SSOAR

Open Access Repository
www.ssoar.info

# Beyond Moral Coupling: Analysing Politics of Privacy in the Era of Surveillance

Heikkilä, Heikki

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

**Empfohlene Zitierung / Suggested Citation:**
Heikkilä, H. (2020). Beyond Moral Coupling: Analysing Politics of Privacy in the Era of Surveillance. *Media and Communication*, *8*(2), 248-257. https://doi.org/10.17645/mac.v8i2.2875

**Nutzungsbedingungen:**
*Dieser Text wird unter einer CC BY Lizenz (Namensnennung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier:*
*https://creativecommons.org/licenses/by/4.0/deed.de*

**Terms of use:**
*This document is made available under a CC BY Licence (Attribution). For more Information see:*
*https://creativecommons.org/licenses/by/4.0*

gesis
Leibniz-Institut
für Sozialwissenschaften

Mitglied der
Leibniz-Gemeinschaft

COGITATIO

**Media and Communication (ISSN: 2183–2439)**
**2020, Volume 8, Issue 2, Pages 248–257**
**DOI: 10.17645/mac.v8i2.2875**

Article

# Beyond Moral Coupling: Analysing Politics of Privacy in the Era of Surveillance

Heikki Heikkilä

Faculty of Information, Technology and Communication, Tampere University, 33014 Tampere, Finland;
E-Mail: heikki.heikkila@tuni.fi

Submitted: 6 February 2020 | Accepted: 14 April 2020 | Published: 23 June 2020

**Abstract**
The article calls into question the prevailing discursive construction in contemporary debate on privacy and surveillance. At the core of this discourse is a moral coupling wherein surveillance is perceived as enemy and privacy as friend. Even if this binary approach renders arguments for democratising data more persuasive, a political cost accompanies it. As this discourse situates political struggle at the level of digital infrastructure and political structures, the moral coupling largely overlooks the ambiguities of how people in their various activities in a digital environment experience surveillance and privacy. Such a framing may discourage users at large from engagement with politics of privacy. Edward Snowden's autobiography is taken as a prominent example of the prevailing discourse. While analysing Snowden's descriptions of privacy and surveillance critically, the author points out the specific value of life stories in describing what privacy means and why it matters. While we cannot assume all people to be equally capable of considering how their own life intersects with the history of their society, we can presume that varying life stories should contribute to the public knowledge of privacy. To provide the framework necessary for appropriately contextualising empirical evidence, the author presents a model wherein privacy is composed of five dimensions: solitude, anonymity, secrecy, intimacy, and dignity.

**Keywords**
digital infrastructure; life-story research; online security; privacy; Snowden; surveillance

**Issue**
This article is part of the issue "The Politics of Privacy: Communication and Media Perspectives in Privacy Research" edited by Johanna E. Möller (Johannes Gutenberg University Mainz, Germany), Jakub Nowak (Maria Curie-Sklodowska University, Poland), Sigrid Kannengießer (University of Bremen, Germany) and Judith E. Möller (University of Amsterdam, The Netherlands).

© 2020 by the author; licensee Cogitatio (Lisbon, Portugal). This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

## 1. Introduction

In the last 15 years, the media environment has witnessed dramatic upheaval. The core of this change has been characterised as the Internet's metamorphosis from a loosely organised, decentralised, and pluralistic system into a tightly controlled, centralised, and commodified one under corporate and government control (Mosco, 2018, p. 210). While library shelves groan under the weight of books about what digital technology is doing to us and our world, many of the media's words about cloud computing, big data-based analysis, and the Internet of Things have been promotional or technically oriented (see Morozov, 2013). Simultaneously, burgeoning critical literature on surveillance is prompting discussion of what Mosco (2018, p. 213) terms "the serious policy issues that arise in a world of massive data centres, nonstop analysis of human behaviour and ubiquitous connectivity."

One of the key topics in critical debate over 'the next Internet' is digital surveillance and its reported effects on people's privacy. While this discussion features a host of perspectives, rooted in fields from social and legal theory to sociology or science and technology studies, I would argue that great centripetal force in media and political debate gets imposed via moral coupling of surveillance and privacy. The associated discourse tends to take a liberal, rights-oriented approach to privacy and

proceed to ask institutions of surveillance "what hidden misuses, what unintended evils…you perpetuate behind your promises of safety" (Hong, 2017, p. 190). At least implicitly, this moral coupling presents surveillance as 'bad' or 'evil' while privacy gets portrayed as a desirable quality (Fuchs, 2011, p. 221), or as 'friend.'

There is much to be said in favour of this moral-coupling discourse. It is instrumental in creating hermeneutics of suspicion around surveillance, thereby supporting political struggle to democratise data power and address worries about possible detrimental effects of digital surveillance on the public (Kennedy & Moss, 2015). In consequence, now "the future of state surveillance [appears] a little less certain, a little more open for negotiation" (Hong, 2017, p. 188). In the process, however, the discourse compromises conceptual depth. Said critique is not easily reconciled with the acknowledged benefits of surveillance in producing valuable knowledge about the population (Foucault, 2004), or in mitigating the ontological insecurity of modernity (Bauman & Lyon, 2013, p. 102). In the absence of theoretical reflexivity, this discourse skims over nuance and sometimes appears too dogmatic.

