Final Report for DATA-PSST ESRC Seminar Series

June 2017

DATA-PSST!

Principle Investigator: Vian Bakir

Debating &
Assessing
Transparency
Arrangements -
Privacy,
Security,
Sur/Sous/Veillance,
Trust

Co-Investigators:
Andrew McStay, Bangor Univ.,
Martina Feilzer, Bangor Univ.,
Dyfrig Jones, Bangor Univ.,
Yvonne McDermott, Bangor Univ.,
Paul Lashmar, Sussex Univ.,
Emma Briant, Sheffield Univ.
Ross Bellaby, Sheffield Univ.
Claire Birchall, Kings College London,
Madeline Carr, Cardiff Univ.,
Claudia Hillebrand, Cardiff Univ.

Contents

Introduction

In 2013, National Security Agency (NSA) whistle-blower, Edward Snowden, revealed that state surveillance had infiltrated the fabric of everyday digital communications, piggy-backing on commercial telecommunications platforms that we all use. This policy had been kept secret from the public, most politicians, and to some extent, the commercial telecommunications platforms. Simultaneously, commercial surveillance of online behaviour by marketers and advertisers was becoming finer-grained, better targeted and ubiquitous. Moreover, the public was increasingly sharing and watching themselves (or 'sousveilling') through selfies, social media postings and biometrics such as wearable devices.

Interested in this *net rise in mutual watching*, DATA-PSST aimed to:

- Think about data transparency in a more nuanced way than 'all or nothing', especially in relation to privacy, security, sur/sous/veillance and trust.
- Explore what different academic disciplines and real world actors, including data regulators, activists, companies, journalists, artists and ordinary citizens, think of existing and desirable transparency arrangements.
- Build a typology of transparency types.
- Intervene in public debate about transparency arrangements.

The DATA-PSST network involved over 100 people discussing these issues in 6 seminars held across 2015-16 – a crucial period in the UK as it debated its Investigatory Powers Bill. It comprised academics from diverse disciplines across 20 UK and 5 international universities, and 30 "real world" actors interested in privacy, security and surveillance of data. They included: the Information Commissioner Office (UK and Wales), politicians interested in data protection and digital rights (e.g. the Pirate Party (UK, Iceland), International Modern Media Institute (Iceland), journalists (Bureau of Investigative Journalism, Reuters Institute), private companies (Californian satellite imagery company Planet Labs, Finnish privacy software company F-Secure), NGOs in UK and Spain (Privacy International, Statewatch, X-Net), artists (from the USA, Netherlands, Canada, Wales and Ireland), security firms (UK), think tanks (International Institute for Strategic Studies, Estonia; Internet of Things Privacy Forum), and an ethical hacker (PatchPenguin).

Core insights

- Transparency has two important dimensions: degree of citizen control over how visible they are; and degree of oversight of the surveillant entity.
- Post-Snowden, we have moved towards a transparency arrangement of *radical translucency*. This is where (a) people have no personal control over their own personal visibility because they have signed this away for the greater good, but the surveillant organisation adds opacity to secure the individual's privacy; and (b) public processes are maximally opened up for inspection.
- Internal and public oversight of surveillant state entities is insufficient. We recommend that we need to re-examine the robustness of whistle-blowing mechanisms to the press. We also recommend that mainstream journalism ensure that information provided by intelligence elites is challenged and balanced by views from other legitimate actors.
- Oversight of commercial entities remains problematic, largely because of transnational business structures, problematic consent mechanisms, collection of more data than is required to fulfil a service, and opaque Terms and Conditions (T&Cs).
- The DATA-PSST network wants a transparency arrangement of *liberal translucency* where *there is* (a) more oversight of surveillant entities (while recognising their need for some secrecy) and (b) greater citizen education and control over their own digital privacy.
- US, UK and wider international publics want more privacy from state and commercial surveillance; but find targeted surveillance of digital communications as more acceptable than blanket surveillance**.**
- DATA-PSST has produced five significant interventions into the public debate on transparency.

The Issues: Privacy, Security and Mutual Watching

Digital communications are central to modern life. By 2015 two thirds of people in the UK and the USA owned a smartphone, using it not just to make calls but to access social media, send texts, browse the internet, follow breaking news, GPS directions, banking and shopping online. They also use it for life events like applying for jobs, looking up health conditions and taking classes (Ofcom 2015, Smith 2015).

Given this digital culture and society, Edward Snowden's unauthorised leaks to the press in 2013 about the USA's post-9/11 mass surveillance policy, and the involvement of multiple nations, received global public attention. The leaks revealed that signals intelligence agencies such as the USA's National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ) mass surveil citizens' communications by collecting data in bulk from the servers of US global telecommunications companies and from directly tapping the companies' private fibre-optic cables carrying internet traffic. This data includes the content of communications (e.g. emails and instant messages); and what was called 'communications data' (in the UK) and 'metadata' (in the USA) (e.g. who the communication is from and to whom; from where it was sent, and to where; and the record of web domains visited).

