Introduction to Special Theme Veillance and transparency

Bakir, Vian; Feilzer, Martina; McStay, Andrew

Big Data and Society

DOI:
10.1177/2053951717698996

Published: 15/03/2017

Publisher's PDF, also known as Version of record

Editorial

BIG DATA & SOCIETY

Big Data & Society
January–June 2017: 1–5

DOI: 10.1177/2053951717698996
journals.sagepub.com/home/bds
SAGE

Introduction to Special Theme Veillance and transparency: A critical examination of mutual watching in the post-Snowden, Big Data era

Vian Bakir[1], Martina Feilzer[2] and Andrew McStay[1]

Abstract

Introducing the Special Theme on *Veillance and Transparency: A Critical Examination of Mutual Watching in the Post-Snowden, Big Data Era,* this article presents a series of provocations and practices on veillance and transparency in the context of Big Data in a post-Snowden period. In introducing the theoretical and empirical research papers, artistic, activist and educational provocations and commentaries in this Special Theme, it highlights three central debates. Firstly, concerning theory/practice, it queries how useful theories of veillance and transparency are in explaining mutual watching in the post-Snowden, Big Data era. Secondly, it presents a range of questions concerning norms, ethics, regulation, resistance and social change around veillance and transparency. Thirdly, it interrogates the upsurge in veillance and transparency discourses and practices post-Snowden, and asks whether they are adequate to the task of educating and engaging people on abstract and secretive surveillance practices, as well as on the possibilities and pitfalls of sousveillance.

Keywords

Equiveillance, Snowden, sousveillance, surveillance, transparency, veillance

Provocations and practices on veillance and transparency

Veillance is Steve Mann's (2013) term for processes of mutual watching and monitoring by surveillant organizations and sousveillant individuals. Surveillance involves monitoring from a position of political or commercial power by those who are not a participant to the activity being watched (for instance, CCTV cameras, undercover policing, sentiment analysis and programmatic tools used by marketing companies and intelligence agencies). By contrast, sousveillance (Mann, 2005) involves monitoring from a position of minimal power, and by those who are participating in the activity being watched or sensed. Sousveillance takes several forms. *Personal sousveillance* is a form of watching without political or legal intent (such as sharing selfies, life-logging and using wearables). *Hierarchical sousveillance* has political or legal intent targeted at the powerful (such as when protesters use their smartphone videos and social media to monitor police at demonstrations, or when insider whistle-blowers leak incriminating documents). The past decade has seen an intensification of veillant forces from all quarters (state, commercial, civil society, citizens), leading to questions of whether it is possible, or desirable, to resist being watched. Accepting the inevitability of surveillance, and the rapid growth of sousveillance, Mann (2013) envisages a state of *equiveillance*, where there is equality between surveillant and sousveillant forces, leading to a *transparent* society. While a balanced condition of mutual watching may be unrealisable in

[1]School of Creative Studies and Media, Bangor University, Bangor, UK
[2]School of Social Sciences, Bangor University, Bangor, UK

Corresponding author:
Vian Bakir, College of Arts and Humanities, Bangor University, JP Building, Bangor LL57 2DG, UK.
Email: v.bakir@bangor.ac.uk

practice, this Special Theme critically examines a range of veillant forces, resistances and tensions, seeking to understand these operations in the context of Big Data in a post-Snowden period.

In June 2013, the leaks by national security whistleblower, Edward Snowden, exposed governments' secret mass surveillance of ordinary citizens' digital footprints in multiple liberal democracies. The leaks revealed that signals intelligence agencies such as the USA's National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ) collect data in bulk from the servers of US global telecommunications companies, compelling them to secretly hand over this data; and that intelligence agencies secretly tap fibre-optic cables carrying internet traffic. The data intercepted and collected includes the content of communications (such as emails, instant messages and full web browsing histories); and metadata information about the communication (for instance, who the communication is from and to whom; from where it is sent, and to where; the record of web domains visited; and mobile phone location data). These disparate data streams, which can be acted upon in real time and/or stored for subsequent analysis (GCHQ, 2012; NSA, 2001), reveal much about a person's actions, thoughts and intentions. Use of Big Data analytics is also common in commercial organisations to better target advertising and marketing content. However, while intelligence and security agencies seek to identify criminals and pre-empt specific threats thereby making individual identification a key goal, commercial entities often try to avoid identifying people so as not to fall foul of privacy regulations, instead using analytics to deliver insights into groups of similar people rather than individuals (McStay, 2017).