Simultaneously, with its dependence on a rights-based approach to privacy, the moral-coupling-based discourse is rather unresponsive to theories wherein privacy is relational and contextual (see boyd, 2014; Nissenbaum, 2004). Hence, the dominant discourse fails to engage with specifics of what people do in and with their privacy and how their lives may (or may not) be harmed by surveillance.

A further deficiency with this coupling lies in the political realm. As legal theorist Daniel Solove (2011, p. 2) notes, security interests—often cited in appeals for surveillance—are readily understood, for life and limb are at stake, while privacy rights remain abstract and vague. In such settings, the concepts are positioned in a hierarchy rather than balance, and the political efficacy of the respective arguments follows the same lines. While state surveillance institutions may be more readily subject to criticism amid the fallout from Edward Snowden's revelations, any effect on intelligence legislation has been quite limited (on the UK's situation, see Hintz & Dencik, 2017; on France, see Baisnée & Nicholas, 2017).

In addition, the moral-coupling discourse situates political struggle at structural level, highlighting roles of technological infrastructure elements and the big players managing these: principally, the most powerful state actors (the US, China, and Russia) and (mostly US-based) Internet behemoths such as Google, Amazon, and Facebook. In so doing, it largely overlooks the ambiguities of how people in their varied activities in digital environments experience surveillance and privacy. This framing has implications for public understanding of what is at stake in 'the politics of privacy' and may actually discourage users at large from political engagement.

Hence, it seems that the moral-coupling discourse, while representing necessary criticism of surveillance, is inadequate. Hong suggests that, for an escape from this predicament, a more robust form of surveillance criticism should reveal privacy to be a fragile and conflict-laden concept (Hong, 2017, p. 192). As tempting as that may sound, I set off in the opposite direction for my recommendation in this article. Given that a vast array of digital surveillance may be reshaping our lives, we must direct more theoretical and empirical effort, not less, to understanding people's life-worlds.

The resulting empirical evidence of people's thoughts on these matters or even of underlying reality would be meaningless without an accompanying pertinent theoretical perspective and research design to inform enquiry (Crotty, 1998, pp. 2–3). Accordingly, this article discusses both aspects: the concept of privacy itself and methodology. The theory-oriented aim for the article is, hence, a two-pronged one, which I pursue not by mapping out all relevant theories of privacy but by outlining a coherent typology of privacy that lends itself to empirical endeavours. While the main focus here is on the typology, I discuss the life story's value for privacy studies alongside this. To that end, Snowden's autobiography *Permanent Record* (2019) serves two functions. On the one hand, it exemplifies the moral-coupling discourse; on the other hand, it also provides hints of how to progress beyond it.

## 2. Surveillance as Enemy

In its contemporary context, the moral-coupling discourse refers most prominently to the US, with the most well-known recent disclosure of mass surveillance programmes pointing a finger at the US National Security Agency. Also, as the scale and scope of surveillance of users online has been revealed, it is large US-based companies that have come under the strongest public scrutiny. For the most part, the ensuing political debate on the subject has been structured by liberal political thought. Though the debate's US political context is in many ways unique, the attendant moral-coupling discourse has found its way to European politics and media.

Snowden is a prominent figure in surveillance-related debates. In his autobiography, he vividly describes his path to learning of the secret mass-surveillance programmes developed and conducted by US intelligence agencies and to gradually growing convinced that those activities had to be revealed to the public, whatever the ensuing damage to his personal life. While the book shows that Snowden's role in this exposure relied on exceptional technological skills, developed from early in life, the book is aimed, more than anything else, at justifying his central political conclusion: Surveillance in the hands of intelligence agencies had deviated from course and must be subject to proper democratic oversight.

Ever since his revelations pertaining to the NSA and other agencies, Snowden has been an important and controversial figure in international politics. Therefore, his autobiography is not just any life story. While the book was carefully designed to be a best seller for large global

audiences, its format enables not only Snowden but also readers to "view the intersection of the life history of men with the history of their society, thereby enabling us to understand better the choices, contingencies and options open to the individual" (Robert Bogdan, as cited in Plummer, 2001).

Snowden (2019, p. 228) presents an occasion, less than a year prior to Snowden's revelations, that constituted a moment of epiphany of the sort cited as typical of autobiographies (Denzin, 1989):

> I picked up [the US Constitution] in earnest. I hadn't really read the whole thing in quite a few years, though I was glad to note that I still knew the preamble by heart. Now, however, I read through it in its entirety, from the Articles to the Amendments. I was surprised to be reminded that fully 50 percent of the Bill of Rights, the document's first ten amendments, were intended to make the job of law enforcement harder.

His view on that foundational law reveal Snowden's civil libertarian leanings, which tie in with the traditions of American political thought. This background aids in recognising that Snowden does not find surveillance bad by default. The problem resides, rather, in surveillance powers having overstepped the checks and balances of democratic governance. Besides the absence of effective systematic oversight, Snowden notes that intelligence activities are no longer truly in the state's hands: Much of the technological expertise is outsourced to private companies and individual system specialists more interested in sizeable pay packets than in the security of the nation. He concludes that, in consequence, digital surveillance has become dangerous, especially when under state auspices, and that there is urgent need for an appropriate political design placing those powers back in check.

