**Tackling Transparency
Beyond the Nation-State**

 31 March 2016

 Cardiff University

This was the fifth of six seminars in the ESRC-funded [DATA-PSST!](http://data-psst.bangor.ac.uk/index.php.en) seminar series. This summary is based on detailed notes provided by PhD student Abigail Blyth from Aberystwyth University and George Petry, University of South Wales.

**Introduction by** [**Prof. Vian Bakir**](http://data-psst.blogspot.co.uk/2016/03/resistance-to-state-mass-surveillance.html) **and Seminar Leader** [**Dr Madeline Carr**](http://data-psst.blogspot.co.uk/2016/03/seminar-5-position-statement-dr.html)

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 University (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 University (Mar 2015) on the [Technical and Ethical Limits of Secrecy and Privacy](http://data-psst.bangor.ac.uk/policy.php.en), Seminar 3 at Brunel University (Jul 2015)on [Media Agenda-Building, National Security, Trust and Forced Transparency](http://data-psst.bangor.ac.uk/policy.php.en) and Seminar 4 at Kings College, London (Sep. 2015) on [Visible Mediations of Transparency: Changing Norms & Practices](http://data-psst.bangor.ac.uk/policy.php.en)**.**

The [aim](http://data-psst.blogspot.co.uk/2016/03/seminar-5-tackling-transparency-beyond.html) of Seminar 5 was to focus on the ongoing attempts at the European and international level to regulate, confine and oversee the global flow of information. To do so, it brought together scholars and practitioners of international relations, political science, international law, human rights, media and journalism to examine key debates, analyse strengths and weaknesses of existing mechanisms of regulation and oversight and explore questions about which political level is best suited to such a demanding mandate.

**Morning Keynote Speakers**

[Peter Mantello](http://data-psst.blogspot.co.uk/2016/03/seminar-5-position-statement-prof-peter.html) began by discussing neo security assemblages. These are of increasing importance following the post 9/11 emphasis upon pre-emption which has resulted in numerous companies creating software to collate information flows. Worryingly, these are based upon racial and ethnic profiling which is inherently problematic from both a political and legal stance and thus the reliability of such technology to predict crime is questionable. [Eneken Tikk Ringas](https://www.iiss.org/en/persons/eneken-s-tikk-ringas) highlighted the difficulties in creating international agreements which include the growing dominance by private companies and the differing perspectives all states have upon secrecy and privacy due to divergent ideological and cultural stances. [Rocco Bellanova](http://data-psst.blogspot.co.uk/2016/03/seminar-4-postion-statement-dr-rocco.html) then discussed the data protection discourse which highlighted a lack of awareness amongst social scientists of data as technology. [Joseph Connor](https://www.youtube.com/watch?v=nrhOqkmRjEg) examined the importance of data privacy particularly following technological advancements in [reading emotion](http://data-psst.blogspot.co.uk/2016/03/seminar-5-position-statement-andrew.html). Apple’s version of this technology stores all data on a cloud with anonymity impossible due to triangulation. However Connor argued there is a worrying lack of public awareness of such technology, despite the increased and continued use of technology and social media.

**Roundtable 1 – Surveillance and** [**Transparency**](http://data-psst.blogspot.co.uk/2016/03/seminar-5-position-statement-matthew.html) **in the International Sphere**

[Mika Kerttunen](https://www.baltdefcol.org/?id=49) suggested that the distinction between the military, law enforcement and the intelligence services has become blurred, perhaps due to the increased emphasis placed upon pre-emption. Tony Bunyan from [Statewatch](http://www.statewatch.org/) highlighted the necessity to focus on the nexus between the users and suppliers of intelligence. He emphasised the importance of informing the public about all political spheres by highlighting the ongoing refugee crisis and the European Union (EU) making certain actions undertaken by NGO’s illegal.

There was a clear consensus that there is a blurring between the military, intelligence and law enforcement and a clear solution is required. Such blurring is unsurprising as consecutive British Governments have failed to state which organisations constitute the British Intelligence Service and there are suggestions that both Defence Intelligence and the Metropolitan Police’s Special Branch constitute a member of the British Intelligence Services. The discussion then emphasised the difficulties of undertaking research, particularly with national security organisations and [secretive commercial surveillance](http://data-psst.blogspot.co.uk/2016/03/seminar-5-position-statement-steve.html) organsiations. Law enforcement and the crack down on human rights activists was discussed with one explanation being the expansion of what constitutes a threat. This is due to software the Police buy from private companies who have a different understanding of ‘threat’ than the Police do; demonstrating the role of private companies in contemporary governance. This linked back to Peter Mantello’s presentation and the emphasis placed upon pre-emption and the difficulties intelligence led policing poses.

**Afternoon Keynote Speakers**

[Gilad Rosner](http://data-psst.blogspot.co.uk/2016/03/seminar-5-position-statement-dr-gilad.html) began by examining how the US Government places business and technological interests above privacy. One example is the Fair Credit Reporting Act which controversially, allows businesses to determine appropriate uses of information. With business and economic interests of paramount importance over privacy, evident in the current Washington discourse, US policymakers decisions will be based upon commercial as opposed to political logic. [Mark Phythian](http://data-psst.blogspot.co.uk/2016/03/seminar-5-position-statement-prof-mark.html) then examined the British case by focusing his presentation upon oversight arrangements which have received substantial attention in the past year with the publication of The Intelligence and Security Committee Report, David Anderson’s A Question of Trust and the Independent Surveillance Review A Democratic License to operate. All criticised existing oversight structures and have led to, the Investigatory Powers Bill. Despite their importance, ‘the public didn’t really turn up’ but is a system they should be aware of. The suggestions made by both Anderson and the ISR are remarkably different from the existing oversight system and provides the ISC with a challenge to demonstrate the continued importance of legislative oversight. However if they were replaced by a system of judicial commissioners, this could be equally damaging.