These security and commercial practices lead us to suggest: *through various veillant forces, we live in a techno-cultural condition of increased transparency*. As cultural philosophers observe, transparency takes various forms (Bakir and McStay, 2015; Birchall, 2014; McStay, 2014; Vattimo, 1992). Historically, transparency has been a liberal principle. As explored in McStay (2014), it is an enlightenment norm advocating accountability and public inspection of state power (Mill, 1962 [1859]), an exemplar being journalism acting as the Fourth Estate. In modern terms, this transparency arrangement also holds that law-abiding citizens should be able to exercise personal choice/control over their own visibility to real or machinic others. Related, Bentham advocates transparency of both public and private processes for the general good, proposing that, 'Every gesture, every turn of limb or feature, in those whose motions have a visible impact on the general happiness, will be noticed and marked down' (1834: 101). The impact of this more *radical transparency* arrangement is that, as these are socially or legally agreed norms, citizens have low individual control over their own personal visibility. *Forced transparency* is the pre-Snowden condition of surveillance that secretly demands high visibility of citizens to maximise the greater good of national security. Unlike a radical transparency arrangement, *forced transparency* largely operates without citizens' knowledge or consent, nor with sufficient oversight of surveillant entities to win social trust.

Our key debates

Through multiple veillant forces, we clearly live in a techno-cultural condition of increased transparency, but what is less clear are the wider implications. As such, we have assembled theoretical and empirical research papers, artistic, activist and educational provocations and commentary to explore three sets of questions that we posed to contributors.

1. Theory-practice

How useful are theories of veillance and transparency in explaining mutual watching in the post-Snowden, 'Big Data' era? Accepting the inevitability of surveillance, Mann and Ferenbok (2013: 26) seek to counter-balance surveillance by increasing sousveillant oversight from below ('undersight') facilitated through civic and technology practices such as better whistle-blower protection, public debate, participatory projects and systems innovations. Once this balance is achieved, they suggest that such a society is both equiveillant and transparent. But can more sousveillance really counter-balance surveillance? What about reincorporation of sousveillant data by surveillant practices? Is it possible to resist veillant forces in contemporary digital societies? Does the answer lie in *counterveillance*, Mann's (2013) term for blocking both surveillance and sousveillance? Does the answer lie in *univeillance* (Mann, 2013) where surveillance is blocked but sousveillance is enabled (exemplified by default encryption adopted by technology corporations post-Snowden)? Our Special Theme's research papers respond to veillance theories in different ways.

Dan McQuillan's analysis of algorithmic paranoia dismisses Mann's concept of veillance as the wrong sort of metaphor for the forms of seeing introduced by Big Data algorithms. McQuillan observes that the data produced by machines is most often 'seen' by other machines in order to find correlations to enable prediction in financial, social or security risk situations; and that this seeing reproduces the prejudices of its input. For McQuillan, this induces a psychological state of algorithmic paranoia that, if it is to be

challenged, requires that we change *how* we see (rather than, for instance, blocking certain types of veillance); and that this demands critical work on algorithms to minimise algorithmic prejudices.