Intelligence agencies argue that their mass surveillance policies are necessary, legal and accountable, albeit secret. Big data analytics enable intelligence agencies to identify, understand and act on potential threats (e.g. a terrorist attack) and opportunities (e.g. the possibility of disrupting an attack) (Anderson 2016: 72-73).

Standing against mass surveillance are those who fear governments with authoritarian tendencies. The leaks highlighted how mass surveillance policies potentially contravene the international human right to privacy of anyone who uses digital communications. As stated in the *UN International Covenant on Civil and Political Rights* 1966 (Article 17): 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation'. The *European Convention on Human Rights* [1953] (Article 8) similarly governs the protection of private life and the confidentiality of correspondence. Any interference with the privacy of a person must first be subject to that person's consent, and the individual must know exactly what he or she is consenting to. While privacy is a restrictable right, the state can balance it against other legitimate considerations, including national security. Where the state seeks to intrude into a person's privacy, the interference must be justified, proportionate and necessary. There must be judicial oversight of any state interference, and people affected by interference must have access to justice to challenge it (Bauman et al. 2014).

While intelligence agencies point out that only a tiny portion of data collected is ever seen by human eyes, the 'chilling effect' of mass surveillance was formally recognised in December 2013, as the United Nations (UN) General Assembly adopted a Resolution tying the right to privacy to the right to freedom of expression: if people know that they are potentially surveilled, they will not express themselves freely. The 'chilling effect' on freedom of opinion and assembly has since been demonstrated regarding: page views of *Wikipedia* articles relating to terrorism (Penney 2016); usage of *Facebook* (Stoycheff 2016); a decline in 'privacy-sensitive' search terms on *Google* that could get users (from 11 different countries including the USA) into trouble with the US government (Marthews and Tucker 2015); and US journalists' behaviour, with a December 2014 survey of 671 US investigative journalists finding that surveillance concerns prevented 14% from pursuing a story or reaching out to a particular source (Pew Research Center 2015).

Snowden's leaks prompted reviews, inquiries and court cases into the mass surveillance policies at political levels, both nationally and at European Union (EU) and UN levels. While clarifying the nature and extent of mass surveillance of data in the USA and UK, legislative change in the USA was minimal: *the USA Freedom Act 2015* banned bulk collection of telephony meta-data. Meanwhile, the UK formally expanded its surveillance powers in the *Investigatory Powers Act 2016*.

The digital nature of everyday life has only intensified since Snowden's leaks. For instance, social media usage has boomed: by 2017, the leading platform, *Facebook*, had almost 2 billion monthly active users, followed by *WhatsApp*, *YouTube* and *Facebook Messenger,* each with over a billion monthly active users (Statista 2017). Trends in the commercial exploitation of data see increased reliance on use of location services, biometric data and even data about people's emotions. Such data streams are collected not just through smart phones and internet usage but in public spaces (such as streets and intelligent advert billboards) and quasi-public spaces (such as retail outlets that seek to personalise shopping experiences, just as is done online) (McStay 2016). In general, a surveillant architecture that has been applied to the web is also being applied to cities and "smart" developments therein. Many welcome the benefits of such surveillance – from more security to better civic services and commercial experiences. But privacy invasions and chilling effects are also real. And it is not just governments and citizens in liberal democracies that embrace surveillant digital cultures and societies, but also non-democratic states. Note that smart cities, for instance, are being built in Dubai and China.

Given this milieu, it remains ever more apposite to understand the nature of contemporary transparency arrangements, and their constituent elements of privacy, surveillance, security and trust. It is only by understanding the nature of contemporary transparency that society can ask itself, what is desirable, and what can or should be changed?

What is transparency? Disciplinary perspectives

One of the valuable things about DATA-PSST's seminars is that it brought together a broad array of disciplines – from computer engineering to media philosophy, embracing digital culture, politics, international relations, sociology, criminology, business studies and more. It showed us how different academic disciplines conceive of transparency.

Computer Engineering perspectives

Coming from a computer engineering perspective, where the focus is on building technology, Steve Mann sees transparency in terms of *oversight of surveillant entities via citizens' technological capacities to observe power*. For several decades Mann has been developing technology to counter and resist surveillance societies. He calls this *sous*veillant technology.

If surveillance involves monitoring from a position of political or commercial power by those who are not a participant to the activity being watched (e.g. CCTV cameras, sentiment analysis and programmatic tools used by marketing and state intelligence agencies), sousveillance (Mann 2004) involves monitoring from a position of minimal power, and by those who are participating in the activity being watched or sensed. *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).

For Mann, a transparent society is achieved when surveillance and sousveillance balance out: this is a state of *'equiveillance'.* This can be achieved partly through (a) numbers (i.e. when sousveillance goes mainstream); and (b) when society has robust mechanisms for enacting political change from below. Mann and Ferenbok (2013: 30) posit that we achieve *equiveillance*/transparency when:

> veillance infrastructures are extensive and the power requirements to enact change from below are marginal. This type of system would likely protect whistle-blowers, encourage public fora and debate, and implement participatory projects and innovations to the system. Even the powers of oversight in this configuration are likely to be seen from below and subject to evaluation.

