CFP: *Big Data and Society*
Proposed Special Issue on Veillance and Transparency: A Critical Examination of Mutual Watching in the Post-Snowden, Big Data Era
Guest Editors: Vian Bakir, Martina Feilzer, Andrew McStay (Bangor Univ.)

We invite papers for a proposed Special Issue in *Big Data and Society*, Sage's inter-disciplinary, open access, peer-reviewed scholarly journal that explores the social implications of Big Data from social sciences, humanities and computing perspectives.

Our central proposition: today we live in a techno-cultural condition of increased and normalised transparency through various *veillant* forces of mutual watching.
Our central question: what are the technical, social, economic, political, legal, ethical and cultural implications of this situation?

Drawing on the many academic disciplines that deal with issues of veillance and transparency, we seek theoretical and empirical academic papers; artistic, activist and educational provocations (the journal can link to digital versions of these); and shorter commentary from the wide range of actors involved in these debates (including data regulators, intelligence and security services, private companies, NGOs, politicians and journalists).

Specifically, we are interested in the following questions (each unpacked further below):

1. *On Theory-Practice:* How useful are theories of 'veillance' in explaining transparency practices in the post-Snowden, 'Big Data' era?
2. *On Ethics, Values and Norms:* What, if anything, can or should we do about practices of watching that operate without informed consent or adequate processes of accountability?
3. *On Regulation, Power, Resistance and Social Change:* Are existing mechanisms of regulation and oversight able to deal with nation-states' desire for forced transparency, or is resistance required from other quarters?
4. *On Representation, Discourse and Public Understanding:* What socio-cultural discourses and practices on veillance and transparency prevail; 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?

KEY TERMS

Veillance
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 (eg CCTV cameras, sentiment analysis and programmatic tools used by marketing and state intelligence agencies). By contrast, *sousveillance* involves monitoring from a position of minimal power, and by those who are participating in the activity being watched. Sousveillance takes several forms. *Personal sousveillance* is a form of watching without political or legal intent (such as ubiquitous social media usage, tweeting what we've had for dinner, selfies, life-logging, wearables, and transparency of everyday life). *Hierarchical sousveillance* has political or legal intent (such as when protesters use their mobile phone cameras to monitor police at demonstrations, or when 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 these veillant forces. Accepting the inevitability of surveillance, and the rapid growth of sousveillance, Mann envisages a state of *equiveillance*, where there is equality between surveillant and sousveillant forces. What, however, does this proposition mean in an age not just of 'Big Data', but also post Snowden?

Big Data
Big data is the tracing of multiple and often strange behavioural correlations that allow strategic opportunities for companies and surveillance organizations. The term 'big data' was coined by tech'

industry analyst Doug Laney (2001), who expounds the three 'Vs' of big data: volume, velocity and variety. This refers to an increase in *volume* of data, the *velocity* by which it moves and needs to be reacted to, and the *variety* of forms it comes in. Although big data certainly involves a great deal of information, 'big' is a relative term, and perhaps even more significant are the processes of aggregation, correlation and cross-referencing to find non-obvious, valuable relationships to assist in planning, decision-making, security and surveillance.

Big Data Post-Snowden

Volume, depth and history. The 2013 leaks by US national security whistle-blower Edward Snowden revealed intelligence agencies' secret bulk data collection and storage of citizens' digital communications where at least one end of the communication is overseas. The aim of such bulk data collection is exploratory – 'to find linkages, patterns, associations or behaviours which might demonstrate a serious threat requiring investigation' (ISC 2015: 13).

Variety and range of sources that information is being collected from. Contemporary surveillance makes use of a range of information sources, not least our online data trails such as web-sites visited and transactional data (eg banking and consumer histories) and data that people generate about themselves and each other through their digital communications (eg via emails, social media postings, uploading data from wearables, and simply by having their mobile phone switched on).

Velocity and analytics processes that seek to better identify future terrorist threats. While intelligence agencies point out that their analytics programs facilitate discovery of unknown threats and reduce 'false positives', they say little on the specifics of their programs. However, what has been published of the Snowden leaks detail a range of analytics programs that intelligence agencies possess. See here for more context on big data, post-Snowden.

Transparency

Transparency takes a number of forms. *Liberal transparency* is, historically, a liberal and enlightenment norm that opens up machinations of power for public inspection (Bentham 1834), an exemplar being journalism acting as the Fourth Estate. *Radical transparency* opens up not just public processes but also the private lives of citizens for inspection, where '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' (Bentham 1834: 101 cited in McStay 2014). An exemplar of radical transparency is the Quantified Self movement, that aims, through collecting and sharing a variety of data that monitors the self (typically sleep, breathing and activity patterns), to achieve greater self-knowledge, well-being and health. Where radical transparency is enacted without citizens' knowledge or consent, we enter the domain of *forced transparency* where resistance to surveillance is tantamount to guilt, and where choice, control and autonomy are stripped away (McStay 2014). An exemplar of forced transparency is Snowden's revelations of signal intelligence agencies' bulk data collection without citizen knowledge or consent, and the now familiar meme that justifies this practice, 'nothing to hide, nothing to fear'. In a less dystopian vein, *equiveillant transparency* is achieved when the forces of surveillance and sousveillance balance out. What this balance might consist of, and whether it is achievable is debatable, but Mann and Ferenbok (2013: 26) suggest that sousveillance would be widespread, with sousveillant oversight from below (what they term 'undersight') facilitated through a range of strengthened civic and technology practices.