In academic literature, the notion of surveillance as enemy is promulgated in empirical and theoretical contexts alike. Empirical studies have been undertaken to shed light on the actual mechanics and ultimate goals related to various surveillance agencies' data-gathering endeavours, profiling, and efforts to follow their targets across as many geographical locations and devices as possible (Morozov, 2013; Turow, 2011). For instance, ethnographic studies conducted in the US (Eubanks, 2018; Madden, Gillman, Levy, & Marwick, 2017) and the UK (Redden, Dencik, & Warne, 2020) attest to how algorithmic surveillance is growing into an indispensable tool for the public sector, most notably in social work and policing.

The main conclusion from the empirical studies is that surveillance in the digital environment is expansive, if not excessive. Critical theorists tend to go even further by claiming that surveillance is, above all, a transformative force. In her discussion of 'surveillance capitalism,' Zuboff (2019, p. 93) argues that the economic market's prevailing logic has changed, declaring that "now serving the genuine needs of people is less lucrative, and therefore less important, than selling predictions of their behavior." Couldry and Mejias (2018), in turn, posit that datafication enables appropriation of all life as raw material for economic exploitation in precisely the ways colonialism enabled appropriating land, resources, and bodies for European rulers' benefit in the eighteenth and nineteenth century.

Whether presented against the backdrop of the Constitution, capitalism-related critical theory, or critique of colonialism, surveillance poses threats to democratic governance. Accordingly, it seems reasonable to assume that surveillance is at least potentially 'bad' or 'evil,' thereby warranting politicisation as 'enemy.' A question remains, though, as to whether this picture is comprehensive enough. Does knowing the enemy mean that we also know the friend?

### 3. 'Privacy' as an Empty Word

With the moral-coupling discourse, surveillance theorists tend to discuss privacy in a narrow sense of the concept. For instance, Zuboff (2019, p. 90) argues that privacy has been not eroded but, as a decisional right, redistributed as surveillance capital; that is, decisions about what to reveal or keep secret are no longer made by individual users, as companies have gained those rights and exercise them by appealing to dubious terms of service. With this stance, her research, while focused on surveillance, covers privacy too. After all, the former has subsumed the latter. Where Zuboff addresses decisional privacy only insofar as it refers to content and data generated by users on digital platforms, others extend the consideration of decisional privacy to matters of lifestyle and the life projects one pursues, as with issues of which church to attend or what education to pursue (Rössler, 2005, p. 79).

Within the moral coupling discourse, limited interest in the concept of privacy is not troubling, as the expansion of surveillance is wrong in its own right, violating such key values of liberal democracy as transparency. For example, in book *The Black Box Society*, Pasquale (2015) argues that people do not comprehend the extent of the information collected through close monitoring by governmental and other institutions, let alone how it is used or the consequences of that collection. The problem is not that people lose their privacy but that their right to know is not respected.

While it may be surprising, then, that Snowden writes at length about privacy, there is a stark contrast against his explicit indictment of state surveillance. His defence of privacy remains abstract and elusive. The autobiography makes this rather explicit (2019, p. 208): "The word 'privacy' itself is somewhat empty, because it is essentially indefinable, or over-definable. Each of us has our own idea of what it is. 'Privacy' means something to everyone. There is no one to whom it means nothing."

Snowden draws from a negative definition of privacy, one referring to absence of intervention and thus leaving

the space relatively empty. That said, ripples from that space are far from absent, for privacy as a right constitutes a foundation to all liberties. Even if Snowden talks about subjects granted privacy in the plural ('Americans'), the emphasis is on the individual and an ideal figure of the autonomous liberal subject:

> Americans only have a 'right' to free speech because the government is forbidden from making any law restricting that freedom, and a 'right' to a free press because the government is forbidden from making any law to abridge it. They only have a 'right' to worship freely because the government is forbidden from making any law respecting an establishment of religion, and a 'right' to peaceably assemble and protest because the government is forbidden from making any law that says they can't. (Snowden, 2019, p. 207)

By claiming that privacy is indefinable and over-definable at the same time, Snowden points to what limits empirically understanding privacy. He suggests, on the one hand, that privacy is so abstract that a proper definition of the concept is beyond his grasp; on the other hand, he simultaneously anchors it in concrete subjective experiences and individuals' choices (either way, any further analysis or theorising that might be possible lies outside his interest here). While the book refers to many concrete moments in which experiences of privacy were particularly meaningful for Snowden—among the positive ones are moments of intimacy experienced both offline and online (2019, pp. 99–100), alongside opportunities for time alone while commuting (p. 108)—he otherwise prefers to talk about privacy in generic rather than personal terms. For instance, in relation to one's autonomy and dignity, he states "you don't have to be a closet fetishist to have done things that embarrass you and to fear that strangers might misunderstand you if those things were exposed" (p. 95).

In Snowden's life story, moral coupling of surveillance with privacy contributes to a narrative of growth toward politically consistent subjectivity. The story presents strict adherence to two central tenets of liberal (if not libertarian) democracy: a belief in privacy as the foundation of all personal liberties and trust in the system of checks and balances in preventing abuse of power. This idealistic, textbook-type formulation is cast in sharp relief against an atmosphere of pervasive surveillance realism aimed at normalising surveillance infrastructure (Dencik, 2018, p. 31). The contrast highlights Snowden's separation from the institutions to which he pledged loyalty once upon a time, and his choice of the former over the latter articulates a difference from his erstwhile colleagues in the intelligence community, presumably more compliant with surveillance realism.

