Media Agenda-Building, National Security, Trust & Forced Transparency

8th July 2015, Brunel University

Seminar Summary

This summary is based on detailed notes provided by PhD students Abigail Blyth, Aberystwyth Univ.; Linda Monsees, who is at Aberystwyth on a research exchange; and Tiewtiwa Tanalekhapat, Aberystwyth Univ.

Introduction by Dr Vian Bakir and Seminar Leader Dr Paul Lashmar: The seminar series aims to bring 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 (Jan 2015), on Transparency Today: Exploring the Adequacy of Sur/Sous/Veillance Theory and Practice, and Seminar 2 at Sheffield (Mar 2015) on the Technical and Ethical Limits of Secrecy and Privacy.

Roundtable 1: Two years on from Snowden

The discussion was initiated by Professor Mark Pythian. He explained that the landscape of current surveillance practices has dramatically changed within the last decade, and that the debate cannot and should not be constrained to national boundaries. Mass surveillance, for example conducted by the USA, not only affects the USA, but has implications for the citizens around the world. Phythian discussed the implications of Snowden upon the intelligence realm, with particular emphasis upon why such vast amounts of data are collected. While the state denies that this constitutes surveillance (calling it 'bulk data collection' instead), an individual (rather than machine) is still required to analyse information. Intelligence agencies argue that unless all information is collected, it is impossible to detect future threats, and this is perceived as crucial following the 9/11 Commission which criticised American intelligence organisations for not 'connecting the dots'. Phythian referred to the June 2015 report from the Independent Reviewer of Intelligence Legislation, David Anderson, and its concern over outdated legislation governing intelligence agencies.

Examining the EU context of this debate, Tony Bunyan (journalist and director of Statewatch) argued that we need to consider the broader context and actors involved in surveillance, and that not only more transparency but also more accountability is needed. To combat terrorism, international businesses are continually relied upon, evident at the European level as Europol continues to gather intelligence on perceived foreign fighters wanting to collude with the Islamic State. Vian Bakir asked what evidence is there that predictive intelligence surveillance tools (such as PRINTAURA, FASCIA, CO-TRAVELER, PREFER, XKeyscore revealed by Snowden) actually work. Various oversight reports from

the UK intelligence community say that they work, but never tell us much about how or why.

The difficulties of establishing accountability and the lack of transparency was forcefully shown in the presentation by Jamie Woodruff, an ethical hacker, who explained the variety of tools state agencies use in order to surveill citizens and how difficult it is to get access to information about these practices. He showed in a live demonstration how easy it is to use these tools (by using affordable hardware and open-source tools for hacking that are available online) and how much information they reveal about every single individual. His presentation was very much applauded and provided a useful insight into the technological aspects of surveillance.

Roundtable 2: Media Agenda Setting

In this session a variety of short presentations were held which focused on the role of the media for furthering a public debate. The difficulties journalists have are not entirely new, as some participants with a long history of investigative journalism could confirm. However, new technologies also allow for the emergence of alternative outlets (e.g. blogs and wikis). Professor Richard Keeble identified the following as some of the best: tomdispatch.com, counterpunch.org, globalresearch.ca; boilingfrogspost.com, whowhatwhy, intelnews, World Socialist Website, infowars.com, coldtype.net, antiwar.com; and the writings of Pepe Escobar at Asian Times. Participants fiercely discussed the question of divergence in coverage between mainstream media and alternative media. In this context Christopher Hird (former managing editor of Bureau of Investigative Journalism) pointed out that RIPA (Regulation of Investigatory Powers Act 2000) violated the rights of journalists but still many media outlets did not support the resistance against it. Assessments regarding to what extent mainstream media are able and willing to be thoroughly critical towards state agencies or international corporations varied, with John Lloyd raising issues of mainstream journalists' co-optation by the intelligence agencies. Agreement was reached that alternative outlets are an important addition to the media landscape, but also that the newspaper *the Guardian* played a vital role in the UK in triggering a public debate about state surveillance. It was suggested that alternative media's consideration of political arguments otherwise ignored occurs as they are not, in Keeble's words, 'ideologically imprisoned' or beholden to proprietors with a tendency to marginalise certain issues, something even *the Guardian* has been accused of. The debate then moved onto the recent *Sunday Times* front page (alleging Snowden's documents were in the hands of Russian and Chinese intelligence) and the critical reception this received from other outlets. Stephen Dorril added to the debate by discussing the role of whistle-blowers in society in the context of a 'secret' or 'dual' state. Although participants disagreed to what extent talking about a secret state, in which agencies behind the scenes rather than elected politicians hold most power, is justified, the debate about this issue continued throughout the rest of the day.