THE QUESTIONS UNPACKED

1. Theory-Practice

How useful are theories of veillance in explaining transparency practices 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? Furthermore, how healthy are current sousveillant civic and technology practices, and where do they need strengthening? For instance, the core principles of sousveillance are that individuals who sousveil must be participants in the activity being watched, as well as able to control the 'capture, processing, storage, recall, and transmission of sensory information' (Mann 2005: 636). But to what extent is such control a practical reality, especially post-Snowden? How can sousveillers resist reincorporation of their sousveillance by

surveillant practices? Does the answer lie in *counter-veillance*, Mann's term for blocking both surveillance and sousveillance (eg technologies that detect and blind cameras; or simply, total disengagement with networked technology by going 'off-grid'). Does the answer lie in *univeillance* (Mann 2013: 7) where surveillance is blocked but sousveillance is enabled (exemplified by default encryption recently adopted by big technology corporations like Apple, this encouraging people to communicate without fear of being surveilled)? What difficulties do high-tech counter-surveillance and univeillance solutions raise (eg digital literacy, and lack of normalisation of practices of secrecy/privacy), and are there better low-tech solutions available?

2. Ethics, Values and Norms

Mann (2015) uses his notion of *priveillance* – a term for the relationship between privacy and veillance that incorporates notions of accountability and care on the part of the watchers alongside the privacy of the watched. *What, if anything, can or should we do about practices of watching that operate without informed consent or adequate processes of accountability?* This includes intelligence agencies' mass collection of citizens' digital communications, with private corporations compelled to comply. It includes the tacit consent that the digital sector assumes is granted by people using their online services who blithely tick the small-print end user license agreements about what happens to their data, but that in reality amounts to enforced agreement rather than informed consent (McStay 2013). It includes individuals recording others (eg on mobile phones or smart-glasses) and sharing data on others through social media without their consent. This raises many questions concerning ethics, values and norms. For instance, if, as intelligence agencies claim, the privacy-security trade-off is real, what are the best ways of balancing lives possibly saved (by preventing terrorism) from lives daily invaded (through privacy infractions)? Does veillance inhibit (through self-censorship) or encourage (through connecting with like-minded people) freedom of speech and freedom of association? What sorts of veillance invasions do people care about, and what can they do about them? From liberal democracies to autocracies, what are the ethics, values and norms of contemporary *priveillance* practices?

3. Regulation, Power, Resistance and Social Change

Are existing mechanisms of regulation and oversight able to deal with nation-states' desire for forced transparency, or is resistance required from other quarters? Given the constant flow of data across the globe, security authorities cooperate ever more closely with each other through surveillant data- and intelligence-sharing agreements (eg GCHQ can receive communications data from their overseas partners, as authorised by the Intelligence Services Act 1994 (ISC 2015); and are inter-connected with private corporations such as internet and telecommunications providers through which the data flows. While national regulations pertain to govern intelligence agencies' access to internal and external communication flows (with internal communications being more stringently regulated), it has been argued that the distinction between internal and external communication is meaningless in an age of global, digital media flows, where most digital communications are routed through communications platforms owned and operated by providers overseas (especially the USA, eg Google, Facebook, DropBox); and where an email, for instance, sent between two people in the UK may well travel via a mirror server in the USA, Europe or Asia. UK intelligence agencies have clarified that they would classify communications as 'internal' if the sender and recipient were both in the UK regardless of whether the communication (eg an email) was routed through webmail services based abroad. However, they classify communications collected as 'external' when the location of the sender or recipient is unknown – which is the case for Google, YouTube, Twitter and Facebook posts (unknown recipients); when accessing a website whose web server is located abroad; and when uploading files to a cloud storage system overseas, such as Dropbox (Anderson 2015, ISC 2015; Simcox 2015).

Given the cross-border and global nature of this flow of information, regional actors such as the EU, the Council of Europe, and the UN are increasingly involved in regulating such data-sharing, protecting privacy and challenging excessive surveillance by security authorities. But, are existing mechanisms of regulation and oversight able to deal with hegemonic nation-states' desire for forced transparency, or capable of protecting individuals' rights to privacy? Indeed, is resistance to veillance meaningful or possible today at an individual (citizen or state) level, or is resistance best enacted through powerful private corporations? For instance, Communication Service Providers in the USA, worried about the pro-privacy public outcry and associated damage to their brands following Snowden's revelations, challenged the US government in court; and Google, Apple, Microsoft, Yahoo! And WhatsApp started to automatically provide encryption for their users. Is this a new form of neo-liberal corporate activism by libertarian corporations keen to 'Do no Evil' (Google), or merely the old story of

brand maintenance and corporate lobbying to protect market share?