While describing some of his own private moments in the book, Snowden says little about lives of people outside his closest circle. Hence, the reader is shown a life-world that, apart from his brief stint in Japan and associations with manga fans, is populated by white Anglo-Saxon civil servants. More importantly, Snowden's portrayal does not overtly connect with lives of people showing less interest in and knowledge of digital systems and surveillance. My point here is not to point a finger at any lack of cultural diversity in Snowden's account so much as highlight possible connections with how surveillance and privacy get coupled in a narrative from this perspective.

On our journey beyond such moral coupling discourse, we can ask what sorts of evidence and voices get overlooked through it. With the discussion below, I issue a challenge to broaden the perspective by overcoming the moral-coupling discourse's limited, outdated understanding of users in a digital environment. However normatively commendable Snowden's perspective may be, it is tied to a specific understanding of the politics of privacy that is not merely specific but also exclusive.

## 4. Surveillance from Users' Perspective

Critical debate on surveillance has a cumulative effect on the moral coupling in that the more information about the scope of surveillance is revealed, the more likely it is for surveillance to be perceived as the enemy. Still, studies among users suggest that user attitudes toward surveillance are often contradictory, even paradoxical. Surveys frequently identify a gulf between user-expressed attitudes and behaviour. Empirical findings indicate that, while users are concerned about their privacy on the Internet in general, and within the social web in particular, usage behaviour does not reflect these concerns correspondingly (CIGI–Ipsos, 2017). Two main factors are cited as behind this privacy paradox: Users reportedly lack awareness of opportunities to protect their privacy, and they tend to underestimate the privacy dangers of self-disclosure (Taddicken, 2014, pp. 248–249).

The privacy paradox and its part in explaining users' relationship to surveillance constitutes a controversial topic in studies of science, technology, and society. Criticisms aside (see boyd & Hargittai, 2010; Tufekci, 2008), the interpretation predominating in surveys is that discrepancies between attitudes and informed actions reflect shortcomings in rationality among users, suggesting that users are unwittingly compliant with surveillance forces that may abuse them (Barth & de Jong, 2017, pp. 1038–1040). This view is consistent with the moral coupling: with people being only partially committed to the idea that surveillance is the enemy and that privacy must be safeguarded, greater education of the public in the hazards of surveillance and in means of defending one's privacy is required. In some cases, the moral-coupling discourse adopts a false-consciousness framework as a foundation for efforts to explain why subjects accept surveillance in an act of 'voluntary servitude' (Robert Pallitto, as quoted in Hong, 2017, p. 189).

This reasoning is problematic, not least because it operates with vague analytical categories such as 'atti-

tudes' and 'behaviour' and draws broad generalisations about them without accounting for the everyday contexts in which uses of social media and the Internet are embedded. At least implicitly, research into the privacy paradox seems to rely on assumptions dating from the mass-communication-dominated era, when media consumption was perceived as introspective; e.g., in his classic study of newspaper-reading, Berelson (1949, p. 199) noted that readers value newspapers for respite functions, as reading 'provides a vacation from personal care by transporting the reader outside his own immediate world.'

Even if respite may be found in media on digital platforms too, this environment tends to facilitate and contribute to encounters involving interaction rather more than introspection. The digital landscape affords activity that can be social while still technical. It enables encounters with "all friends, relatives, teachers, neighbors and many unknown others" (Meyrowitz, 1985, p. 4) via interaction involving much more: numerous functions of computers, as hardware and software, local and remote, respond to every keystroke and mouse movement (Manovich, 2001, p. 155). An appropriate metaphor for the digital landscape is traffic congestion. Users cannot control everything and may recognise this, expecting to be interrupted (or even disturbed) by other users and 'third parties' such as advertisers and infrastructural elements.

Various forms of disturbance online can be readily experienced as surveillance. When official surveillance is associated with situations of social interaction, users tend to deem the matter serious. Among more commonplace cases are incidents of stalking, webcam-based blackmail, blackmail-related scams, and 'sextortion,' in which the actors responsible are usually peer users, not public institutions or commercial entities (Heikkilä, 2018, pp. 68–69). In more everyday activities, users are reminded of surveillance through technical interaction such as automated, algorithm-governed 'communication' that can be generated whenever users purchase goods/services online, participate in customer-loyalty programmes, use online search engines, click on advertisements, upload content to social-media platforms, or sign in to other services via a personal Google ID or Facebook account (Kennedy, 2018).

In day-to-day life, awareness of practices in that last class tends to fade into the background, getting reactivated when clearly surveillance-based feedback reaches the user. Many institutions responsible for surveillance, such as intelligence agencies and the police, deliberately avoid feedback loops, since informing/reminding of surveillance would go against their interests. In the meantime, commercial Internet service providers apply surveillance feedback loops differently, as their business model is predicated on the idea that all advertising must be targeted (Turow, 2013). Therefore, nearly every piece of empirical evidence of surveillance that users see is advertising. All the rest is left to the imagination.

While outputs in selective surveillance feedback loops frequently elicit reactions from users, these are not always interpreted as representing invasions of privacy. Depending on how well the cues calculated by algorithmic systems mesh with users' instantaneous preferences, an automated message may be either pleasing and relevant or disturbing and unsuccessful (Ruckenstein & Granroth, 2019). Users may feel angry when Facebook overtly monetises their personal data (Skeggs & Yuill, 2016, p. 387) and experience 'strange sensations' (Bucher, 2017, p. 35) when seeing evidence of their actions' exposure to outside surveillants—e.g., immediately after loading a friend's Facebook profile, seeing that friend in one's Facebook News Feed.

