|  |  |  |
| --- | --- | --- |
|  | **Visible Mediations of Transparency: Changing Norms & Practices**  10 Sep 2015  Kings College, Univ. of London |  |

**Seminar Summary**

This summary is based on detailed notes provided by PhD students Abigail Blyth, Aberystwyth Univ. and George Petry, Univ. of South Wales.

**Introduction by Dr Vian Bakir and Seminar Leader Dr Clare Birchall**

The seminar series brings together academics and practitioners to understand the promises and pitfalls of current transparency practices and their implications for society (especially privacy, sur/sous/veillance, security and trust) from a multi-disciplinary perspective. We were reminded of seminar 1, held at Bangor Univ. (Jan 2015), on [Transparency Today: Exploring the Adequacy of Sur/Sous/Veillance Theory and Practice](http://data-psst.bangor.ac.uk/policy.php.en), Seminar 2 at Sheffield Univ. (Mar 2015) on the [Technical and Ethical Limits of Secrecy and Privacy](http://data-psst.bangor.ac.uk/policy.php.en) and Seminar 3 at Brunel Univ. on [Media Agenda-Building, National Security, Trust and Forced Transparency.](http://data-psst.bangor.ac.uk/policy.php.en)

The aim of [this Seminar](http://data-psst.blogspot.co.uk/2015/09/seminar-4-visible-mediations-of.html) (4, at Kings College, Univ. of London) was to consider how messages about transparency are mediated, and what public attitudes are towards transparency practices and issues. An animated discussion was prompted by the wide range of experience and expertise of our participants. This included those working in front line services, such as Dr Simon Rice from the Information Commissioners Office, transparency activists like Simona Levi from the Spanish campaign group X-Net, artists like Zach Blas and Metahaven, and psychoanalyst Professor Josh Cohen, among others.

**Morning Keynote Speakers**

Interested in privacy issues from a psychoanalytic perspective, [Prof. Josh Cohen](http://data-psst.blogspot.co.uk/2015/09/seminar-4-position-statement-prof.html) discussed the psycho-social perils of a forced transparency. He argued that the case for the right to privacy cannot rest solely on the demand for legal control and ownership of one’s data. The intrusions of state, corporations and the media impinge not only on externally verifiable aspects of privacy, but on the more elusive and opaque privacy of one’s inner life. The dangers of this are as much in terms of creativity and imagination as politics.

The next speaker, artist and theorist [Dr Zach Blas](http://data-psst.blogspot.co.uk/2015/09/position-statement-zach-blas-goldsmiths.html), discussed his concept of ‘informatic opacity’ by scrutinising sophisticated biometric systems that have transformed the face into a mode of governmentality. Blas argued that facial recognition technologies, based as they are on Caucasians, further marginalise minorities. Through his artwork, Blas explored the idea of a ‘right to opacity’, developed from the philosophy of Eduourd Glissant. Blas discussed a series of works with masks that evade facial recognition technologies and therefore provide a refusal to engage with dominant biometric codes.

**Roundtable One – Public Attitudes Towards Transparency and Privacy**

[Dr Ben Worthy](http://data-psst.blogspot.co.uk/2015/09/seminar-4-position-statement-dr-ben.html) opened the discussion, discussing his work that measures public engagement with Freedom of Information, helping us to think about how the public learn about transparency issues – namely through events, folklore, and privacy scandals. The shock of exposés educates the public about transparency, but, as [Dr Madeleine Carr](http://data-psst.blogspot.co.uk/2015/09/seminar-4-position-statement-dr_8.html) pointed out, most dataveillance ‘events’ fail to engage with coming significant technological changes, like the Internet of Things, which has serious implications for informed consent. Founder of Internet of Things privacy forum, [Dr Gilad Rosner](http://data-psst.blogspot.co.uk/2015/09/seminar-4-position-statement-dr-gilad-l.html) argued that such events distract us from more important privacy considerations such as user control, informational self-determination and the bias towards opt outs. The group discussed how transparency is lazily invoked at times of crisis as a fix-all solution that rarely delivers real accountability, while secrecy is also justified by the state through appeals to security.

As the discussion turned to Snowden, [Dr Evan Light](http://data-psst.blogspot.co.uk/2015/09/seminar-4-position-statement-dr-evan.html) introduced the group to his Snowden Digital Surveillance Archive, an artwork through which users experience the unique sensation of reading top secret documents about mass surveillance while witnessing surveillance of their own actions in real-time. The publics’ reactions at seeing reams of their data lead to a short discussion of affect and surveillance and the uncanny feelings prompted by data doubles. [Dr Yuwei Lin](http://data-psst.blogspot.co.uk/2015/09/seminar-4-position-statement-dr-yuwei.html) reminded us of technological apparatuses like TOR which can enhance privacy. Dr Vian Bakir alerted the group to ongoing research on British public attitudes by the [Digital Citizenship and Surveillance Society project](http://data-psst.blogspot.co.uk/2015/09/seminar-4-position-statement-dr.html). This shows an increase in concerns with online privacy since Snowden’s revelations, with younger people in particular concerned with levels of interception and existing state surveillance powers. This public – especially ethnic minorities - is concerned about lack of transparency over what and how data is collected, and the nature and level of public consent. Any appearance of public apathy or consent is, in fact, public resignation, as it feels unable to change this situation. Given that recent [EU studies](http://data-psst.blogspot.co.uk/2015_03_01_archive.html) find that few people are willing to give up privacy in favour of more security, Vian asked why UK intelligence agencies, their oversight boards and their regulators continue to claim the opposite.