With the internet so prominent, the Intelligence Services and the media have had to adapt and therefore RIPA is no longer effective. In journalism, this can be seen as the start of a new era, something Glenn Greenwald (the journalist who broke the stories of Snowden's leaks) believes, arguing there should be hostility towards the Intelligence Services as they lie and hide information. John Lloyd raised the security and transparency debate in relation to publishing national security matters and whether journalists can judge this. To effectively report on the intelligence realm, arguably specific training is required.

Discussion then turned to whistle-blowers' motivations, and how their lives change, particularly if prosecuted under the Official Secrets Act, something that has also affected journalists. Dorril argued that whistle-blowers believe they act for a moral and ethical purpose. In contrast, Iain Bourne (Information Commissioner's Office) suggested that Snowden had far less noble motives.

The media are an important facet in public engagement and the Intelligence Services can attempt to set the media agenda by encouraging and discouraging certain stories. Within the media, politicians are the most cited sources and defend the actions of the Intelligence Services, something borne out by the DCSS study into British press coverage of the Snowden leaks and digital surveillance, presented by Jonathan Cable. Emma Briant pointed out that in relation to propaganda, US-UK cooperation has become paramount since 2005: this, together with Snowden's revelations, shows how British and American governments can evade their own national propaganda rules about who can be exposed to propaganda, with the UK seen as 'useful' to the US due to its different rules and lack of legal audience restrictions. This discussion led to the importance of culture being highlighted and whether this is something which affects the openness of a Government.

Roundtable 3: Trust and Accountability

This last roundtable focused on the beliefs and interests of the public, the possibilities of resistance and the relationship between the state and citizens. The discussion began with Iain Bourne (Information Commissioners' Office) providing a policy perspective. He stated that legislation is there to protect the work of the Intelligence Services and therefore the public should receive minimal, if any information; and that transparency is exempt when pertaining to matters of national security. On the whole, participants understood that the Intelligence Services are in a difficult position as they are unable to publish the work they undertake, but felt that surely there is a balance where they could be more open which would result in the public being more trusting of them. Such a debate could begin with Governmental annual reports being more effective, a theme Mark Phythian highlighted earlier – although Bourne also alerted us to the recent publication of reports by the Interception of Communications Commissioner's Office.

While participants disagreed about the extent to which the public understands or cares about surveillance and intelligence issues, the consensus was that if there was more engagement from the state, the public would be more interested. Bourne said he thought the public is, in general, trusting of the state and agrees to security measures that intrude on their privacy because they want to have better security. Other participants disagreed about this assessment and pointed out that the current situation is so complex and disconcerting that resistance is often difficult. The public has no insight into, for example, what the criteria for targeted policing are, and filing a formal complaint is often a laborious task. Furthermore, the role of companies in public-private-partnerships is often kept secret which is another reason why assessing and resisting current practices is difficult.

Broadening the debate, technology standards developer Mark Lizar talked about the problems with commercial companies' opaque data sharing and surveillance practices; and Professor Mike Levi asked if authorities were collecting and examining white collar crime through Snowden-styled surveillance, or if this was protected under corporate

privacy. Martina Feilzer suggested that the governments in multiple countries appears to be ignoring public opinion on surveillance rather than managing it; and Lada Trifanova-Price pointed out the importance of looking at questions of trust and accountability in Central European Countries in which the role of the state or secret services might differ because of their history, and where the traditions of democracy are much more fragile.

This final discussion was also concerned with the possibilities of resistance (do we need real-world examples or is resistance always utopian?). Yuwei Lin reminded us that anonymity and privacy are vital for individuality and identity, and are a sign of how liberal a society is.

Policy Recommendations

1. More accountability, not only transparency, concerning the actions of the state and secret-services is needed if public trust is to be rebuilt. Given the many conflicting opinion polls and studies conducted since Snowden, a definitive analysis is needed on public perceptions of intelligence, surveillance, oversight and accountability.
2. More education and a better quality public debate (eg in the media) are required to inform the public on matters of surveillance and national security. The complexity of the issue makes it difficult to explain, and we need to find ways of making these issues both clearer and more relevant for a general public, bearing in mind that social change can happen through 'agitators' creating a better debate.
3. Specific training for journalists focusing upon the intelligence realm is needed in NCTJ courses, including understanding RIPA and new technology. Journalists must be able to understand current technologies and be able to assess them in their regulatory context.
4. An academic think tank, perhaps stemming from DATA-PSST participants, is needed to intervene on policy and media debates on these issues. We should also conduct a workshop on state secrecy structures and how to research them. This group could also try to do the ethical assessment analysis required by every EU security program that weighs the possible results against the intrusions of privacy and freedom.
5. A very high proportion of consent notices are non-compliant. Better implementation is needed, and enforcement by the ICO. The ICO would like us to come up with real systems that work better, rather than just generalised talks on transparency.
6. At policy-making level, participants recommend that: the government's definition of its targets and who extremists are needs to be much more narrow; and selling surveillance technologies to non-democratic states must be regulated with better monitoring.