Book Review

The Crowdsourced Panopticon: Conformity and Control on Social Media—Jeremy Weissman (New York, NY, USA: Rowman & Littlefield, 2021)

Reviewed by Katina Michael
School for the Future of Innovation in Society
Arizona State University
Tempe, AZ 85287 USA

School of Computing and Augmented Intelligence
Arizona State University
Tempe, AZ 85281 USA

The provocative cover of Jeremy Weissman's debut monograph captures well the new visibility we are all subject to. Reminiscent of the times we live in, is the idea of the "photoborg" [1].

The Crowdsourced Panopticon: Conformity and Control on Social Media explores the role of "the network" and social media, its meaning and thrust toward meaninglessness, its empowerment *of* the public and power *over* the public, normalized behavior, and how to resist the impact of this socio-technological phenomenon on our everyday lives.

The book is divided into eight accessible chapters in three parts and is jam-packed with evidence for the insights and claims the author makes through the selection of a unique ensemble of references. Part 1 provides a normative critique of conformity from an institutional perspective; Part 2 is focused on emerging socio-technological trends and future scenario forecasts; and Part 3 moves to offer resistance solutions against the current and impending cultural forces [2].

In his opening pages, Weissman writes: "We are today merging with our technologies, becoming more deeply intertwined with them than ever before" [p. 2]. He points to the invisible internet and the impact smartphones sporting cameras have had and makes his own predictions that "soon enough from there these networked devices will likely creep inside many if not most people's bodies" [p. 2]. This is something M. G. Michael and I also strongly conclude from three decades in the field of emerging technologies [3], [4].

Weissman notes his book is one of resistance to the overbearing Internet cultural forces. Juxtaposing the "self" against the "collective," Weissman reminds us that privacy and human rights are individual. To declare them moot because of technological diffusion in the hands of the masses is akin to an attack on our fundamental freedoms, albeit our survival as a species [5].

Digital Object Identifier 10.1109/MTS.2023.3342852
Date of current version: 22 January 2024.

In our current hyperexposure, we can no longer have anonymity in a crowd. Rather, the new visibility will maintain that there is essentially "nowhere to hide" [6], [7]. Everyone with a smartphone might be considered a mobile camera mounted on a body, in essence, a photoborg.

In his opening chapter, Weissman eloquently describes the ancient story of the Ring of Gyges as depicted in Plato's *Republic*, linking it with invisibility and converting it to a modern context of the Digital Ring of Gyges. Weissman informs his analysis by referencing Freud, Mill, and others. He notes: "Conformity allows us to feel part of a crowd, accepted, just like everyone else, and that brings us the feeling of connection that as social animals, we so desperately seek" [p. 22]. However, as Weissman reflects, that "comes at a cost to our freedom" [8], [9].

One of Weissman's skills as an author is to see things that others may not. In Chapter 2, titled "Social Media as an Escape from Freedom," he goes on to report on persuasive artificial intelligence (AI), on compulsive behaviors [p. 28] that are propelled "by design" [10]. In citing Egebark and Elstrom [11], he refers to the fact that "Facebook constitutes a close to ideal environment for studying conformity" "because it allows a large number of people to observe each other's actions while attempting to assert their status" [p. 33].

Weissman beautifully summarizes what this kind of lifelogging [12], [13] can do to someone, referring to Marx et al. [14] noting that "under such conditions, the soul inside the human is essentially sucked dry in the production of the object… we are building the object, but it is as if the object controls us from the inside" [p. 35]. What an eye-opening reference [15]!

Chapter 3 is about meaninglessness in the present age, heeding the warnings of existentialist philosopher Søren Kierkegaard, who wrote that to become our authentic selves means to commit oneself "to an idea for which [they] are willing to die" [p. 43]. In other words, we are asked at point blank: what is our true passion; what is our calling? Weissman interprets this calling citing existentialist analyst Viktor Frankl: "in order to realize ourselves, we must actually transcend ourselves…" [p. 44].

But Weissman rightly asks how might it be possible to achieve this aim if we are endlessly distracted? If we are always on, always connected, having brain drain—which can act as a barrier to pursuing our calling. Belonging may well mean having our feet on the ground tangibly, getting off the computer, ceasing to be a spectator of others, *being* and *getting real*, and living in the present.

In Chapter 4, "The Spectacular Power of the Public," Weissman explores social media in its full force. He describes the potential for public shaming, especially in the context of the "global village" online. It should be spelled out, however, that while social media posts may provide an avenue to "blame and shame" publicly, context may be missing. Who is doing the shaming, who is suffering the humiliation, and who the public side with very much determine who may be in control.