[Simona Levi](http://data-psst.blogspot.co.uk/2015/09/seminar-4-position-statement-simona.html) was more positive about transparency than some other participants. She stated that in the case of Spain, transparency within civil society resulted in corruption being overcome. Dr Clare Birchall and [Dr Ben Worthy](http://data-psst.blogspot.co.uk/2015/09/seminar-4-position-statement-dr-ben.html) presented the neoliberal characteristics of open data transparency – and the way in which responsibility for noticing corruption or problems was placed onto armchair auditors with little power. [Dr. Simon Rice (ICO)](http://data-psst.blogspot.co.uk/2015/09/seminar-4-position-statement-dr-simon.html) provided a perspective from the UK data regulators, explaining that processing of personal data must be fair, with fairness generally requiring transparency. He suggested that to encourage public awareness, it is necessary to explain why individuals should care about such matters.

**Afternoon Keynote Speakers**

[Dr Mark Coté](http://www.kcl.ac.uk/artshums/depts/ddh/people/academic/cote/index.aspx) reminded us that the systematic interception of communication is nothing new. The shift, however, is datafication: a non-neutral cultural, social and political process. Mark took us through some of the more important shifts in the relationship between the state and citizens in the age of dataveillance.

Daniel van der Velden from the design collective, [Metahaven](http://futuregallery.org/past/metahaven-black-transparency/), discussed his idea of ‘Black Transparency’ – the disclosure of information that seeks to embarrass or shame. Playing on a feminist trope, he suggested that in the age of dataveillance, the personal is geopolitical. The far-reaching effects of forced transparency should be thought alongside the black transparency of WikiLeaks, an organisation that people have tried to narrate according to Liberal logic, but which goes much further than this, tapping into the realm of fantasy. WikiLeaks was a prank on every kind of power.

**Roundtable Two - Mediating Transparency**

[Paul Bradshaw](https://www.blogger.com/blogger.g%3FblogID=2285745947385684898%23editor/target=post;postID=4127173095149457315;onPublishedMenu=allposts;onClosedMenu=allposts;postNum=6;src=postname) talked about the promise of data journalism to communicate complex issues to the public, but also warned that data journalism is itself a form of obfuscating mediation. [Dr Dan McQuillan](https://www.blogger.com/blogger.g%3FblogID=2285745947385684898%23editor/target=post;postID=2917708542936622545;onPublishedMenu=allposts;onClosedMenu=allposts;postNum=10;src=postname) also warned that there is no transparency, only ways of seeing. The group also discussed the lag of cultural representation concerning the current veillant conjuncture; how the panopticon model of surveillance makes little sense in an [algorithmic, multi-veillant culture](http://data-psst.bangor.ac.uk/big-data-society.php.en).

We discussed different kinds of rights – the right to opacity from Zach Blas’ talk earlier, but also, [Prof. Ben O’Loughlin](https://www.blogger.com/blogger.g%3FblogID=2285745947385684898%23editor/target=post;postID=5209747186688039821;onPublishedMenu=allposts;onClosedMenu=allposts;postNum=0;src=postname) discussed the right not to know in our culture of connectivity. [Dr Andrew McStay](https://www.blogger.com/blogger.g?blogID=2285745947385684898#editor/target=post;postID=2045136003855317622;onPublishedMenu=allposts;onClosedMenu=allposts;postNum=3;src=postname), presented the brave new world of what he calls “Empathic Media”, which read our feelings and emotional responses as data for consumer advantage, raising questions about how such intimate data should be regulated.

Paul Bradshaw and Dr Paul Lashmar raised the question of ethics in response to journalism and academia. Depending on the media outlet, divergent understandings of acting ethically are evident. Although journalists acting unethically received substantial news coverage following the phone hacking trial, they do have a code of ethics to adhere to whereas in relation to intelligence, the ethical debate is still relatively new. This is not surprising as academia has only been able to discuss British intelligence in a contemporary manner in the past 20 years.

Policy Recommendations

* As people are demonstrably concerned about privacy, we need to enable resistance to dominant surveillant players’ ethical positions (of forced transparency or radical transparency). The public needs the right, and ability, not to be part of the technological assemblage.
* The public needs more digital and data literacy. As an ethical starting point, governments should more fully share with the public what their capacities to surveil are. The public needs to understand the surveillant black boxes that pervade everyday life, and what it gives up if it withholds data from commercial surveillers. We need a public debate involving mainstream media on whether we are able to understand these abstract surveillant processes.
* We need more playful responses to surveillance than the standard one so far (which has been encryption). For instance, wearing ten different masks; norm-core fashion to disappear into a big data crowd; and crypto-parties. Artists can help through ‘artivism’. We should organise a DATA-PSST! art exhibition (or street arts or musical concerts) to raise awareness, initiate debate and re-articulate concepts, e.g. secrecy beyond securitisation.
* Resources need to be found for grassroots activist groups or ‘artivist’ groups, encouraging bottom-up practices and participatory practice. We also need to increase the visibility of artivism in mainstream media.
* Understanding how to encrypt email is just the start. We also need to understand cooperative self-governance and how to manage the digital commons, bearing in mind that the internet was built to be open rather than secure.
* As well as educating the public, those who care about preserving privacy should channel their energy into different forms of oversight and resistance – such as at regulatory and commercial levels. This presents lots of opportunities for Privacy Enhancing Technology start-ups. Pro-privacy businesses, activists and politicians need to find out what the public cares about and work backwards from there.
* As technologies open up participatory research to produce citizen science, can we also have citizen social science or citizen cultural studies? This Invisible College could teach us much about public attitudes to mutual forms of watching (‘veillance’), and educate many about possible pathways of resistance, but also what is given up if a resistive stance is taken.
* Researchers need to engage in hackathons and inter-disciplinary research to know what questions to ask.