While users in Ruckenstein and Granroth's (2019) study did not know how Facebook's or Google's proprietary algorithms operate, they recognised the workings of algorithms online. Interviewees proved well versed in surveillance and privacy issues, mainly through everyday understandings of algorithms as shaped by what is taught in schools, discussion with friends, and the media. These observations reveal that, while users hold contradictory attitudes to surveillance and privacy, this phenomenon stems not from lack of awareness/knowledge but from experiences of banality, a concept referring (per Lehmuskallio, Heikkilä, & Kortesoja, 2018), to non-distinctive, ordinary, dull, and clichéd parts of our digitally enhanced life.

While this perspective does not imply surveillance being 'bad' by default, it does point to banality as an indirect consequence of surveillance. Surveillance implies certain structures that impose social order, structures that cannot be willed away. That consequence is daunting, in that banality tends to undermine the very qualities that the moral-coupling discourse is employed to encourage: moral and political reflexivity surrounding the effects of surveillance (see Arendt, 1958).

## 5. Pursuing Meaningful Analysis of Privacy

Liberally oriented theory characterises privacy as a right or an individual's choice. As a right, privacy constitutes a circle around every individual, "which no government…ought to be permitted to overstep…and within which that person ought to reign uncontrolled either by any other individual or by the public collectively" (Mill, 1965, p. 938). The second liberal framing defines privacy as a claim of individuals' stake for determining when, how, and to what extent information about them is communicated to others (Westin, 1967, p. 7). Both ideas abstract from issues related to political economy of capitalism, such as exploitation and income/wealth inequality (Fuchs, 2011, p. 226). In so doing, they do not merely ignore the fact that neither rights to privacy nor opportunities to control one's personal information are equally distributed. As studies on the uses of data-profiling and algorithmic analysis of underprivileged neighbourhoods and social groups suggest, one's resources for establish-

ing and maintaining privacy depend on a combination of sociological variables, such as race, income, and gender (Eubanks, 2018; Gangadharan, 2012).

Liberal theories of privacy vary with regard to the elasticity of the private realm articulated. In rights-based versions, privacy is an ethical imperative so should exist relatively independently of human actions. For choice-based theories, privacy depends on individuals' behaviour, which renders it variable, dynamic, and flexible. In relational theories of privacy, both rights and choices are subject to context-bound interpersonal negotiation. Communication privacy management theory is a school of research that undertakes analysis of how people make decisions about revealing or concealing information they consider private (Petronio & Durham, 2015, p. 336). These scholars subscribe to microanalysis in the style of Goffman, whereby researchers observe an open-ended set of social negotiations over privacy norms. This research assignment should provide a basis for aggregating people's various expectations as to privacy. There is an obvious methodological problem with this strategy: Given that the number of social situations that people engage in is unbounded, the selection of situations submitted to empirical analysis must be likewise unbounded.

In another recommendable methodological strategy, privacy is conceived of as a condition. With this intermediate design, privacy could be approached as a cluster of related but mutually independent components. While there are numerous candidates for such a list (see Fuchs, 2011, pp. 222–224), I would begin with three categories suggested by legal theorist Raymond Wacks (2010, pp. 41–42): solitude, anonymity, and secrecy.

Solitude, sometimes referred to in the privacy literature as seclusion or retreat, involves a time and place wherein people can be unobserved and undisturbed by others (Rössler, 2005, p. 144). Moments of seclusion offer possibilities for stepping outside social events and populated surroundings to be alone. Solitude constitutes a space that other people cannot see for an individual's habits or routines. The value of solitude lies in its voluntary and temporary nature; where the condition is imposed and cannot be lifted, it produces loneliness, which people usually try to avoid. Unlike other dimensions of privacy, solitude is anchored in spatial settings, the spaces people tend to regard as the safest, such as one's home.

Anonymity, in turn, brings in the possibility of not standing out relative to others in the population. With anonymity, people may attend social events (public rallies etc.) without being recognised/identified, and it may encourage individuals to experiment with their identity. This may be a source of independence, as anonymous groups are difficult to control. There is a darker side too, since capacity for unidentified agency may be exercised irresponsibly (e.g., contemporary problems of uncivil behaviour on online discussion boards are strongly linked to anonymity). However, anonymity can entail lack of power, because anonymous people are not fully visible to each other even if they may engage in the same practice or activity. A well-known example is visible in traditional media audiences (viewers and readers), who have limited capacities to make themselves heard and influence media production (Ang, 1991; Heikkilä, 2018, p. 70).

Finally, secrecy is a characteristic of interpersonal communication arising among selected persons while hidden from others. In close interpersonal relations, secrecy and trust are mutually constitutive elements, depending upon and strengthening each other. Secrecy is significant for politics of privacy, and classic theories of the public sphere regard it as an essential precursor to citizenship in that political ideas tend to spring from non-public reflexivity. At the same time, secrecy also provides a veil for terrorist 'sleeper cells' or perpetrators of domestic violence.

From our discussion of Snowden's autobiography, we can see that secrecy is an important aspect of privacy for him. This view resonates with the Habermasian theory of the bourgeois public sphere, in which the emergence of rational publics depends on opportunities for wealthy men to reflect on current affairs in literary clubs, private homes, and coffee houses without interference from those in power. The same dynamics have been identified with regard to many other political movements, aimed at national independence, civil rights for minorities, equality for women, and sexual self-determination (Fraser, 1989). Outside his autobiography, Snowden rarely uses such words as 'citizenship' or 'politics.' He speaks more generally of 'liberty.' About a year after his most explosive revelations, he told interviewers that "reasonable people would grant that privacy is a function of liberty. If we get rid of privacy, we're making ourselves less free" ("Edward Snowden interview," 2014).

