropriate response to these shifts cannot simply be an effort to recover the older normative framework and its configuration of legal and social provisions. That specific array of values and risks is history. In the age of social media, many of us take

a certain amount of visibility for granted while we work hard to exercise a measure of control over it. This is a marked change from earlier conditions, when invisibility was presumed and securing wider visibility, should it even be desired, required hard, deliberate work. Privacy, we might say, was the default setting of the experience of the self. Now, to the degree that social media is the dominant technology of the self, these older parameters of the private self are as likely to be experienced as privation and a failure to appear in social media feeds may be experienced as a social liability.

In this new context, privacy has become a matter of negotiating the terms of our heightened visibility to maintain a degree of autonomy over our self-presentation. It is no longer a matter of shielding wide swaths of our personal lives from view or assuring that one does not unfairly become a “person of interest” to the powers that be. We’re more open to sharing aspects of our lives that may have been previously considered as appropriate only for the self or a select set of intimate others. In no small measure, this derives from the widespread adoption of platforms engineered to reward self-disclosure with greater visibility, a system that depends on seeing the platforms as ubiquitous. The incentives work together with the inescapability they presuppose to produce subjects who more readily accept and participate in the broader surveillance regime, further entrenching the dynamics of networked privacy.

Under this regime, older conceptions of privacy—which construe privacy as a merely individual concern—may misread the threat pervasive surveillance poses, leading to a paradox in which a deeper concern for privacy produces only more despair or indifference about it. For example, when weighing the risks of invasive data gathering, privacy pragmatists may conclude that they have nothing to hide, or that the capture of their anonymized consumer data poses no particular risk to them. They may be right on both counts, but they are missing the collective privacy risks presented by a networked society.

Personal data, even when insignificant on its own, contributes to the massive data pools that fuel the emerging machinery of persuasion, prediction, and control that touch everyone’s lives. As Brett Frischmann and Evan Selinger point out in *Reengineering Humanity*, individualized concerns “fall woefully short of acknowledging the full power of techno-social engineering.” Personalized solutions, such as tweaks to disclosure agreements and a commitment to informed consent, are insufficient to address this.

From Frischmann and Selinger’s perspective, the most serious threats digital technologies pose are not strictly personal concerns like identity theft or companies’

surreptitiously listening in on conversations but the emergence of a softly deterministic techno-social order designed chiefly to produce individuals that are its willing subjects. They note, for example, that when a school deploys fitness trackers as part of its physical education program, privacy concerns should extend not only to questions of students' informed and meaningful consent. Even if consent is managed well, such a program, Frischmann and Selinger argue, "shapes the preferences of a generation of children to accept a 24/7 wearable surveillance device that collects and reports data." This is to say that these programs contribute to "surveillance creep": our gradual acquiescence to the expanding surveillance apparatus. Such an apparatus, in their view, appears pointed ultimately toward the goal of engineered determinism. Frischmann and Selinger conclude by advocating for legal, cultural, and design strategies that aim at securing our freedom from engineered determinism. And I would suggest that we would do well to reframe our understanding of privacy along similar lines.

A better understanding of privacy does not merely address the risk that someone will surreptitiously hear my conversations through my Apple Watch. Rather it confronts the risk of emerging webs of manipulation and control that exert a softy deterministic influence over society. The Apple Watch (or the phone or the AI assistant or the Fitbit) is just one of many points at which these webs converge on individuals. Tech companies, who have much to gain from the normalization of ubiquitous surveillance, have presented their devices and apps as sources of connection, optimization, convenience, and pleasure. Individualized understandings of privacy have proved inadequate to both perceiving the risks and meeting them effectively.

As it turns out, concerns about engineered determinism are no more novel than concerns about privacy. In Fyodor Dostoevsky's *Notes from the Underground*, the unnamed narrator mocks proponents of a rational and utilitarian vision of the future, typified by 19th century Russian social critic and political activist Nikolay Chernyshevsky. For the Underground Man, these "gentlemen," as he consistently calls them, believe "human action will automatically be computed according to these laws, mathematically, like a table of logarithms, reaching to 108,000 and compiled in a directory," and that human beings will assent to this regime because it will be shown to be in their best interest. If humanity's best interest can be rationally determined with mathematical precision, the laws governing human affairs, like those governing the rest of the natural order, can be discovered. He imagines one of these men sarcastically asking, "Well, gentlemen, why don't we get rid of all this good sense once

and for all, give it a kick, throw it to the wind, just in order to send all these logarithms to hell so that we can once again live according to our own foolish will?" Free will as an illusion best cast aside in favor of a regime of predictive manipulation for the sake of the greatest, scientifically determined good.

Against this understanding of human nature, the Underground Man asserts his foolish will as a defining quality. A person's greatest advantage, he claims, is "one's own, independent, and free desire, one's own, albeit wild caprice, one's fantasy, sometimes provoked to the point of madness." He, too, longs for freedom from engineered determinism. This assertion of will doesn't make him a unique hero though—it is part of what makes him, in Dostoyevsky's view, a type that "is bound to exist in our society, taking account the circumstances that have shaped our society." That is, his stubborn refusal to adapt to the prospect of predictive control is as much a product of that order as the acquiescence of those who willingly or thoughtlessly adapt. And this entrapment perhaps explains the Underground Man's wild emotional swings, his self-loathing, his paralysis, his anxieties about self-consciousness, his theoretical embrace of violence as a way of asserting his individuality, his bitterness, and his spite.

The Underground Man's chief problem may be his unquestioning acceptance of an individualist framing of identity. It sunders him from any human-scaled networks of interdependence—i.e., communities—within which his individuality might have flourished. Instead he accepts his isolation and doubles down on its terms.

It would similarly be a mistake for us to respond to the prospect of techno-social engineering by doubling down on the privatization of privacy that has been one of the conditions of its emergence. We need a new story to make the value of privacy seem compelling again. It may be that the best reason for me to guard my privacy is my desire to protect your freedom. But we're a long way, it seems to me, from this being a universally plausible account of privacy, much less an account from which public action will spring. Instead, as they purveyors of surveillance capitalism would have it, we careen toward engineered determinism down a path greased by our indifference and despair.

L. M. Sacasas is an independent scholar based in central Florida. He writes at his website, [The Frailest Thing](#), and publishes [The Convivial Society](#) newsletter.

REPRINT

*"[Personal Panopticons](#)" (L. M. Sacasas, *Real Life*, November 5, 2018)*

REPRINTED WITH PERMISSION FROM REAL LIFE, WHICH RESERVES ALL RIGHTS