Westminster Papers in Communication and Culture

Troullinou, P. (2017). Rethinking Privacy and Freedom of Expression in the Digital Era: An Interview with Mark Andrejevic. *Westminster Papers in Communication and Culture,* 12(3), 72-77, DOI: https://doi.org/10.16997/wpcc.270

COMMENTARY

Rethinking Privacy and Freedom of Expression in the Digital Era: An Interview with Mark Andrejevic

Pinelopi Troullinou
Open University, UK
pinelopi.troullinou@open.ac.uk

Mark Andrejevic, Professor of Media Studies at the Pomona College in Claremont, California, is a distinguished critical theorist exploring issues around surveillance from pop culture to the logic of automated, predictive surveillance practices. In an interview with *WPCC* issue co-editor Pinelopi Troullinou, Andrejevic responds to pressing questions emanating from the surveillant society looking to shift the conversation to concepts of data holders' accountability. He insists on the need to retain awareness of power relations in a data driven society highlighting the emerging challenge, 'to provide ways of understanding the long and short term consequences of data driven social sorting'. Within the context of Snowden's revelations and policy responses worldwide he recommends a shift of focus from discourses surrounding 'pre-emption' to those of 'prevention' also questioning the notion that citizens might only need to be concerned, 'if we are doing something "wrong"' as this is dependent on a utopian notion of the state and commercial processes, 'that have been purged of any forms of discrimination'. He warns of multiple concerns of misuse of data in a context where 'a total surveillance society looks all but inevitable'. However, the academy may be in a unique position to provide ways of reframing the terms of discussions over privacy and surveillance via the analysis of 'the long and short term consequences of data driven social sorting (and its automation)' and in particular of algorithmic accountability.

Keywords: Data; surveillance; privacy; accountability; security; prevention

Edward Snowden's revelations in the summer of 2013 brought to public attention the full extent to which data generated by everyday activities on digital platforms can be monitored and used by the state apparatus. However, there has been a long-standing debate in academic circles on surveillance and control, exploring the surveillance-industrial complex and its emerging social impact. Current research expands on this theme of the societal implications of predictive analytics used by the state and the market. Mark Andrejevic, Professor of Media Studies at the Pomona College in Claremont, California, is a distinguished critical theorist exploring issues around surveillance from pop culture to the logic of automated, predictive

surveillance practices. His work has appeared in several edited collections, in prestigious academic journals and he has been an invited speaker at international conferences. He is a member of the editorial board of the University of Westminster Press's book series 'Critical Digital and Social Media Studies'.

His three books portray how plugged into the zeitgeist he has been for more than a decade. His first book *Reality TV: The Work of Being Watched* (Andrejevic, 2004) explores how surveillance was introduced as a normality throughout popular culture. His second book, *iSpy: Surveillance and Power in the Interactive Era* (Andrejevic, 2007) examines the power relations of a new form of surveillance with an interactive and participatory character that operate through the deployment of social media. His third book, *Infoglut: How Too Much Information Is Changing the Way We Think and Know* (Andrejevic, 2013), focuses on the social, cultural, and theoretical implications of data mining and predictive analytics. In his latest academic article 'To Preempt A Thief' (2017), he explores the consequences of predictive policing. What does it mean for Democracy to shift from preventing to pre-empting criminal activities? In this light, Mark Andrejevic in an interview with *WPCC*, responds to pressing questions of a surveillant society shifting the conversation to concepts of data holders' accountability. He explains the power relations in a data driven society highlighting the emerging challenge, 'to provide ways of understanding the long and short term consequences of data driven social sorting'.

Pinelopi Troullinou: Snowden's leaks underlined a longstanding academic imperative to problematize the nature and extent of state surveillance and highlight the risks for the society and democracy. The leaks received heavy media coverage but this focused mainly on discourses of securitization. How would you reflect on the Snowden leaks at this moment some months on?

