|  |  |  |
| --- | --- | --- |
| WB Crest | Seminar 6: Cohering Inter-disciplinary responses and rebuilding the agenda 20 May 2016 |  |

Seminar Summary

*This summary has been prepared with the help of PhD students Abigail Blyth from Aberystwyth University and George Petry from University of South Wales.*

[**Introduction**](http://data-psst.blogspot.co.uk/2016/05/welcome-to-data-psst-seminar-6-cohering_17.html) **by Martina Feilzer and Yvonne McDermott:** This seminar aimed to synthesise what we have learned from previous [Seminars 1-5](http://data-psst.bangor.ac.uk/policy.php.en); to decide on key messages for the general public and policy makers; and to think about how these ideas can be best communicated.

[**Vian Bakir**](http://data-psst.blogspot.co.uk/2016/05/seminar-6-vian-bakir-position-statement.html)discussed some of the outputs that have arisen from the Seminar Series, including the [website](http://data-psst.bangor.ac.uk/index.php.en), [blog](http://data-psst.blogspot.co.uk/), listserv, a related project on [public feeling on privacy, security and surveillance](http://data-psst.bangor.ac.uk/policy.php.en); a journal [special issue](http://data-psst.bangor.ac.uk/big-data-society.php.en), successful funding applications, and individual publications. One of the key aims of this seminar series was to better understand and theorise the nature of contemporary (post-Snowden) transparency. We started the Seminar Series by proposing a typology of three types of transparency; two originally identified by Bentham: Liberal and Radical Transparency, and one coined by McStay, that appears increasingly pertinent to today’s society: Forced Transparency, or transparency without consent or choice, and where accountability of surveillant organisations is insufficient to generate social trust. Pointing to Bakir and McStay’s recent [Ethical Space article](http://www.communicationethics.net/journal/v12n3-4/feat2.pdf), Bakir explained how, drawing on the range of positions held by the inter-disciplinary and multi-end user participants in the Seminar Series, they had since refined and added to that typology. By building in degrees of opacity, or ‘transclucency’, the typology now represents five positions, on transparency, each describing different combinations of (a) control over personal visibility, and (b) accountability of surveillant organisations. It can be used to identify what type of transparency arrangement we are currently in, and what sort we would like to be in.

Using the advertising industry practice of creative briefs, [**Andrew McStay**](http://data-psst.blogspot.co.uk/2016/05/seminar-6-andrew-mcstay-position.html)thenled the group in the difficult task of focusing down on what core messages we felt the public and policy-makers most needed to hear. There was a detailed discussion about whether our messages should be targeted at the general public, many of whom may not be engaged in these issues, or at a section of the public which already harbours some disquiet about surveillance but does not understand what is taking place. All agreed that the tone of these messages would be important, in particular the need to avoid coming across as paternalistic or patronizing to the public. The tone to be taken with policy makers was more controversial: some participants favoured a non-confrontational, solutions-oriented approach, while others felt that the message should be strong, and that confrontation need not be avoided at all costs.

**Roundtable 1 – explaining complex security, privacy & transparency practices to publics**

This examined how creative techniques can be utilised to explain complex practices of data sur/sous/veillance to the public and policymakers. [**Ronan Devlin**](http://data-psst.blogspot.co.uk/2016/05/ronan-devlin-seminar-6-position.html) began by discussing the art project *Veillance*, which demonstrates the problems of data ownership by physically showing people what information is collected from their mobile devices during five minutes of online browsing. Of course, there are ethical dilemmas involved in such a project, and these were also clearly considered. More broadly, the *Veillance* project highlights the role of art in addressing the themes of this seminar series: art can render an abstract idea (such as data flows) visible, make it comprehensible, and provide a place of safe simulation.