These mechanisms for enacting political change from below are all forms of oversight of the surveillant entity (or what Mann terms 'undersight').

Philosophy, Privacy and Digital Media perspectives

Coming from the perspective of philosophy and privacy applied to digital media and journalism, Vian Bakir and Andrew McStay agree that oversight of the surveillant entity is important, but that this is not enough in itself. Citizens also need to have control over their own personal visibility.

This notion of transparency has two important dimensions:

(a) Degree of *citizen control over how visible they are;*
(b) Degree of *oversight of the surveillant entity*.

Bakir and McStay (2015) use these two dimensions to pinpoint different societal transparency arrangements.

In 2013, Snowden showed that we were in a condition of ***forced transparency***.

(a) Citizens had no control over their own personal visibility, because the state had secretly imposed mass surveillance on people. Because of the secret imposition, citizens cannot be said to have consented to this surveillance.
(b) The level of oversight of the state and corporations was insufficient to built social trust – as evident

by the huge social outcry over mass surveillance in states like the USA following Snowden's leaks.

However, other transparency arrangements are possible.

A ***liberal transparency*** arrangement is informed by classic liberal and enlightenment norms of personal liberty as the avoidance of interference from others (Mill (1962 [1859]); and of opening up machinations of power for public inspection, rationally using the knowledge gained as a force for promoting societal net benefit and happiness (Bentham 1834). In this transparency arrangement:

(a) Citizens would have high control over their personal visibility;
(b) And the extent of oversight of the surveillant entity would also be high (to ensure no unwanted prying into citizens' lives).

A ***radical transparency*** arrangement is where everything – both public processes and the private lives of citizens - is visible to everyone for the social good (a principle developed by utilitarian philosopher Jeremy Bentham). In this transparency arrangement:

(a) Citizens would sign away control over their personal visibility (to maximise the social good), but;
(b) The extent of oversight of the surveillant entity would be high (i.e. everything is visible to everyone throughout the power structure).

Drawing on Andrew McStay's (2014) book *Privacy and Philosophy,* DATA-PSST started with these notions of transparency, and interrogated them across its six seminars. We examined US and UK documents on intelligence agency surveillance produced by the state following Snowden's leaks. We also studied opinion polls and in-depth studies of citizens' views on privacy, security, and state/commercial digital surveillance. These highlighted that both the state and citizens did not want a radical transparency arrangement. Rather, both wanted to be able to shield their activities and have some privacy and secrecy. Drawing on this, Bakir and McStay expanded their transparency typology to include *opacity* via the notion of *translucency*. They conceived of two types of translucency.

Liberal translucency: this adds some opacity to a liberal transparency arrangement. As with liberal transparency, people have control over their own personal visibility; and power is opened up for public inspection. However, liberal translucency also sees the need for socially or legally agreed limitations on such oversight, with opacity regarding what is disclosed to citizens about specific operational details of surveillance. For instance, citizens can see the *shape* of the state secret but not operational details – a proposal put forward by think tank, the Henry Jackson Society (Simcox 2015).

Radical translucency: this adds some opacity to a radical transparency arrangement. As with radical transparency, people have no control over their own personal visibility because they have signed this away for the greater good; and public processes are maximally opened up. In addition to this, opacity is added by the surveillant entity to ensure a modicum of secrecy for the surveillant entity and a modicum of privacy for the citizen. Examples include *PlanetLabs* (a company that takes photographs of the earth from satellites in space) ensuring its image resolution is such that it can see the shape and impact of what humans do on the planet (e.g. deforestation), but cannot reveal an individual's identity. Another example is state intelligence agencies applying what they call 'minimisation procedures' to ensure that the data they mass surveil only gets further examined by human eyes on meeting certain criteria.

Table 1 Transparency Arrangements: Visibility, Control, Oversight

Transparency Type	Citizen Control over Personal Visibility	Extent of Oversight of Surveillant Entity
Forced Transparency	None (state/corporate-imposed, secret control)	Insufficient to win social trust
Liberal Transparency	High	High (to ensure no unwanted prying into citizens' lives)
Radical Transparency	Low (everyone has signed away their control to maximize social good)	High (to ensure concurrent citizen & state/ corporate openness)
Liberal Translucency	High	Socially/ legally agreed limitations
Radical Translucency	Low (everyone has signed away their control to maximize social good)	Socially/ legally agreed limitations

(For more depth on this, see Bakir, V. & A. McStay. 2015. Theorising Transparency Arrangements: Assessing Interdisciplinary Academic and Multi-Stakeholder Positions on Transparency in the post-Snowden Leak Era. *Ethical Space* 12 (3/4).)

Transparency today: Towards radical translucency

Post-Snowden, the British surveillant state appears to be moving from a position of forced transparency towards one of *radical translucency* (Bakir and McStay 2015). This advocates the opening up of both public and private processes for the general good, but with socially or legally agreed limits to the extent of oversight of the surveillant entity and the extent of citizens' visibility. In principle, the limits imposed should not compromise the general good achieved by visibility.

