Institution:
Bangor University, 10007857

Unit of Assessment:
UoA 21 – Sociology

Title of case study:
'Veillance': Digital Power & Accountability in an Era of Mutual Watching

Period when the underpinning research was undertaken:
2013 – 2020

Details of staff conducting the underpinning research from the submitting unit:

Name(s):	Role(s) (e.g. job title):	Period(s) employed by submitting HEI:
1) Vian Bakir	1) Professor in Journalism	1) September 2010 - present
2) Andrew McStay	2) Professor in Digital Media	2) September 2010 - present
3) Yvonne McDermott	3) Senior Lecturer in Law	3) November 2011 - August 2017

Period when the claimed impact occurred:
1 January 2014 - 31 July 2020

Is this case study continued from a case study submitted in 2014? N

1. Summary of the impact

Bangor University's research into 'veillance' has highlighted the harms to citizens arising from digital profiling by state and commercial entities including privacy violations and exposure to targeted online disinformation. This has enabled civil society to develop a better understanding of how to hold secretive state and commercial surveillant entities publicly accountable. The research has directly informed a range of national and international stakeholders and policymakers, including the UK parliament; the EU; the Indian and Jamaican Supreme Courts; the South African High Court; British and Irish professional journalist practices; nongovernmental organisations; and the wider public via global media coverage.

2. Underpinning research

Under the umbrella term *veillance*, Bangor University identified three clear processes of mutual watching, and an understanding of its power dynamics. They are: watching from positions of power (*sur*veillance), watching from positions of powerlessness, including peer-to-peer watching and watching the watchers to hold them accountable (*sous*veillance), and blocking being watched (*counter*veillance).

Following revelations by Edward Snowden, the US National Security Agency whistle-blower, of routine mass surveillance of people's digital communications by intelligence agencies to identify security threats, this issue became a wider public concern. Commercial organisations also routinely surveil people's data to serve audiences micro-targeted information, including disinformation especially during elections. These data flows are fed by people watching the self via wearables but also peer-to-peer watching via social media. Challenges to such state/commercial surveillant power include watching the powerholders to hold them publicly accountable via investigative journalism and resisting being watched via encryption.

In response, we held ESRC-funded seminars (GBP30,365) between 2014 and 2017 on *Debating & Assessing Transparency Arrangements: Privacy, Security, Sur/Sous/Veillance, Trust* **[3.a]**. They engaged 70 academics (from over 20 disciplines), data regulators, politicians, companies, NGOs, journalists, artists and ethical hackers drawn from Europe and north America to examine these various veillance practices, and to consider implications for public accountability of surveillant organisations. These seminars generated publications **[3.1, 3.5, 3.6]** and initiated further academic activity and grant capture comprising an AHRC Fellowship (GBP133,374) **[3.b]**, its publications **[3.3]** and significant multi-stakeholder engagement on dataveillance. These programmes of research intervened in political, regulatory, legal, journalistic, and public discourses; and created guidance to change journalistic and NGO professional practice as follows.

On public accountability of intelligence elites. Bakir's monograph explores the far-reaching impacts for citizens by the 'intelligence elites', namely networks of intelligence agencies and political-corporate-military entities, that create intelligence policies including digital surveillance **[3.1]**. Bakir identified their secrecy, silencing and propagandistic strategies for manipulating civil society, and society's arising difficulties in holding them publicly accountable.

On commercial data surveillance and 'fake news'. McStay's (2017) ground-breaking work on Digital Advertising clarified opaque practices of commercial data surveillance that enable targeted digital adverts **[3.2]**. Building on this, Bakir & McStay's (2017) work on future profiling, Artificial Intelligence (AI) and content optimisation is the first to identify commercial and propagandistic drivers of online 'fake news' and emotive disinformation. They establish how, since the 2016 US presidential election, it is a recognised phenomenon particularly in how its targeted manipulation of electorates poses problems for democracy. They also evaluated and proposed solutions to combat contemporary fake news and the near-horizon variant of automated fake news driven by AI and optimised to exploit emotions **[3.3]**.

On mutual watching, privacy and possibilities for resistance. McStay's (2014) monograph, Privacy and Philosophy, re-evaluated privacy's philosophical foundations, and implications for digital media **[3.4]**. Building on this, Bakir (2015) developed the unique concept of 'veillant panoptic assemblage' to highlight the interlinkages between state, commercial and peer-to-peer modes of watching digital communications. It identified possibilities and difficulties for civil society in holding surveillant organisations publicly accountable, where the panoptic state through its intelligence agencies secretly re-appropriates people's digital communications flowing through corporate platforms **[3.5]**. Applying the concept of the 'veillant panoptic assemblage' to legal thinking on consent and the right to data protection, McDermott (2017) examined challenges implementing this right in an era of big data and mutual watching **[3.6]**.