Mark Andrejevic: The Snowden leaks revealed what people who had been paying attention had long suspected: that once you put information online or use an online platform, you have lost control over that information. What was striking about the media response to these revelations was that it was almost taken for granted that private companies already have all of this information. This fact – important as it is – was not the primary source of the concern, which was directed toward the fact that the government could access all of this data without warrants. I understand the reason for differential levels of concern, given that government information collection is centralized and that the state has different types of power over citizens than commercial organizations. However, it is still striking to me the way in which the perceived violation (posed by government intrusion) nonetheless preserves the norm (of comprehensive commercial data collection). The response was not: 'wow, look how much detailed information is stored up about everyone in the vast databases of the private sector.' But rather: 'isn't it alarming that the government is accessing all of this information – without warrants.' And it is – but once that data is stored, it will become a target for the surveillance community one way or another. That's pretty much a given. So the further question – that did not receive as much attention as it should have – is, 'why are we building our information infrastructure on the back of a system that fosters this kind of data warehousing in the first place?' This seems to me one of the more neglected questions of our time. Perhaps the most astounding aspect of the leaks is how little change has transpired in the data collection environment. Data capitalism, like finance capitalism, is allowed to continue all but un-harassed because of the role it plays in the contemporary economy.

PT: In the UK, the Digital Economy Bill (soon to be Act) seems to clearly legitimize the extensive state surveillance practices Snowden revealed by establishing a data-driven governance. What are the challenges and risks for citizens everywhere of this UK legislative development?

MA: It seems inevitable to me that we are entering an era in which states will have unprecedented access to information about citizens (and their environments). In the database era, it's harder to silo information than it once was, and there is a tendency to try to continuously combine databases (across government departments, across the online/offline divide, and so on). I think there are times when the public sector looks at the private sector and feels comparatively disadvantaged, not least because there has been an epochal shift in where data resides in society. Once upon a time the government and public institutions were the primary repositories of the data generated by society. Now the private sector has galloped ahead, and is not subject to the same types of controls and accountability that had developed over time to govern the public sector. It is not surprising that governments, including that in the UK, are embracing many of the strategies that have become commonplace in the private sector – including data migration and function creep (sharing data collected for one purpose with other departments for other purposes).

I think that some developments and practices (privacy by design, use of encrypted browsers, etc.) might slow or thwart aspects of this process, but the overall trajectory seems clear and unavoidable. This means that accountability becomes crucially important. To date, accountability practices have not kept up with the pace and scope of the development of monitoring practices. This is one of the reasons that 'leaking' has come to play an increasingly important role in our media and information environment – because 'legitimate' forms of accountability are either non-existent or dysfunctional. What has made emerging forms of surveillance seemingly irresistible – even to end users – is that they are ushered in on the promise of convenience. The platforms and applications upon which we are becoming increasingly dependent have data collection baked into them. The affordances of interactivity, of smart spaces and devices, and even of information management systems all rely on increasingly comprehensive forms of data collection. Unsurprisingly, then we find ourselves confronting what might be described as 'data collection creep' in both the public and private sectors. That is applications and services, both public and private, routinely expand the type of information they collect. Even if they don't need it for the purpose at end, they imagine that they can find myriad uses for it somewhere down the road.

PT: In one of your latest papers (Andrejevic, 2017) you discuss the shift to predictive policing. What are the implications of such a development for democracy and citizenship?

MA: I think we need to replace discourses and practices of pre-emption with those of prevention. I use these terms to suggest that discourses of pre-emption tend to focus on real-time interception without much of an emphasis on long-term, underlying, or structural causes. Prevention, by contrast, assumes the possibility of understanding and intervening at the level of the social and the political. Pre-emption is technocratic, which means that it promises technological solutions to social problems. Prevention, in the sense that I'm using it, is political, insofar as it asks us to think about how we might want to address the underlying social influences that shape identified social problems. Pre-emption promises to nip crime in the bud by sending police to the right place at the right time to stop an imminent crime – but it tends to take for granted the overall level of criminality. Prevention seeks to transform this overall level: with enough prevention, it might be possible to lower the need for pre-emption. Pre-emption, insofar as it fails to reach the level of underlying causes, can never create the conditions for its own obsolescence: it just ramps up the demand for more surveillance, more data, and more processing power.