For instance, the UK's *Investigatory Powers Act 2016* clarifies an expanded range of state surveillance powers. These comprise:

- Bulk interception (of international communications as they travel across networks);
- Bulk acquisition (of communications data in bulk from Communications Service Providers);
- Bulk personal datasets (e.g. passport and electoral registers; datasets containing operationally focused information from law enforcement or other intelligence agencies; and datasets enabling identification of individuals' travel and finance-related activity);
- And bulk equipment interference (e.g. intelligence agencies hacking mobile phones).

Arguably the *Investigatory Powers Act* merely unifies and clarifies what had previously been done in secret, and under confusing legislation. But, pointing to an expansion in the surveillance regime the Act allows 48 government agencies, many of them beyond the security services (e.g. the Information Commissioner, Department for Work and Pensions, and Department of Health), to access communications data (including internet browsing history by requiring Internet Service Providers to keep logs for a year and hand them over to the government on request). Yet, this expansion is tempered by greater and clearer oversight. The Act introduced a safeguard that warrants should enter into force only after approval by a judge. It also created a new regulatory and supervisory body (the Investigatory Powers Commission) and extra protections for communications of sensitive professions and groups such as lawyers, Members of Parliament and journalists (Anderson 2016: 8).

Post-Snowden, key surveillant corporations that suffered reputational damage (as Snowden's leaks pointed to their complicity in mass surveillance) also appear to be moving towards a transparency position of *radical translucency*. They continue to make extensive use of their customers' non-personally identifiable data for commercial ends, but they also now see commercial opportunities in enforcing the privacy of their customers (in regard to state surveillance). For instance, in September 2014 *Apple* and *Google* moved towards encrypting users' data by default on their latest models of mobile phones; and popular messaging service *Whatsapp* announced in November 2014, that it would implement end-to-end encryption. In 2017, at the time of writing this report, social media firms continue to defy the government's desire for removal of all encryption from suspect messages. Critically, these opacity decisions are primarily being made by corporations rather than by citizens.

What sort of transparency arrangement do we want?

DATA-PSST participants said that they wanted more oversight and limits on surveillers, and for citizens to better understand and control their own personal visibility.

We want more oversight and limits on surveillers.
DATA-PSST participants said that while they recognised the state's need for some secrecy, they wanted:

- More oversight of law enforcement, intelligence communities and the private sector;
- People's privacy to be protected, be this through technological solutions, or surveillance safeguards such as enforcement of rights for 'surveillees'.

We want citizens to better understand and control their own personal visibility.
DATA-PSST participants said that they wanted:

- To find out what people want their digital rights to be, and what concerns them about data-mining;
- To increase digital and technological literacy to raise awareness of private data flows, so that people can take appropriate action to safeguard their privacy.

The two over-arching messages are (a) more oversight of surveillant entities (while recognising their need for some secrecy) and (b) greater citizen education and control over their own digital privacy. **This tallies with a *liberal translucency* arrangement.**

Is oversight of surveillant entities sufficient?

Intelligence agencies have numerous internal, political and legal oversight mechanisms on their actions. However, such internal and formal oversight did not prevent or expose the mass surveillance policy, which came to light primarily through a *whistle-blower* who leaked to the *press*. These *public* oversight mechanisms of the surveillant state are therefore important. However, as Bakir (2015) shows, both in the UK and USA, whistle-blower protections and debate in public fora are weak. (Notably, these are two areas that Mann and Ferenbok (2013) propose are vital for an *equiveillant* society to take root.)

1. National security whistle-blower protection is weak

Snowden was not technically a whistle-blower as he did not follow US national security whistle-blower protocol (which would have meant giving his information to an authorised member of Congress or Inspector General – a process that assumes that internal reform ensues, but that Snowden had no faith in). So, Snowden remains stranded in Russia and does not enjoy even the limited protections given to national security whistle-blowers in the USA, despite initiating an international public and political debate that has led to re-evaluations of surveillance policy and intelligence oversight.

Meanwhile, there were multiple indictments of national security whistle-blowers by President Barack Obama under the USA's *Espionage Act 1917*. Obama's post-Snowden *Review Group on Intelligence and Communications Technologies* (2013) further recommends better/more continuous national security employee vetting to prevent leaks. Furthermore, in 2017, the UK is considering its own version of the US *Espionage Act*.

Whistle-blowing to the press, then, is discouraged, channelled, and remains a weak formal mechanism to enact change from below. ***We recommend that we need to re-examine the robustness of whistle-blowing mechanisms to the press.***

2. Debate in *public fora is weak*

Intelligence agencies are able to manipulate the press via secrecy and propaganda (Bakir 2016).

They have various **secrecy-maintaining techniques**.