Although minimal international law relating to intelligence cooperation exists, [Peter Gill](http://data-psst.blogspot.co.uk/2016/03/seminar-5-position-statement-pete-gill.html) stated how it still occurs via informalism. This poses significant difficulties for national oversight bodies, which do not have any international jurisdiction and therefore cannot see any information from other countries due to the Originator Control (ORCON) principle. They may also be deceived by the intelligence services who wish to ensure information remains secret. Cooperation is deemed to be so important to states that they seek to protect it at the detriment of protecting national oversight investigations by using national security as a trump card to prevent investigation into a particular manner.

**Roundtable 2 – Strengths and Weaknesses of the Existing Oversight System**

Helen Thomas from the [Information Commissioner’s Office](https://ico.org.uk/) began by discussing how organisations often have a limited understanding of the Data Protection Act, something also evident within the public. An example of this is how many small businesses do not fully understand the deal they have with their cloud provider which can be problematic. Data protection is being made harder with staff increasingly using their own devices at work, something many may not understand the ramifications of, in part due to the difficulties of providing information to front line staff. Despite the younger generation being the most concerned about their privacy, young entrepreneurs tend to lack awareness of data protection and differing types of surveillance. Non-state actors engaged in [privacy by design](http://data-psst.blogspot.co.uk/2016/03/seminar-5-position-statement-lachlan.html) also need guidance on how to embed appropriate principles into technology. Such issues require substantial public engagement to ensure the public are informed, something the ICO and other bodies need to ensure in a manner above simply placing information on their websites.

All countries have [different legislation](http://data-psst.blogspot.co.uk/2016/03/seminar-5-position-statement-yuwei-lin.html) pertaining to trans-border information flows, understandable due to the inability of states to agree on such themes at the international level. But this causes problems for companies who not only operate in different countries but also use cloud storage facilities which are governed by the legislation of other countries. This occurs due to the complex nature of internet and cyber governance which requires substantial international dialogue to find a solution, particularly as data protection and associated themes are affected by [the political will](http://data-psst.blogspot.co.uk/2016/03/seminar-5-position-statement-yvonne.html). The [problems with public oversight of intelligence agencies](http://data-psst.blogspot.co.uk/2016/03/seminar-5-position-statement-paul.html) and of commercial surveillers was also much debated, along with associated [trust deficits](http://data-psst.blogspot.co.uk/2016/03/seminar-5-position-statement-grace-eden.html).

**Concluding Summary**

The seminar analysed numerous important themes such as ensuring that a state’s world views are considered within international negotiations and is perhaps one of the biggest obstacles to discovering a harmonised and international approach to data and privacy. The lack of public interest in this theme is puzzling, perhaps in part due to complex legislation. Although the lack of interest can be construed as the public not caring, it is impossible to assess this until the public have information on which they can make an informed decision. Below are the policy recommendations and potential further research questions the seminar has created.

**Policy Recommendations**

1. We suggest greater transparency about data collection and processing, and about the effectiveness of policies based on such surveillance.
2. We recommend a particular form of transparency – with opacity built in to protect necessary secrets, but with regular and periodical review of all stages of the data process by diverse actors drawn from citizenry, civil liberties groups, technologists, industry and of course intelligence agencies.
3. For surveillance systems to work in a predictive capacity, they need and want people to behave freely, so that peoples’ real intentions can be discerned. The objective for those interested in maximizing civil liberties and those working in intelligence and security is that people behave in an unconstrained fashion (that is, without being subjected to any ‘chilling effect’). After all, the objective of bulk data collection is to discern unusual patterns against normalcy. We argue there is a danger of an ‘observer effect’ taking place.
4. We suggest that the aims of any governmental or commercial surveillant organisation involved in data collection and processing are publicly articulated more fully and clearly. They should provide more detail than blanket terms such as ‘protecting national security’, and more meaningful clarity than complex Terms and Conditions and associated tick-boxes of consent and compliance.
5. For these aims to be better understood within society we suggest the need for greater public engagement by surveillant entities with citizens. This would help generate challenges, dialogue and perhaps even consensus and greater trust.
6. Technological change on what it is possible to capture, through data, continues apace: contemporary examples include application of artificial intelligence and machine learning, data analytics, biometric devices and emotion detection. Given rapid technological progress that outstrips common understanding of what it is possible to collect, and what it reveals about an individual, we need regular review of both the adequacy of regulation and public preparedness. In other words, as technology develops, do people and politicians understand what is really going on and how it will affect them on a personal, and societal level?

**Further Research Questions**

* How can the public be better educated into the technological aspects of everyday technology?
* To enhance public understanding, can legislation be clearer on the actions undertaken by the military, intelligence services and law enforcement on data surveillance?
* How can practitioners and academia effectively engage with civil society?
* How can international oversight of intelligence be improved?
* What is the overall political agenda that creates such debates?
* What are the key public and private relationships behind these policies?
* What are the values which underpin policies and where do these originate from?