Snowden's view on privacy differs from that in algorithmic imaginaries of ordinary Internet users, who discuss their relations to digital surveillance almost exclusively from the perspective of anonymity (Bucher, 2017; Ruckenstein & Granroth, 2019). For them, privacy enables relative freedom of movement over the digital landscape, whereby their behaviour might be visible to third parties but their identities are not revealed. Thus, their access to online services and platforms comes with a cost but this involves negotiation, quite different from the bargaining related to secrecy or seclusion. At some point, these components do intersect, though, since much of targeted advertising relies on age-gender-location-based sorting categories. Therefore, young women are continually told about beauty products and pregnancy tests while young men are targets for dating-site ads and claims of 'hot singles near you.'

Outside the particular conditions considered, users in these and other groups may switch role (e.g., from citizen to consumer or vice versa) as the situation dictates. Nonetheless, even the brief analysis above demonstrates that privacy has multiple meanings and functions, which need to be taken into account for meaningful debate on surveillance and the politics of privacy. Because

**Table 1.** Dimensions of privacy.

| Dimension | Meaning | Functions | Threatened by… |
|---|---|---|---|
| Solitude | being unseen and unheard by others | tranquillity, relaxation | peer users, the Internet of Things |
| Anonymity | being non-distinctive among one's peers | agency without accountability | digital-market actors |
| Secrecy | strategic interpersonal communications | formation of opinions | the security state |
| Intimacy | sharing of emotional and/or physical proximity | showing love and devotion | accidental or deliberate 'peeping toms' |
| Dignity | absence of humiliation and embarrassment | self-esteem, mutual respect | peer users, digital-market actors |

Source: Adapted from Heikkilä (2018) and Wacks (2010).

these dimensions of privacy, or clusters, represent such valuable tools for analysing what privacy would mean as condition, it is worth looking at additional attributes mentioned in privacy studies, outside these categories, for further tools. To gain a fuller toolbox, I would add to the list, alongside seclusion, anonymity, and secrecy, at least two further categories: intimacy and dignity. All five dimensions of the resulting framework are shown in Table 1.

Intimacy involves communication and sharing of emotional and/or physical proximity with others, such as a spouse, child, or friend. Referring to a specific quality of close mutual connection and the process of building this (Jamieson, 2011), intimacy ties in with the positive human qualities of love and commitment. It also enables playfulness in the form of 'backstage language' and unedited conversation (Goffman, 1959, p. 128), which is instrumental to forging the connection but could lead to harm for the intimate partners if stripped of context and revealed to others. A historical figure symbolising threats to intimate privacy is Peeping Tom, whose role was at some point adopted by tabloid journalists and paparazzi. Recent important developments in cameras, drones, and other devices have put the same techniques at anyone's disposal (Andrejevic & Burdon, 2015; Koskela, 2011).

Finally, dignity involves self-respect and reputation, which point to conditions that, while within the innermost self, are taken on and maintained intersubjectively (Honneth, 1995). Dignity is grounded in cultural norms of behaviour or 'good manners.' Hence, codes of dignity are contingent, not universal. The value of dignity is revealed when it is breached—when someone feels embarrassed or humiliated by disclosure of deeds or thoughts that were not intended for sharing with others (Margalit, 1996).

Only this dimension of privacy does not involve a specific mode of 'doing' that one would purposefully pursue for privacy. Rather, dignity involves a state of mind, which may be aggregated from other aspects of privacy though dignity does not necessarily require all of the other conditions to be met. An elderly person dependent on constant professional assistance from nurses or social workers may feel dignified even if opportunities for solitude, anonymity, secrecy, or intimacy are greatly compromised. Given that dignity is a state of mind, it is dependent on one's personal psychological resilience. In addition, it seems that dignity is the facet of privacy least easily restored after undermining.

## 6. Conclusion

With this article, I have challenged a discursive construction that permeates much of contemporary debate on privacy and surveillance, a discourse at whose core is moral coupling wherein surveillance is taken as an enemy and privacy as a friend. While this discourse is widespread in news media and finds support in considerable recent critical surveillance literature, it proved particularly fruitful to problematise it by considering Snowden and his autobiography as exemplars of this line of thought.

Although he and other critics of surveillance contribute to public knowledge of digital surveillance in numerous ways, they, at the same time, seem remarkably indifferent to the fact that Internet users in general are not similarly outspoken critics of surveillance. Additionally, surveillance critics demonstrate limited interest in delving into conceptual analysis of privacy. Might there be something more concrete or nuanced than an 'empty' word, a 'no-go zone,' or an abstract right?

While privacy has elicited interest within many fields of research, the concept has also frustrated many. In the course of listing several typologies and taxonomies of privacy, Fuchs (2011, p. 222) notes a key problem with privacy typologies in that they are arbitrary: "There is no theoretical criterion used for distinguishing the differences between the categories." For Hong (2017, pp. 191–192), privacy is too fragile and contradiction-rife a concept to employ for countering the growth of surveillance. These arguments are warranted but, in my view, they should not distract us from examining what people do in and with their privacy.