Other research papers in this Special Theme adapt the veillance metaphor to explore specific variants of mutual watching. Critiquing the idea that equiveillance captures our contemporary condition of mutual watching, Clare Birchall advances the notion of *shareveillance* in her discussion of subjectivity, open data (that governments willingly share with citizens) and closed data (such as that collected by intelligence agencies). For Birchall, the contemporary condition of mutual watching is not an evenly poised balance between surveillant and sousveillant forces. Rather, we are in a state of *shareveillance*: an 'anti-politicised role the datafied neoliberal security state imagines for its public; the latter is configured more as either a flat dataset or a series of individual auditor–entrepreneurs than as a force with political potential'. To challenge this state of affairs, she offers suggestions for how data sharing could be more ethically distributed, and unpacks what citizens' 'right to opacity' might mean in the digital context.

Focusing on the pre-crime assemblage – an automated, fluid disciplinary space designed to modify and monetise human behaviour to pre-empt harmful futures – Peter Mantello advances the notion of *ikea-veillance*: 'a do-it-yourself, voluntary opt-in approach to algorithmic governance' that contributes to the pre-crime assemblage. Examining case studies from the USA, Australia and Japan, he concludes that the masses, rather than seeking resistance, are complicit in voluntarily trading privacy or sacrificing anonymity for product discounts, benefits and services, or to self-enhance notions of civic-minded servitude.

Piro Rexhepi's Early Career Researcher essay sees Big Data surveillance as tantamount to what she terms *sur/violence* (for instance, drone strikes killing people via metadata identification). By focusing on peripheral political spaces, Rexhapi queries the ability of sousveillance to destabilise and disrupt *sur/violence*. In the periphery, surveillance is not framed by middle class concerns over privacy, democracy and civil society, but is a matter of life and death.

2. Norms, ethics, regulation, resistance and social change

Are existing mechanisms of regulation and oversight able to deal with the security states' practices of forced transparency, and corporations' drive to maximise data collection for commercial gain, or is resistance required from other quarters? How healthy are current sousveillant civic and technology practices, and where do they need strengthening? What, if anything, can or should we do about practices of watching that operate without informed consent or adequate processes of accountability?

Anthony Mills and Katherine Sarikakis address these questions through the lens of investigative journalism. They argue that legislative change towards stronger state surveillance across multiple countries disrupts the preconditions for a strong democracy based on free media and free citizens. Their examination of journalists' experiences with surveillance in non-Western and Western countries finds that investigative journalists have been intimidated through surveillance; but that they fight back through often-fraught cooperation with hacktivists, and through self-directed protection of communications and sources.

Lina Dencik, Arne Hintz and Jonathan Cable address these questions through the lens of British social justice activists. They find that their resistance to state surveillance largely takes shape in techno-legal responses to encryption, and policy advocacy around privacy and data protection. They find this problematic because of activists' ambiguity around technological resistance strategies, with critical responses to Snowden's leaks largely confined to expert communities. Introducing the notion of *data justice*, they suggest that resistance to surveillance needs to be reconceptualised and connected to broader social justice agendas.

Focussing on advertising and the net rise in *empathic media* (namely, technologies that track bodies and react to emotions and intentions), Andrew McStay advances the notion of *emotiveillance*: the use of biometrically sensitive technologies to infer peoples' emotions. McStay examines the use of biofeedback in advertising, both for in-house emotion detection of responses to adverts, and for digital out-of-home advertising that reacts to peoples' emotional expressions. Through survey work, he finds that few British citizens are comfortable with having data about their emotional state linked with personal information. Setting this insight against industry practices that claim not to use personal data, he argues that rather than fixating on privacy invasions based on identification, regulators and self-regulators should attend to the principle of intimacy, as this is a core characteristic of data about emotions.

Focusing on regulations and rights, Yvonne McDermott-Rees' commentary observes that the Charter of Fundamental Rights of the European Union entered into force in 2009. This created a fundamental right to data protection, standing as distinct to the right to privacy. In examining this new and unique right to data protection, she posits that its underpinning principles reflect key European legal values, namely: privacy, transparency, autonomy and non-discrimination. She notes the challenges in

implementing this right in an era of ubiquitous veillance practices and Big Data. These include the volume of data on the self that is 'volunteered' by others, such as via social media, which means that a consent-based model cannot ensure protection of one's data; and finding the balance between the security state's dataveillance and the right to data protection.