4. Representation, Discourse and Public Understanding

What socio-cultural discourses and practices on veillance and transparency prevail; 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? For instance, Snowden provoked libertarian pro-privacy discourses and practices (encryption software, courses in how to use these, and encrypted consumer technologies have proliferated); discourses of public accountability of intelligence agencies (with arguments made for greater citizen involvement in intelligence agencies' oversight, and calls for transluscency rather than transparency to reveal the general shape of the state's secrets rather than their details); discourses of private accountability ('nothing to hide, nothing to fear'); and consumerist discourses on envaluing and monetizing one's own data flows (eg Ghostery and Disconnect flag up online commercial trackers and what they collect). These discourses have manifested in multiple sites post-Snowden, including investigative journalism (eg *The Guardian*, *The Intercept*), documentaries (*CitizenFour*), feature films (Oliver Stone's forthcoming film, *Snowden*), think tank reports (Simcox 2015), internet and technology firms' advertising 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 (ISC 2015, Clapper 2013), digital rights political parties (The Pirate Party), and anti-surveillance NGOs' representations (eg a wide range of civil liberties, human rights, privacy, transparency and press freedom groups were consulted by post-Snowden surveillance review boards and reports in the USA and UK). Public opinion has been variously measured through multiple opinion polls, and through far more in-depth citizen summits (eg those arising from the EU-funded SURPRISE project examining factors affecting public acceptance and acceptability of security-oriented surveillance technologies) (Pavone et al 2015). With this upsurge in socio-cultural discourse and practices on veillance and transparency post-Snowden, do citizens yet understand how their data is surveilled and sousveilled, and how they may take charge of this data flow? If not, how can we make people better understand, care about, and act on such issues?

References

Anderson, D. 2015. *A Question of Trust: Report of the Investigatory Powers Review*. June. Presented to the Prime Minister pursuant to section 7 of the Data Retention and Investigatory Powers Act 2014. OGL. https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/

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

Clapper, J. 2013. *Welcome to IC on the Record*. Office of the Director of National Intelligence. http://icontherecord.tumblr.com/post/58838654347/welcome-to-ic-on-the-record

ISC. 2015. *Privacy and Security: A Modern and Transparent Legal Framework*. House of Commons [12 March]. Intelligence and Security Committee. http://isc.independent.gov.uk/

Laney, D. 2001. *3-D Data Management: Controlling Data Volume, Variety and Velocity*. Application Delivery Strategies. Meta Group.

Mann, S. 2015. *Priveillance*. http://wearcam.org/mannventions-password-stefanosmannaz13/priveillance.htm

Mann, S. 2013. *Veillance and reciprocal transparency: surveillance versus sousveillance, AR Glass, Lifeglogging, and wearable computing*. http://wearcam.org/veillance/veillance.pdf

Mann S.2005. Sousveillance & cyberglogs. *Presence: Teleoperators & Virtual Environments*, *14*(6): 625–46.

Mann, S. & 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: Peter Lang.

McStay, A. 2013. I Consent: An Analysis of the Cookie Directive and its Implications for UK Behavioural Advertising. *New Media & Society*, *15*(4): 596- 611.

Pavone, V. et al. 2015. *D2.4 – Key factors affecting public acceptance and acceptability of SOSTs. Surprise. Surveillance, Privacy and Security*. http://surprise-project.eu/

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

The Privacy and Civil Liberties Oversight Board. 2014. *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. https://www.pclob.gov/events/2014/july02.html

SUBMISSION GUIDELINES/DEADLINES

Submission Details
Proposals of no more than 1000 words are invited for consideration and inclusion in this proposed Special Issue of *Big Data & Society* (BD&S). All papers should foreground why Big Data practices are important to their central argument, as outlined in this CfP.

Manuscripts should be 8,000 words for an Original Research Article, 3,000 words for a Commentary, and 1,000 words for an essay in the Early Career Research Forum section.

Proposals should be sent to the Guest Editors: v.bakir@bangor.ac.uk, mcstay@bangor.ac.uk, m.feilzer@bangor.ac.uk

Manuscript and Style Guidelines
As this is an online only journal, there are fewer restrictions on format, including the use of visualizations (which are encouraged, where this helps the explanation). Full guidelines are below: http://www.uk.sagepub.com/msg/bds.htm#Prep

Peer review
All submissions of Original Research Articles to BD&S are double-blind, and triple peer-reviewed. Anonymous peer review feedback will be accompanied by comments from the guest editors that draw on the central arguments of other papers selected for inclusion in order to enhance the coherence of the proposed Special Issue.
Commentaries, Early Career Research Forum submissions, and artistic, activist and educational provocations are reviewed by the Guest Editors.

Deadline for academic papers (original research articles and early career research forum essays)

- Proposal Deadline: 15 Oct 2015
- Notification of Acceptance: 1 Dec 2015
- Paper Deadline: 1 May 2016
- Reviews Returned: 31 Jul 2016
- Revised Paper Deadline: 1 Nov 2016

Deadlines for commentaries and artistic, activist and educational provocations:

- Proposal Deadline: 27 May 2016
- Notification of Acceptance: 1 Jul 2016
- Revisions Deadline: 1 Nov 2016

Anticipated Publication date for Special Issue: Jan/Feb 2017.