Pre-emption has its uses: there surely are inexplicable and incomprehensible events whose causes are difficult to discern and address, but they also tend to be quite hard to predict. Pre-emptive strategies are important but they should not be used as an alibi for neglecting to

engage with underlying causes. This shift is a familiar move by the proponents of the so-called War on Terror, who have made it taboo to inquire about possible causes and therefore to bring to bear political discourses of prevention. Instead we are told: 'do not try to understand' (because this would be a form of complicity); rather trust the authorities with increasingly powerful forms of surveillance and increasingly aggressive and un-accountable strategies of pre-emption. I am terrified of terrorism and want to see it prevented as much as anyone, but I believe that this requires also addressing underlying causes in the realms of the political and the social. That some acts might be beyond the reach of analysis does not mean that all of them are.

PT: The discourse of securitization and the dominance of state-security seems to lead to the widespread acceptance of the 'nothing to hide, nothing to fear' security mantra. What are your thoughts on this and do you see any signs of resistance or greater awareness appearing?

MA: Daniel Solove (2011), among others, has done a good job of dismantling the 'nothing to hide' argument. He argues that the flawed premise of such an argument is that privacy is solely about secrecy, narrowly construed – that is, the attempt to hide unsavoury or 'bad' facts about oneself. I'd push the argument further, that the 'nothing to hide' argument ignores power relations and assumes that only unsavoury facts can be used against someone. This, of course, is refuted by contemporary media practices that seek to turn perfectly banal facts about our daily lives into instruments of manipulation and inclusion or exclusion. The long history of bias, discrimination, and oppression indicates that even information that we don't think of as private can be turned against us. Indeed, the notion that we need only to be concerned if we are doing something 'wrong' relies on the ideal of state and commercial apparatuses that have been purged of any forms of discrimination – a truly utopian ideal, that has no basis in actually existing societies and their histories. The nothing to hide mantra might be turned back around onto the security apparatus itself. If we have nothing to fear from monitoring, than surely the monitors would be willing to open themselves up to scrutiny. Indeed, any functioning democracy would need to have its surveillance apparatuses subject to meaningful forms of monitoring and accountability. Certainly there are logistical issues here: some forms of scrutiny might interfere with intelligence operations in real time. But this should not exempt such operations from subsequent scrutiny. In the end, I'm not particularly optimistic – the monitoring technology is becoming so pervasive, so comprehensive, and so reliant upon the information and communication systems of everyday life that a total surveillance society looks all but inevitable.

PT: Arguably, the digital nature of everyday transactions and interactions result in a participatory surveilled society. Data are gathered not solely by state apparatuses such as CCTV cameras and body-scanners but rather more by personal digital gadgets such as smartphones. Do you think technology itself might have potential to provide an answer to the misuse of mass data collection practices?

MA: I think we need a political solution and technology does not provide such solutions on its own. We live in a society that is so strongly shaped by the economy, and the economy is becoming increasingly reliant upon digital devices and platforms that allow for the information-based rationalization of almost every sphere of social existence. The hyper-efficiency and productivity of contemporary life rely on the automated collection and processing of increasingly detailed data sets. At the same time a growing portion of our social, professional, and personal lives are taking place online, redoubling themselves in the form of data. The only answer the techno-economic imperative provides here is: more data collection, faster.

There is a temptation to provide technological answers at the individual level – but this offloads the problem onto end users, making privacy their responsibility. I'm all for individual responsibility, etc., but I am wary of this approach when the problem at issue is a societal

one. Trying to fight pollution at the receiving end (getting people to test their own water, purchase gas masks, maybe one day to buy tanks of clean air for their homes) doesn't make sense. I think something similar is true of the changing information environment. We need to address the issue at the socio-political level, even if this need is anathema to the current climate of neoliberal individualism.

Much hinges on the notion of 'misuse' in the question above. When it comes to privacy, misuse is framed as illegal forms of intrusion and hacking: stealing personal data, identity theft, fraud, etc. Interestingly, we do find ways to address these issues without making them exclusively the responsibility of the end user. That's because there is an economic imperative at work: companies want to make sure that their systems are trusted, otherwise they run the danger of losing customers/users.