By focusing upon the internet of things, such as ‘smart’ home systems which raise multiple legal and political questions, [**Lachlan Urquhart**](http://data-psst.blogspot.co.uk/2016/05/seminar-6-position-statement-lachlan.html) discussed ‘privacy by design’ (which makes encryption of data the default) and how this can be made clearer to those engineers creating such systems. Although this had proved difficult, privacy by design playing cards have been created, allowing complex legal terms to be fully understood.

[**Yuwei Lin**](http://data-psst.blogspot.co.uk/2016/05/seminar-6-position-statement-yuwei-lin_17.html) showed videos her Undergraduate students had created about privacy and surveillance, highlighting how students express awareness of such themes. She reflected on how the students’ attitudes towards privacy, surveillance, and security were impacted by their engagement with these issues through their studies.

**Roundtable 2 – Towards an effective communications plan**

[**Paul Lashmar**](http://www.communicationethics.net/journal/v12n3-4/feat1.pdf) discussed the overarching themes of the seminar series from the perspective of Foucault’s ‘power/knowledge’ theoretical framework and Bentham’s Panopticon, amongst others. He discussed how self-censorship and self-monitoring have, in practice, impacted on the right to privacy. Engagement with policy makers and academics from the field of intelligence studies was discussed in detail, given their seeming unwillingness to engage with outsiders on these topics, suggesting that the importance of public accountability is not necessarily recognised by the Government and Intelligence Services. This led to our policy recommendation of the establishment of an inter-disciplinary *Centre of Accountability* with the aim of publically holding surveillant powers such as the Intelligence Services to account when required.

The roundtable then moved to examine how engagement with the public could occur via an online documentary, which is one of the promised outputs of the DATA-PSST Seminar Series. [**Dyfrig Jones**](http://data-psst.blogspot.co.uk/2016/05/seminar-6-dyfrig-jones-position.html) highlighted the importance of ensuring that the concepts could be easily transferred to film, have a strong visual identity and would engage and/or entertain the public. The online nature of the documentary lends itself to a series of very short videos and the VINE. There was a discussion on how to identify the key themes. One idea was to link a short video to each of the seminars’ themes; another was for each short video to explore the main themes of the academic papers that will be published as part of the special issue; a third option was to identify key ideas or themes that recurred across all the seminars and use those as a basis for the documentary. A number of good examples of videos on this theme were shown, many from NGOs, and participants agreed that the wider DATA-PSST! community should be engaged to identify key messages/themes that we wish to explore in the video(s)/VINE(s), and that a smaller group of interested participants should be involved with editorial/content decisions. Another suggestion was to create a competition, predominantly focusing on students aged 15 – 20, which would not only create more short clips on the topic, but also create wider awareness of the themes amongst the younger generation. Whatever we decide regarding the specific content and look of the videos and VINE, as [Clare Birchall](http://data-psst.blogspot.co.uk/2016/05/seminar-6-position-statement-clare.html) advises, the formal properties of our chosen medium must be used carefully to best communicate our chosen content.

Policy Recommendations

1. The argument that citizens willingly trade their privacy for the sake of security has been shown to be an over-statement. Public debate should acknowledge and address citizens’ very real concerns surrounding surveillance.
2. Legislators (at national and supra-national levels) should be mindful of the opacity and inaccessibility of the legislation outlining certain obligations, such as data protection legislation, and the emerging requirement for ‘privacy by design’. Public bodies should do more to make these obligations more accessible and understandable to engineers and designers faced with such legal obligations.
3. There is a need for greater focus on *public* *accountability* from the actions of the state and other bodies collecting information. Transparency alone will not lead to greater accountability.
4. Governments and others involved in surveillance and data collection should embrace transparency insofar as is possible. Recognising that total transparency may not always be feasible, we recommend a push towards greater translucency – in other words, transparency should not be seen as an ‘all or nothing’ exercise.
5. Academics should consider ways of making theories and concepts surrounding privacy, transparency, surveillance and security more accessible to a broader audience through, for example, engaging with the artistic community and providing more accessible messages via social media, to create a public space for engagement on these issues.