Therefore, in this article, I have attempted to conceptualise privacy as a condition of being in which five dimensions may be distinguished for purposes of analysis. The term 'being,' again, has a double meaning: It pertains to situations wherein people decide on revealing/concealing information that they consider private, and it also denotes people's sociologically varying situations in life. It remains for empirical studies to shed light on how, if at all, the meaning of privacy differs with what people do in and with privacy and uncover any contingency on whether they are male or female, rich or poor, residents of a mansion or a shack. This awareness is crucial for extending studies of privacy beyond the abstract standard citizen found in so many textbooks and legislative documents. Moving from discussions about privacy as right to work on privacy as condition is a huge first step, even if the setting remains the context of Western societies. Shifting still further would call for even more profound rethinking both theoretically and methodologically.

In this endeavour, fittingly enough, Snowden's autobiography may be transformed from a theoretical problem into a methodological solution. It holds value in not merely setting forth an authorised stakeholder's view on one of the most important political processes of the last decade but also employing the life story as its format. Thereby, readers can view the intersection of an individual's life history with the history of society. This story is open to multiple analytical readings, and our brief analysis of Snowden's relations to surveillance and privacy provides only a taste of the potential of the approach. The next move on the path would be to locate life stories that decisively differ from Snowden's.

Life-history research, of course, has its own life, dating back to the Chicago School of Sociology in the early 20th century and still further (Plummer, 2001). This methodology has been applied to feminist surveillance studies (see Dubrofsky & Magnet, 2015). Since the rich methodological insights developed within that research tradition cannot be discussed here in detail, I refer only to Marwick and boyd (2018), who highlight the value in advancing research into privacy at the margins. The stark reality is that achieving privacy is especially difficult for those who already are otherwise marginalised. They emphasise: "Parents argue that they have the right to surveil their children 'for safety reasons.' Activists who challenge repressive regimes are regularly monitored by state actors. And poor people find themselves forced to provide information in return for basic services" (Marwick & boyd, 2018, p. 1158).

It seems that if we want to know more about privacy and how surveillance reshapes privacy, there is much to learn from people for whom privacy is a distinctly scarce resource, those who work hardest to maintain what is left of it.

Studies of privacy-related vulnerability would guide us toward hearing and heeding the life stories of people with experiences of discriminatory surveillance practices, such as redlining and profiling of whatever sort, be it racial, medical, or political (Eubanks, 2018; Gangadharan, 2012; Redden et al., 2020). This is not to say that only experiences of the underprivileged matter but, rather, to suggest that this form of knowledge is essential for dealing with politics of privacy.

**Acknowledgments**

This article is based on research conducted in the Banal Surveillance research project (2018–2022), funded by the Academy of Finland. The author wishes to thank the two anonymous reviewers for their comments. I am grateful also for feedback from Anna Shefl, Minna Saariketo, and my IASR colleagues Laura Ahva, Risto Heiskala, Mervi Kaukko, Hanna Ojala, and Saara Pellander.

**Conflict of Interests**

The author declares no conflict of interests.

**References**

Andrejevic, M., & Burdon, M. (2015). Defining the sensor society. *Television & New Media*, *16*(1), 19–36.

Ang, I. (1991). *Desperately seeking the audience*. London: Routledge.

Arendt, H. (1958). *Eichmann in Jerusalem: A report on the banality of evil*. New York, NY: Viking Press.

Baisnée, O., & Nicholas, F. (2017). Security, terror and freedom: The dynamics of public opinion in the French surveillance debate. In R. Kunelius, H. Heikkilä, A. Russell, & D. Yagodin (Eds.), *Journalism and the NSA revelations: Privacy, security and the press* (pp. 91–112). London: IB Tauris and Reuters Institute for the Study of Journalism.

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior: A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058.

Bauman, Z., & Lyon, S. (2013). *Liquid surveillance: A conversation*. Cambridge: Polity.

Berelson, B. (1949). What 'missing the newspaper' means. In P. Lazarsfeldt & F. Stanton (Eds.), *Communication research 1948–1949* (pp. 111–128). New York, NY: Harper & Brothers.

boyd, d. (2014). *It's complicated: The social lives of networked teens*. New Haven, CT: Yale University Press.

boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, *15*(8), 1–23.

Bucher, T. (2017). The algorithmic imaginary: Exploring the ordinary affects of Facebook algorithms. *Information, Communication & Society*, *20*(1), 30–44.

CIGI–Ipsos. (2017). 2017 CIGI–Ipsos global survey on Internet security and trust. *CIGI Online*. Retrieved from http://www.cigionline.org/internet-survey-2017

Couldry, N., & Mejias, U. (2018). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, *20*(4), 336–349.

Crotty, M. (1998). *The foundations of social research: Meaning and perspective in research process*. London: SAGE.

Dencik, L. (2018). Surveillance realism and the politics of imagination: Is there no alternative? *Krisis*, *1*(1), 31–43.

Denzin, N. (1989). *Interpretive biography*. London: SAGE.

Dubrofsky, R., & Magnet, S. A. (Eds.). (2015). *Feminist surveillance studies*. Durham, NC: Duke University Press.

Edward Snowden interview: The edited transcript. (2014, July 18). *The Guardian*. Retrieved from http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. New York, NY: St. Martin's Press.

Foucault, M. (2004). *Security, territory, population: Lectures at the Collège de France 1977–1978*. London: Palgrave Macmillan.