But the core issue here is what we mean by 'misuse' – and how this very definition might serve as an alibi for what counts as accepted use ('non misuse'). Identity theft is a misuse – we can build agreement around that. But what about mining data to determine moments of emotional vulnerability to advertising appeals (something Facebook has been accused of doing); or using data to exclude people who fit a predefined risk profile from private medical coverage? What about the use of existing databases to guide the allocation of policing forces, to assess risk or guide the sentencing of convicted criminals? How might the proper 'use' of information in these contexts 'launder' historical forms of bias by building them into algorithmic decision-making processes? What kind of processes do we need to have in place as a society to hold the algorithms accountable? Social sorting for a whole range of purposes is the 'use' associated with many data mining regimes – and this is a use that those committed to social justice and democracy are concerned about.

PT: Recent studies such as Stoycheff's (2016) suggest that mass surveillance can result in self-restriction of self-expression so that minority views are forcefully silenced with serious implications for participation and democracy. What's your opinion concerning the argument that privacy is necessarily always traded off against security?

MA: It's interesting that trade-off hasn't been turned back upon the surveillance apparatus itself. If we want a secure intelligence sector – it must also give up a certain amount of privacy: it cannot operate under the cover of total immunity from scrutiny and accountability. For their own purposes, security agencies actually equate privacy and security: they want to operate in conditions of total secrecy, indefinitely. Their guiding assumption in this regard is that they stand above the fray: that because they are acting in the name of security, they can be exempted from suspicion in a way that those they monitor cannot. History tells us this assumption is false. Security requires both some degree of privacy – but also some degree of scrutiny – and this holds equally for those who are being monitored and those who are doing the monitoring. It is important that, as a society, we are not simply told 'trust us' by those in power – but that we guarantee the institutional structures and practices that hold power accountable.

PT: Lastly what would you say is the responsibility of the academic critical community to say and to do when it comes to people's engagement concerning the implications of surveillance in our apparently neoliberal/populist environment. How can we reach out to the lay public that may be informed exclusively by mass media that so often oversimplify the risks for the population or engage with media practitioners that do not start out with an alternative viewpoint? Is this an important research agenda or would you highlight others as priorities?

MA: I do think this is a crucial research agenda – and one that the academy is uniquely positioned to undertake. The challenge is no longer to bring the scale and intensity of monitoring practices to light: the media have been doing a pretty good job of this lately. The real contemporary challenge is to provide ways of understanding the long and short term consequences

of data driven social sorting (and its automation). In this regard, work on algorithmic accountability is crucial in helping to expose the way in which bias and discrimination work their way into automated decision-making processes. It will become increasingly important to hold such processes accountable, rather than taking for granted their alleged effectiveness. As always, interrogations of power relations are critical to any investigation of the collection and use of data. The Internet of Things, that enables the communication and exchange of information of all digital devices in one's household for example, is not the logical outgrowth of a drive for interactivity: it is a strategy for control and rationalization (via the 'tyranny of convenience' in some quarters, and the tyranny of authoritarianism in others).

Competing Interests

The author has no competing interests to declare.

References

Andrejevic, M. (2004). *Reality TV: The Work of Being Watched*. Lanham, Maryland: Rowman & Littlefield.

Andrejevic, M. (2007). *iSpy: Surveillance and Power in the Interactive Era*. Lawrence, KS: The University Press of Kansas.

Andrejevic, M. (2013). *Infoglut: How Too Much Information Is Changing the Way We Think and Know*. New York: Routledge.

Andrejevic, M. (2017). Digital Citizenship and Surveillance|To Preempt A Thief. *International Journal of Communication*, 11: 879–896.

Solove, D. J. (2011). *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven: Yale University Press.

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. *Journalism & Mass Communication Quarterly*, 93(2): 296–311. DOI: https://doi.org/10.1177/1077699016630255

How to cite this article: Troullinou, P. (2017). Rethinking Privacy and Freedom of Expression in the Digital Era: An Interview with Mark Andrejevic. *Westminster Papers in Communication and Culture,* 12(3), 72–77, DOI: https://doi.org/10.16997/wpcc.270

Submitted: 28 September 2017 **Accepted:** 28 September 2017 **Published:** 31 October 2017