- The most basic is to ***withhold information***. The surprise of Snowden's leaks in 2013 attests to the successful secrecy of surveillant intelligence practices. They date back to changes in US surveillance law introduced under President George W. Bush under s.215 of the *Patriot Act 2001*, and s.702 of the *FISA Amendments Act 2008* - a Bush amendment renewed for five years under President Barack Obama in December 2012, enabling the NSA to collect data (including in bulk) when at least one party to the communication is foreign.
- The most draconian secrecy-enforcing technique is ***prior constraint*** on what journalists can publish. *The Guardian* believed that its biggest threat in breaking the Snowden story was legal injunctions to prevent publication *The Guardian*'s then editor, Alan Rusbridger, says most of the UK's press complied with the UK's Defence Advisory Notice not to publish the leaked material in 2013.
- ***Threats of criminal prosecution against whistle-blowers***. On 14 June 2013, Snowden was charged under the *Espionage Act 1917*. One hundred years later, in 2017, the UK is considering its own version of the *Espionage Act*.
- ***Blacklisting and harassing non-compliant press***. In July 2013, *The Guardian*'s employees were forced to physically smash their computer hard drives in London, under GCHQ's tutelage, as they refused to hand over the leaked documents.
- The most common secrecy-maintaining technique is to ***engender self-censorship*** by journalists, who comply with state secrecy requests to ensure continued access to official information or because they are persuaded by government's national security arguments.

On **propaganda**, Bakir et al. (2017) argue that information provision becomes propagandistic when there is *systematic omission of, distortion of, or misdirection from, pertinent information.* Studies show this happening in the UK press and broadcasting across the two-year period following Snowden's initial revelations, as most outlets privileged political sources seeking to justify and defend the security services and mass surveillance (Branum and Charteris-Black 2015, Di Salvo and Negro 2016, Lischka 2016, Wahl-Jorgensen, Bennett and Cable 2016, Wahl-Jorgensen, Bennett and Taylor 2017). Prominent press themes were that social media companies should do more to fight terrorism, and that while surveillance of politicians is problematic, surveillance of the public should be increased. Citizens' privacy rights and surveillance regulation were minimally discussed, while mass surveillance was normalised by suggesting that it is necessary for national security. The most frequent opinions covered largely support mass surveillance efforts by corporate and state actors (Wahl-Jorgensen, Bennett and Cable 2016, Wahl-Jorgensen, Bennett and Taylor 2017). British broadcasting gave governmental, pro-surveillance actors a voice by default as pro-surveillance arguments were expressed explicitly through the societal threat of terrorism, whereas counter-surveillance arguments about the consequences of mass surveillance for liberty and democracy remained obscure (Lischka 2016).

The quality of the public debate is important, because it helps influence both public and political opinion, yet it was skewed towards government perspectives in the UK. ***We recommend that mainstream journalism ensure that information provided by political and intelligence elites is challenged and balanced by views from other legitimate actors.***

Is oversight of commercial entities sufficient?

In short, no. Commercial actors are overseen by data protection regulators, such as the Information Commissioner's Office in the UK, who has the power to levy sanctions. Legal tools in the UK currently include the *Data Protection Act 1998* that implements the EU's current Data Protection Directive. (Other European data protection implements include the forthcoming General Data Protection Regulations (GDPR) and the ePrivacy Directive.)

However, as discussed in DATA-PSST's seminars, existing data protection tools have been shown to be inadequate, particularly in relation to unread T&Cs and lack of provision in current and forthcoming legislation for new forms of data surveillance (particularly on data about emotions and that which is intimate, but not strictly personal) (McStay 2016).

Furthermore, commercial entities typically see data protection and privacy in terms of compliance, rather than an opportunity to engage positively with customers. Thus, while most companies' activities are legal and sufficiently overseen so as to be legally compliant, this does not necessarily equate to being privacy-friendly. For example, behavioural advertising is supposed to be based on consent whereby we clearly indicate our preference about whether or not we prefer to be tracked and received tailored advertising. Recognising that privacy and issues of consent are in many ways liberal matters that indicate respect for subjectivity and the right of a person not to be intruded upon without good reason, the extent to which current commercial tracking enjoys *meaningful consent* is highly questionable. This should be placed in context of research that finds that people care deeply about online privacy (McStay 2017). Note too, this is not just academic work, but is echoed in studies carried out for the advertising industry that finds that 89% of people 'want to be in control of their online privacy'. In practical, legal and philosophical terms consent is the fundamental lynchpin, and while there is legal compliance, the degree to which this is meaningful is highly questionable.

It remains to be seen what the GDPR's impact will be, but the context that it will be asked to regulate is a complex one. After all, it is not just our devices that are surveilled, but also the home itself and out-of-home environments that use sensors to detect human behaviour, the body, emotional life, attention, intention and preferences.

What do citizens think?

Many of the six seminars queried what people think about privacy, especially the state's proposed trade off between privacy and security. To answer this question we produced a report that summarised UK opinion polls and studies into these questions (Bakir et al. 2015). As well as this, Bakir (*in preparation* 2018) summarises studies of public opinion of mass surveillance policies in the US, UK and internationally.