We could deduce interconnectedness and social media to be a tool for empowering the masses, that is, technology that serves the public interest. However, corporations and governments armed with their lawyers, large budgets, and even the police using open-source intelligence (OS-INT) can now utilize the internet as a strategic tool to surveil the masses and their sentiments, to gather evidence without a warrant, unobtrusively [16], [17]. Every day, people would not even know they were in the process of having their civil liberties impinged [18].

Another gift the author offers is the interlinking of ideas between chapters. With each successive chapter, Weissman reveals a little more about the inner reflections that form his opinions. In Chapter 5, titled "P2P Surveillance," the author stresses, "we need to be keenly aware of surveillance in whatever forms they manifest" [p. 83].

Following James Rule, Weissman also emphasizes that *systems of surveillance* are accompanied by *systems of control* [p. 84]. The author goes on to refer to the future impact of companies like Clearview AI, Regina Dugan's Facebook "Building 8," and Elon Musk's Neuralink. The chapter closes with references to the aptly named: "Crowdsourced Panopticon" [pp. 95–97], otherwise known in the literature as "Lots of Little Brothers" (versus a single Big Brother) [19].

We are reminded again that there are many camera views, that there is constant watching occurring [20], "power through transparency" and "subjection by illumination" [p. 95], following Foucault [21]. In every direction and at every hour, we can assume we are being watched, and this is particularly true of the public sphere [22], [23]. However, this is true even at home. Zoom has invaded our personal space

without filters. Additionally, tiny pinhole cameras on our television sets, laptops, and phones possibly see us and hear us "legitimately" because the product's terms and conditions say they can and are allowed to. Some even suspect that audio chipsets embedded in products are always in "active mode" listening to the next conversation and somehow linked to search engine recommender systems. The proof of the latter is in ad hoc personal tests and anecdotal conversations with experts in the field, but no one has had the audacity—nor the hard evidence to prove it [28], [29].

We can no longer say this is the thinking of the paranoid, these are widely accepted "givens." M. G. Michael has referred to this as the "axis of access" in an uberveillant world [24]. Ordinary people will be subjected to all forms of surveillance and will struggle to resist given the pervasive and persistent lens. They cannot elect nor afford to live off the grid. The intelligentsia and powerful will pay for their protection or have general clearance unless they too are considered replaceable. No one is safe in this world of watching because there are layers upon layers of interdependencies, intricacies, and need I say webs.

In Chapter 6, the "Net of Normalization" is all about Foucault's "disciplinary power." Weissman, in his analysis of peer-to-peer (P2P) surveillance in this chapter, focuses on the following key elements: 1) soul/psyche; 2) micropenalty; 3) rating and ranking; 4) quantification; 5) ranked distribution; 6) shameless class; 7) normalizing gaze; and 8) case files [p. 105]. All this, Weissman says, has to do with repetitive continual and compulsory inspection. As analog beings, we are at the mercy of the digital that meticulously records, remembers, and plays back [25].

In the final part of the book dedicated to the idea of resistance, there is a call to action. How do we regain our freedom in this public age? What are the risks? Weissman recounts the learnings from Google's Digital Glass and the first "Explorers" (i.e., wearers) of this technology. Incessant filming in a public space without regard for other people who may be compromised through the act of recording. The question today that most ask themselves is: can we ever regain our privacy in a public space?

Chapter 8 is titled "Strategies of Resistance," describing a "mutual transparency solution." This is, perhaps, one of the weakest parts of the book, likely due to its brevity and well-known thesis, which to me simply falls short of a practical and plausible resolution. I was expecting more from Weissman given where the book began, philosophically at least.

He poses a rhetorical question toward the conclusion: "Is resistance futile?" This chapter completes the book [pp. 144–157]. The difficulty of finding solutions to address the multidimensional complexities we live in cannot be underestimated [30]. There is no silver bullet solution to any of this current "state of affairs." Weissman offers some core reflections that should be considered.

This was an informative read all in all. It relied on a mixture of academic sources, philosophers, and modern scholars intermingled with sober perspectives recorded in popular media. The book contained illustrative examples and cases to make it relevant to the reader and accessible, in today's context, and always with a twist. This is indeed Weissman's craft—to connect the ancient with the modern, and to convey to us, "we've somehow been here before." We can use these ancient stories to inform our modern-day narrative and to use the learnings from today to ensure we create a better future and not fall into the traps that had been foreseen.