3. Representation, discourse and public understanding

Snowden's leaks provoked libertarian pro-privacy discourses and practices: encryption software, courses in how to use these, and encrypted consumer technologies have proliferated. The leaks also provoked discourses and practices concerning public accountability of intelligence agencies. Arguments were made for greater transparency of regulation concerning intelligence agencies' surveillant powers, and for translucency rather than transparency to reveal the general shape of the state's secrets rather than their details. These discourses have manifested in multiple sites including investigative journalism (for instance, *The Guardian*, *The Intercept*), documentaries (Laura Poitras' (2014) *CitizenFour*), feature films (Oliver Stone's (2016) *Snowden*), think tank reports (Simcox, 2015), internet and technology firms' promoting their privacy-enhancing technologies and lobbying for legislative change on bulk data collection and transparency (The Privacy and Civil Liberties Oversight Board, 2014), public reports and statements by intelligence agencies and their official oversight bodies (Clapper, 2013; Intelligence and Security Committee, 2015), and NGOs' representations as a wide range of civil liberties, human rights, privacy, transparency and press freedom groups were consulted by post-Snowden surveillance review boards (Bakir, 2015). While we have seen an upsurge in veillance and transparency discourses and practices post-Snowden, *how do they position the sur/sous/veillant subject; and are they adequate to the task of educating and engaging people on abstract and secretive surveillance practices, as well as on the possibilities and pitfalls of sousveillance?* These questions are addressed in our commentaries by people at the coal-face – educators, artists, engineers and legal experts (the categories overlap).

Evan Light's Snowden Archive-in-a-Box is an offline wireless network and web server providing private access to a replica of the Snowden Digital Surveillance Archive – a digital archive that hosts all the published leaked documents from Snowden as well as the newspaper articles that published the leaks (2013–2015). Light explains how Archive-in-a-Box is both a research tool and a tool for public education on data surveillance.

Derek Curry and Jennifer Gradecki's interactive artwork, *Crowd-Sourced Intelligence Agency*, innovatively contributes toward an informed public debate about large-scale monitoring of open source, social media data and provides a prototype for counterveillance and sousveillance tools for citizens. By demonstrating that what a dataveillance program 'sees' when it 'reads' social media posts is nothing like what a human being sees, they aim to create a debate over current dataveillance technologies, and the efficacy and ethics of mass automated dataveillance.

Benjamin Grosser's interactive artwork, *Tracing You*, includes data provided by *Google*'s Maps Service to present a website's best attempt to see the world from its visitors' viewpoints. This makes transparent the potential visibility of one's present location, and gives each site visitor the ability to watch other visitor 'traces' in real time. By making its surveillance capacity and intention overt, this computational surveillance system provokes questions about how the architecture of networks affects our own visibility both within and outside of the network.

Yuwei Lin 's commentary reflects on her experiences of teaching privacy and surveillance to media arts practice university students in the UK. Reflecting on the creative media practices, attitudes and behaviours of her students, her commentary raises questions about the role educators play in enriching public engagement with critical thinking about Big Data.

Ben Brucato's commentary on Big Data, transparency and measuring and representing killings by the US police notes that there are few national, longitudinal studies or records of police use of force. This perceived lack of transparency amplifies concerns that many of these killings are unjustified and signals a deliberate avoidance of accountability. He considers efforts by journalists and activists to construct databases that document and measure police violence, particularly in terms of how they exemplify the new transparency.

Last but not least, Steve Mann's commentary draws our attention to the need for bottom-up transparency in computer engineering, arguing that scientists have the right and responsibility to be able to understand the instruments that they use to make their discoveries. He posits that veillance is important not just in human–human interaction (such as people watching other people) but also in terms of Human–Computer Interaction. Advancing the idea that "'Little Data'' is to sousveillance (undersight) as ''Big Data'' is to surveillance (oversight)', he suggests that we need *Sousveillant Systems*, namely forms of Human–Computer Interaction in which internal computational states are made visible to end users, when and if they wish. He envisages an interim solution (an app called LUNATIC) by which a virtual personal assistant interacts on our behalf with erratic websites or servers,

thereby making people aware of the need for *Sousveillant Systems*.