Fraser, N. (1989). *Unruly practices: Power, discourse, and gender in contemporary social theory*. Minneapolis, MN: University of Minnesota Press.

Fuchs, C. (2011). Towards an alternative concept of privacy. *Journal of Information, Communication and Ethics in Society*, *9*(4), 220–237.

Gangadharan, S. (2012). Digital inclusion and data profiling. *First Monday*, *17*(5). https://doi.org/10.5210/fm.v17i5.3821

Goffman, E. (1959). *The presentation of self in everyday life*. New York, NY: Doubleday.

Heikkilä, H. (2018). Privacy under surveillance: Towards a conceptual analysis of the price of connection. *Northern Lights*, *16*(1), 59–74.

Hintz, A., & Dencik, L. (2017). The politics of surveillance policy: UK regulatory dynamics after Snowden. *Internet Policy Review*, *5*(3), 1–16.

Hong, S. (2017). Criticizing surveillance and surveillance critique: Why privacy and humanism are necessary but not sufficient. *Surveillance & Society*, *15*(2), 187–203.

Honneth, A. (1995). *The struggle for recognition: The moral grammar of social conflicts*. Cambridge: Polity Press.

Jamieson, L. (2011). Intimacy as a concept: Explaining social change in the context of globalisation or another form of ethnocentricism? *Sociological Research Online*, *16*(4), 1–13.

Kennedy, H. (2018). Living with data: Aligning data studies and data activism through a focus on everyday experiences of datafication. *Krisis*, *1*(1), 18–30.

Kennedy, H., & Moss, G. (2015). Known or knowing publics? Social media data mining and the question of public agency. *Big Data & Society*, *2*(2). https://doi.org/10.1177/2053951715611145

Koskela, H. (2011). Hijackers and humble servants: Individuals as camwitnesses in contemporary controlwork. *Theoretical Criminology*, *15*(3), 269–282.

Lehmuskallio, A., Heikkilä, H., & Kortesoja, M. (2018). *Banal surveillance: An introduction to a framework of a study*. Paper presented at the Amsterdam Privacy Conference 2018, Amsterdam, The Netherlands.

Madden, M., Gillman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review*, *95*(1), 53–125.

Manovich, L. (2001). *The language of new media*. Cambridge, MA: MIT Press.

Margalit, A. (1996). *The decent society*. Cambridge, MA: Harvard University Press.

Marwick, A., & boyd, d. (2018). Understanding privacy at the margins. *International Journal of Communication*, *12*, 1157–1165.

Meyrowitz, J. (1985). *No sense of place: The impact of electronic media on social behavior*. New York: Oxford University Press.

Mill, J. S. (1965). *Principles of political economy* (Vol. 2). London: University of Toronto Press.

Morozov, Y. (2013). *To save everything, click here: Technology, solutionism, and the urge to fix problems that don't exist*. New York, NY: Public Affairs.

Mosco, V. (2018). A critical perspective on the post-Internet world. *Javnost: The Public*, *25*(1/2), 210–217.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–157.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge, MA: Harvard University Press.

Petronio, S., & Durham, W. (2015). Communication privacy management theory: Significance for interpersonal communication. In L. Baxter & D. Braithwaite (Eds.), *Engaging theories in interpersonal communication* (pp. 335–347). London: SAGE.

Plummer, K. (2001). *Documents of life 2: An invitation to critical humanities*. London: SAGE.

Redden, J., Dencik, L., & Warne, H. (2020). Datafied child welfare services: Unpacking politics, economics and power. *Policy Studies*. https://doi.org/10.1080/01442872.2020.1724928

Rössler, B. (2005). *The value of privacy*. Cambridge: Polity.

Ruckenstein, M., & Granroth, J. (2019). Algorithms, advertising and the intimacy of surveillance. *Journal of Cultural Economy*, *13*(1), 12–24.

Skeggs, B., & Yuill, S. (2016). Capital experimentation with person/a formation: How Facebook's monetization refigures the relationship between property, personhood and protest. *Information, Communication & Society*, *19*(3), 380–396.

Snowden, E. (2019). *Permanent record*. London: Macmillan.

Solove, D. (2011). *Nothing to hide: The false trade-off between security and privacy*, New Haven, CT: Yale University Press.

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Assisted Communication*, *19*(2), 248–273.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*(1), 20–36.

Turow, J. (2011). *The daily you: How the new advertising industry is defining your identity and your worth*. New Haven, CT: Yale University Press.

Turow, J. (2013). *The aisles have eyes: How retailers track your shopping, strip your privacy, and define your power*. New Haven, CT: Yale University Press.

Wacks, R. (2010). *Privacy: A very short introduction*. Oxford: Oxford University Press.

Westin, A. (1967). *Privacy and freedom*. New York, NY: Altheneum.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York, NY: Public Affairs.

**About the Author**

**Heikki Heikkilä** is Associate Professor in Journalism Studies at Tampere University (starting September 2020) and Senior Research Fellow at the Advanced Research Centre for Social Research (IASR). His research focuses on the effects of digitalisation on journalism and its (assumed) audiences. He is also written about surveillance and privacy. He is co-editor of the book *Journalism and the NSA Revelations: Privacy, Security and the Press* (IB Tauris, 2017, with Risto Kunelius, Adrienne Russell and Dmitry Yagodin), and he has published articles in *Journalism: Theory, Practice & Criticism*, *Digital Journalism*, *European Journal of Communication*, and *Javnost: The Public*.