Readers are truly spoiled at every turn because this book is an original contribution in the way it weaves and interweaves the fundamental storyline: our technologies have social implications—do we see what they are doing to us, our community, and society at large [26], [27]?

In the end, the book will make you stop and think in a very personal way. It convicts without telling you what to do. Do you have an online persona(s)? Why? What is your core mission and who are the stakeholders you engage with? Are you impacted by pressures of conformance? Have you reflected on what you contribution is? Would you change anything about the value of that contribution?

Weissman does not preach or moralize; he points to the patterns and trends and you cannot help but ask yourself where all this surveillance is leading us to. In this modern era of quantified everything, what should really matter to us? The answer to this question will be different for each person as they determine their place in the world. Armed with this new knowledge, described so clinically by Weissman, we are set a challenge. The question is, are we up to it? ■

References

[1] K. Michael, "Wearables and lifelogging: The socioethical implications," *IEEE Consum. Electron. Mag.*, vol. 4, no. 2, pp. 79–81, Apr. 2015, doi: 10.1109/MCE.2015.2392998.

[2] D. Gokye and K. Michael, "Digital wearability scenarios: Trialability on the run," *IEEE Consum. Electron. Mag.*, vol. 4, no. 2, pp. 82–91, Apr. 2015, doi: 10.1109/MCE.2015.2393005.

[3] M. G. Michael and K. Michael, "Toward a state of Überveillance [special section introduction]," *IEEE Technol. Soc. Mag.*, vol. 29, no. 2, pp. 9–16, Summer 2010, doi: 10.1109/MTS.2010.937024.

[4] M. G. Michael and K. Michael, *Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies*. Hershey, PA, USA: IGI Global, 2014.

[5] K. Michael, "Sousveillance: Implications for privacy, security, trust, and the law," *IEEE Consum. Electron. Mag.*, vol. 4, no. 2, pp. 92–94, Apr. 2015, doi: 10.1109/MCE.2015.2393006.

[6] M. G. Michael, K. Michael, and C. Perakslis, "Überveillance, the Web of things, and people: What is the culmination of all this surveillance?" *IEEE Consum. Electron. Mag.*, vol. 4, no. 2, pp. 107–113, Apr. 2015, doi: 10.1109/MCE.2015.2393007.

[7] M. G. Michael, K. Michael, and T. Bookman, "Wim Wenders' wings of desire: Anticipating uberveillance," *J. Asia–Pacific Pop Culture*, vol. 6, no. 1, pp. 109–129, Jul. 2021, doi: 10.5325/jasiapacipopcult.6.1.0109.

[8] S. R. Bradley-Munn and K. Michael, "Whose body is it? The body as physical capital in a techno-society," *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 107–114, Jul. 2016, doi: 10.1109/MCE.2016.2576518.

[9] A. L. Puhalo, "A conversation with Lazar Puhalo [interview]," *IEEE Technol. Soc. Mag.*, vol. 34, no. 3, pp. 25–28, Sep. 2015, doi: 10.1109/MTS.2015.2473995.

[10] R. Abbas et al., "Machine learning, convergence digitalization, and the concentration of power: Enslavement by design using techno-biological behaviors," *IEEE Trans. Technol. Soc.*, vol. 3, no. 2, pp. 76–88, Jun. 2022, doi: 10.1109/TTS.2022.3179756.

[11] J. Egebark and M. Ekström, "Like what you like or like what others like? Conformity and peer effects on Facebook," Res. Inst. Ind. Econ., Stockholm, Sweden, IFN White Paper no. 886, 2011. [Online]. Available: http://www.ifn.se/wfiles/wp/wp886.pdf

[12] K. Michael, "Beyond human: Lifelogging and life extension [editorial]," *IEEE Technol. Soc. Mag.*, vol. 33, no. 2, pp. 4–6, 2014, doi: 10.1109/mts.2014.2322915.

[13] K. Michael, D. Gokyer, and S. Abbas, "Societal implications of wearable technology: Interpreting, "trialability on the run," in *Managing Security Issues and the Hidden Dangers of Wearable Technologies*, A. Marrington, D. Kerr, and J. Gammack, Eds. Hershey, PA, USA: IGI Global, 2017, pp. 238–266, doi: 10.4018/978-1-5225-1016-1.ch010.

[14] K. Marx, J. J. O'Malley, and R. A. Davis, *Marx: Early Political Writings*. Cambridge, U.K.: Cambridge Univ. Press, 1994, p. 72.