Across 2013-2014, more polls show a majority of Americans against mass surveillance, but by 2015, public opinion had become more divided. By contrast in the UK, more polls find a majority of the British public in favour of mass surveillance across 2013-2014, but by 2015, it had become more divided, moving in the direction against these surveillance powers (Bakir, *in preparation* 2018).

Public opinion from countries beyond Britain or America regards the mass surveillance policies as unacceptable. In most of the 43 countries in Pew Research Centre's 2014 global attitudes survey, large majorities opposed US government monitoring of emails and phone calls of citizens from their own country (a median of 81%), of leaders from their country (73% opposed) or of American citizens (62% opposed); although 64% approve monitoring of terrorist suspects. A 2015 poll questioning 15,000 people from 13 countries across every continent, found 71% opposed the US government spying on their internet and phone communications, with 59% opposing their own government intercepting, storing and analysing internet use and mobile communications of its citizens.

Deeper studies find a complex picture. A 2014 study unpacked people's views via large citizen summits of 2000 citizens from nine European countries (including the UK) on security-oriented surveillance technologies (Ball et al. 2014, Pavone et al. 2015). It finds that this public does not accept blanket mass surveillance. While the public thinks some surveillance technologies are useful and effective for combating national security threats and should be used, acceptability varies according to whether the surveillance is of communications or bodies, and blanket or targeted. Surveillance of physical bodies (e.g. smart CCTV) and targeted surveillance of digital communications (e.g. smartphone location tracking) are more acceptable than blanket surveillance of digital communications (e.g. deep packet inspection). This study also shows that the EU public tends to reject security-oriented surveillance technologies where they are perceived to negatively impact non-conformist behaviour; and it demands enforced and increased accountability and transparency of private and state surveillant entities. Notwithstanding national differences, few people are willing to give up privacy for more security (Pavone et al. 2015: 133).

UK-based focus groups in 2015, sampled with sensitivity to ethnic, socioeconomic and geographic diversity, show that the public is often uncertain and confused about digital surveillance. It is concerned about lack of transparency and legal safeguards for how and why personal data is collected: many want to know more about, and have more control over, what happens to their data and would actively circumvent forms of surveillance if they were aware of alternatives and felt skilled in their adoption (Bakir et al. 2015, Dencik and Cable 2017).

As far as commercial surveillance goes, polls on public perceptions of privacy from the advertising industry show that everyone wants more online privacy, and that this feeling pre-dates Snowden's leaks. For instance, in 2012, the Internet Advertising Bureau found that: 89% of the UK's internet users 'want to be in control of their online privacy' and that 62% 'worry about online privacy' (IAB 2012). Post-Snowden, 91% of US adults agree or strongly agree that consumers have lost control of how personal information is collected and used by companies (Pew Research Centre 2016).

To summarise, US, UK and wider international publics want more privacy from state and commercial surveillance; but find targeted surveillance of digital communications as more acceptable than blanket surveillance of digital communications.

DATA-PSST's five interventions

Each of DATA-PSST's seminars made recommendations. Recurring themes were as follows:
- Because of its complex, abstract nature, it is difficult to understand how our digital data flows are surveilled, especially the relationship between commercial and state surveillance;
- People working in the media and cultural sectors need to better explain these abstract dataveillance processes;
- Only then can public opinion on mass surveillance be meaningfully known.

Arising from this, we generated five significant public interventions:
- An art installation, *Veillance*, that makes people aware of their personal digital data flows via their smart devices, and the extent to which these are surveilled by commercial and state actors.
- A series of three short documentaries that we shared on social media.
- A project website, hosting the seminars' summaries and recommendations, main academic findings, blog and documentaries.
- A JISCMAIL listerv, PSST, to keep the conversation going after the life of the grant.
- A series of academic works exploring DATA-PSST issues.

1. Veillance

Veillance is a theory-practice art installation on processes of mutual watching. The DATA-PSST seminars inspired artist Ronan Devlin (Pontio designer-in-residence) to co-create an iterative, immersive art installation to raise awareness of personal data leakage, privacy and transparency. Across February - March 2017, '*Veillance'* projected on the four walls of a room in Pontio Arts and Innovation Centre (Bangor, Wales) some of the data (anonymised and re-rendered creatively) that attendees' digital devices publicly broadcast on connecting to the art's wifi.

The work highlights state surveillance of data by projecting onto the walls the captured data that matches the watchwords the government looks for in people's digital communications. It also highlights commercial surveillance by projecting the domain names of the companies that attendees' data flows to when connecting to the web via a mobile device. Finally, it also highlights 'sousveillance' (monitoring from a position of minimal power, and by those who are participating in the activity being watched), as the work responds directly to people's internet browsing while physically in the installation; people can witness their own, and each other's, data capture via the projections on the walls.

Funded by The Space, the team comprised Ronan Devlin (Project Manager and Artist), Carwyn Edwards (Developer), Ant Dickinson (Sound), Michael Flueckiger (Front end), Jamie Woodruff (Ethical Hacker), Vian Bakir, Andrew McStay and Gillian Jein (Bangor University academics).