To conclude, this Special Theme highlights the importance of inter- and multi-disciplinary debate on current forms of mutual watching. We argue that the veillance field is multi-perspectival and characterised by tension. To understand contemporary data transparency by focusing on surveillance alone is to misunderstand modern watching, sensing and data analytics, although it remains to be seen whether we will ever see Mann's equiveillance in practice. However, we do not subscribe to a politics of pessimism, but end by calling for continued critical, technical, legal, political, educational and artistic intervention into the veillance field.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: the Economic and Social Research Council (ESRC) Seminar Series (2014–16), *DATA – PSST! Debating & Assessing Transparency Arrangements: Privacy, Security, Surveillance, Trust*. Grant Ref: ES/M00208X/1.

References

Bakir V (2015) ''Veillant panoptic assemblage'': Mutual watching and resistance to mass surveillance after Snowden. *Media and Communication* 3(3): 12–25 (DOI: 10.17645/mac.v3i3.277.

Bakir V and McStay A (2015) Theorising transparency arrangements: Assessing interdisciplinary academic and multi-stakeholder positions on transparency in the post-Snowden leak era. *Ethical Space: the International Journal of Communication* 3(1): 24–31.

Bentham J (1834) *Deontology*. London: Rees, Orme, Brown, Green and Longman.

Birchall C (2014) Radical transparency? *Cultural Studies, Critical Methodologies* 14(1): 77–88.

Clapper J (2013) Official statement. *Welcome to IC on the Record*. Available at: https://icontherecord.tumblr.com/post/58838654347/welcome-to-ic-on-the-record (accessed 3 March 2017).

Government Communications Headquarters (GCHQ) (2012) *News*. Available at: http://www.spiegel.de/media/media-34103.pdf (accessed 3 March 2017).

Intelligence and Security Committee (2015) *Privacy and Security: A Modern and Transparent Legal Framework*. London, UK: House of Commons. Available at: http://isc.independent.gov.uk/ (accessed 3 March 2017).

Mann S (2005) Sousveillance and cyberglogs. *Presence: Teleoperators & Virtual Environments* 14(6): 625–646.

Mann S (2013) *Veillance and Reciprocal Transparency: Surveillance versus Sousveillance, AR Glass, Lifeglogging, and Wearable Computing*. Available at: http://wearcam.org/veillance/veillance.pdf.

Mann S and Ferenbok J (2013) New media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance & Society* 11(1/2): 18–34.

McStay A (2014) *Privacy and Philosophy: New Media and Affective Protocol*. New York, NY: Peter Lang.

McStay A (2017) *Privacy and the Media*. London: Sage.

Mill JS (1962 [1859]) *Utilitarianism, On Liberty, Essay on Bentham*. London: Fontana Press.

National Security Agency (NSA) (2001) *Business Records (BR) FISA – Course Welcome*. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH017d/9ecf019c.dir/doc.pdf (accessed 3 March 2017).

Poitras L (2014) *Citizenfour*. Praxis Films, Participant Media, HBO Films.

Simcox R (2015) *Surveillance after Snowden: Effective Espionage in an Age of Transparency*. London: The Henry Jackson Society.

Stone O (Dir.) (2016) *Snowden*. Open Road Films.

The Privacy and Civil Liberties Oversight Board (2014) *Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT ACT and on the Operations of the Foreign Intelligence Surveillance Court*. Available at: https://www.pclob.gov/events/2014/january23.html (accessed 3 March 2017).

Vattimo G (1992) *The Transparent Society*. Cambridge, UK: Polity Press.

This Editorial is an introduction to the special theme on Veillance and Transparency. To see a full list of all articles in this special theme, please click here: http://bds.sagepub.com/content/veillance-and-transparency.