[15] L. Perusco and K. Michael, "Control, trust, privacy, and security: Evaluating location-based services," *IEEE Technol. Soc. Mag.*, vol. 26, no. 1, pp. 4–16, 2007, doi: 10.1109/mtas.2007.335564.

[16] S. Bronitt and K. Michael, "Human rights, regulation, and national security [introduction]," *IEEE Technol. Soc. Mag.*, vol. 31, no. 1, pp. 15–16, Spring 2012, doi: 10.1109/MTS.2012.2188704.

[17] K. Michael and R. Clarke, "Location and tracking of mobile devices: Überveillance stalks the streets," *Comput. Law Secur. Rev.*, vol. 29, no. 3, pp. 216–228, 2013.

[18] R. Abbas et al., "Emerging forms of covert surveillance using GPS-enabled devices," *J. Cases Inf. Technol.*, vol. 13, no. 2, pp. 19–33, Apr. 2011.

[19] R. Abbas, K. Michael, and M. G. Michael, "Using a social-ethical framework to evaluate location-based services in an Internet of Things world," *Int. Rev. Inf. Ethics*, vol. 22, pp. 42–73, Dec. 2014.

[20] K. Michael and M.G. Michael, "No limits to watching?" *Commun. ACM*, vol. 56, no. 11, pp. 26–28, Nov. 2013, doi: 10.1145/2527187.

[21] J. Ferenbok, S. Mann, and K. Michael, "The changing ethics of mediated looking: Wearables, veillances, and power," *IEEE Consum. Electron. Mag.*, vol. 5, no. 2, pp. 94–102, Apr. 2016, doi: 10.1109/MCE.2016.2516139.

[22] C. Perakslis, K. Michael, and M. G. Michael, "The converging veillances: Border crossings in an interconnected world," *IEEE Potentials*, vol. 35, no. 5, pp. 23–25, Sep. 2016, doi: 10.1109/MPOT.2016.2569724.

[23] S. J. Fusco et al., "Monitoring people using location-based social networking and its negative impact on trust," in *Proc. IEEE Int. Symp. Technol. Soc. (ISTAS)*, May 2011, pp. 1–11.

[24] K. Michael et al., "Uberveillance and the rise of last-mile implantables: Past, present, and future," in *Embodied Computing: Wearables, Implantables, Embeddables, Ingestibles*, I. Pedersen and A. Iliadis, Eds. Cambridge, MA, USA: MIT Press, 2020, ch. 5, pp. 97–130.

[25] M. G. Michael and K. Michael, "The fallout from emerging technologies: Surveillance, social networks, and suicide," *IEEE Technol. Soc. Mag.*, vol. 30, no. 3, pp. 13–17, Fall 2011.

[26] K. D. Stephan et al., "Social implications of technology: The past, the present, and the future," *Proc. IEEE*, vol. 100, no. Special Centennial Issue, pp. 1752–1781, May 2012, doi: 10.1109/jproc.2012.2189919.

[27] R. Pringle, K. Michael, and M. G. Michael, "Unintended consequences: The paradox of technological potential," *IEEE Potentials*, vol. 35, no. 5, pp. 7–10, Sep. 2016, doi: 10.1109/MPOT.2016.2569672.

[28] A. Ng and M. Wollerton, "Google calls nest's hidden microphone an 'error,'" *CNET*, Feb. 20, 2019. [Online]. Available: https://www.cnet.com/home/smart-home/google-calls-nests-hidden-microphone-an-error/

[29] Staff, "Sorry, we didn't mean to keep that secret microphone a secret, says Google," *Sophos News*, Feb. 21, 2019. [Online]. Available: https://news.sophos.com/en-us/2019/02/21/sorry-we-didnt-mean-to-keep-that-secret-microphone-a-secret-says-google/

[30] M. G. Michael and K. Michael, "Resistance is not futile, nil desperandum," *IEEE Technol. Soc. Mag.*, vol. 34, no. 3, pp. 10–13, Sep. 2015, doi: 10.1109/MTS.2015.2473981.

Katina Michael is a tenured professor with the School for the Future of Innovation in Society, Arizona State University, Tempe, AZ 85287 USA, and the School of Computing and Augmented Intelligence, Arizona State University, Tempe, AZ 85281 USA. She is also the research director of the Society Policy Engineering Collective (SPEC).

■ Direct questions and comments about this article to Katina Michael, School for the Future of Innovation in Society, Arizona State University, Tempe, AZ 85287 USA; School of Computing and Augmented Intelligence, Arizona State University, Tempe, AZ 85281 USA; katina.michael@asu.edu.