2. Three short documentaries

DATA-PSST co-Investigator, Dyfrig Jones, attended the six full-day seminars, each of which discussed different aspects of transparency, privacy, security, surveillance and trust. He produced an online documentary, aiming to present the most important issues arising from this complex, inter-disciplinary and multi-end user discussion in an engaging way.

This took form as a triptych – a series of 3 short, interconnected documentaries on:
- *Empathic Media: Emotiveillance in Retail and Marketing* (about the rapid rise of a new form of data surveillance – of our emotions);
- *Sousveilance: Utah* (about the difficulties of publically documenting the NSA's surveillance centre in Utah);
- And *Veillance: Mutual Watching* (about the art installation to raise public awareness of their data flows via their smart devices).

3. DATA-PSST Project website
This hosts the seminars' summaries and recommendations, main academic findings, the blog and documentaries.

4. JISCMAIL listerv, PSST
This inter-disciplinary Privacy, Security, Sur/Sousveillance, Trust listserv keeps the conversation going after the life of the grant. *All are welcome to join in*.

5. Academic Publications
DATA-PSST directly informed two Special Issues of academic journals, a number of journal papers, and a book.

Special Issue: Veillance and Transparency: A Critical Examination of Mutual Watching in the Post-Snowden, Big Data Era. *Big Data & Society*, 4(1) 2017. Guest editors: Vian Bakir, Martina Feilzer, and Andrew McStay. [OPEN ACCESS]

This special issue presents a series of provocations and practices on veillance (i.e. processes of mutual watching) and transparency in the context of 'big data' in a post-Snowden period. In introducing the theoretical and empirical research papers, artistic, activist and educational provocations and commentaries, three central debates are addressed. Firstly, concerning theory/practice: how useful are theories of veillance and transparency in explaining mutual watching in the post-Snowden, big data era? Secondly, there are questions concerning norms, ethics, regulation, resistance and social change around veillance and transparency. Our third debate queries whether the upsurge in veillance and transparency discourses and practices post-Snowden are able to educate and engage people on abstract and secretive surveillance practices, as well as on the possibilities and pitfalls of sousveillance.

Contributors are as follows:
Guest Editor's Introduction:

- Vian Bakir, Martina Feilzer & Andrew McStay. Veillance and Transparency: A Critical Examination of Mutual Watching in the Post-Snowden, Big Data Era

Research Papers:

- Clare Birchall: Shareveillance: Subjectivity between open and closed data
- Andrew McStay: Empathic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy)
- Anthony Mills & Katharine Sarikakis: Reluctant activists? The impact of legislative and structural attempts of surveillance on investigative journalism
- Dan McQuillan: Algorithmic paranoia and the convivial alternative
- Lina Dencik, Arne Hintz & Jonathan Cable: Towards data justice? The ambiguity of anti-surveillance resistance in political activism
- Peter Mantello: The machine that ate bad people: The ontopolitics of the precrime assemblage

Artistic/Educational Provocations and Commentaries

- Evan Light: The Snowden Archive-in-a-Box: A year of travelling experiments in outreach and education
- Yvonne McDermott: Conceptualising the right to data protection in an era of Big Data
- Yu-Wei Lin: A reflective commentary of teaching critical thinking of privacy and surveillance in UK higher education
- Steve Mann: Big Data is a big lie without little data: Humanistic intelligence as a human right
- Jennifer Gradecki & Derek Curry: Crowd-Sourced Intelligence Agency: Prototyping counterveillance
- Benjamin Grosser: Tracing You: How transparent surveillance reveals a desire for visibility
- Piro Rexhepi: Liberal luxury: Decentering Snowden, surveillance and privilege

Special Issue: *Sleepwalking towards Big Brother? The Ethics of Communication in an Era of Mass Surveillance*. *Ethical Space*, 12 (3/4) 2015. Guest editor, Paul Lashmar.

The topics addressed in this Special Issue include the role of 'sousveillance', and journalistic and NGO strategies to deal with intelligence agencies. This includes:

- Paul Lashmar: Spies and journalists: Towards an ethical framework?
- Vian Bakir & Andrew McStay: Theorising Transparency Arrangements: Assessing Interdisciplinary Academic and Multi-Stakeholder Positions on Transparency in the post-Snowden Leak Era.
- Steve Wright: Watching them: watching us – where are the ethical boundaries?

Other academic publications from DATA-PSST:

- Bakir, V. 2015. Veillant Panoptic Assemblage: Critically Interrogating Mutual Watching through a Case Study of the Snowden Leaks. *Media and Communication* 3(3).
- Bakir, V. 2017. Political-Intelligence Elites, Strategic Political Communication and the Press: the Need for, and Utility of, a Benchmark of Public Accountability Demands. *Intelligence and National Security,* 32(3).
- Bakir, V. 2016. News Media and the Intelligence Community. In R. Fröhlich et al. (eds.) *Routledge Handbook of Media, Conflict & Security*. Routledge, pp. 243-254.
- Bakir, V. *in press* 2017. Afterword. In S.Flynn and A.Mackay (eds.) *Spaces of Surveillance: States and Selves.* Palgrave-Macmillan.
- Bakir, V.in preparation/2018. *Intelligence Elites and Public Accountability: Relationships of Influence with Civil Societ*y. Routledge.

Acknowledgements

A debt is owed to our participating PhD students, who wrote up summaries of each seminar and helped keep us on track:

- Abigail Blythe, Aberystwyth University
- George Petry, University of South Wales
- Tiewtiwa Tanalekhapat, Aberystwyth University

References

Anderson, D. 2016. *Independent Report: Investigatory Powers Bill: Bulk Powers Review*. Aug. CM 9326. Home Office.

Bakir, V., D. Miller, P. Robinson and C. Simpson 2017. *Fake News: A Framework for Detecting and Avoiding Propaganda*. Submission to Fake News UK Parliamentary Inquiry for Dept. of Culture, Sport and Media.

Bakir, V. 2015. "Veillant Panoptic Assemblage": Mutual Watching and Resistance to Mass Surveillance after Snowden. *Media and Communication* 3(3). ISSN: 2183-2439, Doi: 10.17645/mac.v3i3.277

Bakir, V. & A. McStay. 2015. Theorising Transparency Arrangements: Assessing Interdisciplinary Academic and Multi-Stakeholder Positions on Transparency in the post-Snowden Leak Era. *Ethical Space* 12 (3/4): 25-38.

Bakir, Vian, Cable, Jonathan, Dencik, Lina, Hintz, Arne & MStay, Andrew. 2015. *Public Feeling on Privacy, Security and Surveillance*. A Report by DATA-PSST and DCSS. November 2015.

Ball, K. et al. 2014. *Citizen Summits on Privacy, Security and Surveillance: Country report United Kingdom. SurPRISE. Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe*.

Bauman, Z., D.Bigo, P.Esteves, E.Guild, V.Jabri, D.Lyon and R.B.J. Walker. 2014. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* 8: 121–144.

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

Branum, J. and Charteris-Black, J. 2015. The Edward Snowden affair: A corpus study of the British press. *Discourse & Communication*, 9(2): 199–220. doi:10.1177/1750481314568544

Dencik, L. and Cable, J. 2017. The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks. *International Journal of Communication, 11:* 763–781.

Di Salvo, P. and Negro, G. 2016. Framing Edward Snowden: A Comparative Analysis of Four Newspapers in China, United Kingdom and United States. *Journalism* 17 (7): 805–822.

IAB 2012. *Consumers and Online Privacy 2012 - Bitesize Guide*.

Lischka, J.A. 2016. Explicit terror prevention versus vague civil liberty: how the UK broadcasting news (de)legitimatise online mass surveillance since Edward Snowden's revelations. *Information, Communication & Society*, DOI: 10.1080/1369118X.2016.1211721

Mann, S. 2004. "Sousveillance": Inverse surveillance in multimedia imaging. In *International Multimedia Conference: Proceedings of the 12th annual ACM international conference on Multimedia*, (pp. 620-627). ACM Press, New York.

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.

Marthews, A. and Tucker, C. 2015. *Government Surveillance and Internet Search Behaviour*. http://ssrn.com/abstract=2412564

McStay, A. 2017. *Privacy and the Media*. London: Sage.

McStay, A. 2016. Empathic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy), *Big Data & Society*: 1-11.

McStay, A. 2014. *Privacy and Philosophy: New Media and Affective Protocol*. New York: Peter Lang.

Mill, John S. 1962 [1859]. *Utilitarianism, On Liberty, Essay on Bentham*. London: Fontana Press.

Ofcom. 2015. *The Communications Market 2015* (August).

Pavone, V., S.D.Esposti, & E Santiago. 2015. *D2.4 – Key factors affecting public acceptance and acceptability of SOSTs. Surprise.*

Penney, J. 2016. Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal*. Pew Research Centre. 2016. The state of privacy in post-Snowden America, September 21.

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

Smith, A. 2015. U.*S. Smartphone Use in 2015*. Pew Research Centre.

Statista, 2017. Most famous social network sites worldwide as of April 2017, ranked by number of active users (in millions)**.** *Statista*.

Stoycheff, E. 2016. Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. *Journalism & Mass Communication Quarterly*, 93(2): 1–16. DOI: 10.1177/1077699016630255

Wahl-Jorgensen, K, L.K.Bennett & J.Cable. 2016. Surveillance Normalization and Critique. *Digital Journalism*. doi.org/10.1080/21670811.2016.1250607

Wahl-Jorgensen, K., L.K.Bennett and G.Taylor. 2017. The Normalization of Surveillance and the Invisibility of Digital Citizenship: Media Debates After the Snowden Revelations. *International Journal of Communication* 11: 1–22 1932–8036/20170005