3. References to the research

Research Outputs

3.1 **Bakir, V.** (2018) Intelligence Elites & Public Accountability: Relationships of Influence with Civil Society. Routledge. Submitted to REF 2021 (REF identifier UoA21_28)
3.2 **McStay, A.** (2016) Digital Advertising (2nd ed.). Palgrave-Macmillan. (Copy available on request)
3.3 **Bakir, V.** & **McStay, A.** (2018) 'Fake News & the Economy of Emotions: Problems, Causes, Solutions', *Digital Journalism,* **6**(2), 1-22. DOI Submitted to REF 2021 (REF identifier UoA21_21)
3.4 **McStay, A.** (2014) Privacy and Philosophy: New Media & Affective Protocol. Peter Lang. Submitted to REF 2021 (REF identifier UoA21_42)
3.5 **Bakir, V.** (2015) 'Veillant Panoptic Assemblage': Mutual Watching and Resistance to Mass Surveillance after Snowden, *Media & Communication*, **3**(3) 12-25 DOI Submitted to REF 2021 (REF identifier UoA21_60)
3.6 **McDermott, Y.** (2017) 'Conceptualising the right to data protection in an era of Big Data', *Big Data & Society*, **4**(1), 1-7 DOI

Grants

3.a **Bakir, V**. (2014 - 2017) *DATA - PSST! Debating and Assessing Transparency Arrangements - Privacy, Security, Sur/Sous/Veillance, Trust.* Economic and Social Research Council (ESRC) ES/M00208X/1, GBP30,365 (BU: R07R04)
3.b **McStay, A**. (2015 - 2017) *Empathic Media: Theory-Building and Knowledge-Exchange with Industry, Regulators and NGOs.* Arts and Humanities Research Council (AHRC) AHM0066541/1, GBP133,375 (BU: R07R05)

4. Details of the impact

Because state and commercial surveillance of digital communications is complex and abstract, policymakers, lawmakers, civil society and the public were unaware of how online behaviour feeds these practices. They were also unclear on how to resist and/or hold surveillant organisations publicly accountable. Bangor University's research impacted national and international bodies by illuminating the causes of, and problems with, such 'veillance', including the power imbalances

therein, thereby guiding and enabling more informed solutions. These fall into three clear categories.

Public accountability of intelligence elites

a) *Guidance for National Union of Journalists (NUJ).* Members of the UK/Ireland trade union representing over 30,000 journalists often try to hold intelligence elites accountable in the public interest. Until recently, however, they lacked clear guidance on how to avoid surveillance. The 2016 Investigatory Powers Act allows bulk acquisition, storage and analysis of personal digital data by over 40 public bodies, including the police, with enhanced powers for intelligence agencies, including the hacking of encrypted messages. Informed by Bakir's research, in 2019 Bangor University and City, University of London co-created the first NUJ-endorsed plain English guidance to help all UK and Irish journalists protect their confidential sources and information **[5.1]**. This novel guidance was subsequently promoted to an international audience of journalists and editors at the International Journalism Festival in Perugia in 2019 and insights informing the guidance were conveyed to the European Broadcast Union in Berlin in 2015. Supporting the need for such guidance, Bakir and McStay submitted invited evidence to the House of Lords Joint Committee on Human Rights, *Inquiry on Human Rights on Attitudes to Enforcement*, in 2018 ('The Sorry Tale of British Journalism & our Right to Privacy') that improved its understanding of how British journalism minimally promotes privacy rights, preferring the intelligence elite's narrative on the need for surveillance for national security.

b) *NGO CAGE review of media strategy*. Bangor University's research prompted the NGO CAGE, which campaigns on behalf of people subject to extraordinary rendition and indefinite detention in the 'War on Terror', to review the adequacy of its media strategy when dealing with UK intelligence agencies. Bakir was the sole academic cited in its review **[5.2]**.

Commercial data surveillance and 'fake news'

a) *Shaping the direction of globally influential UK Parliament Inquiry into Fake News and Disinformation, Digital, Culture, Media & Sport (DCMS) Committee*. Bakir and McStay submitted evidence based on their research to Phase 1 of the Inquiry in 2017. They were instrumental in directly influencing Phase 2 between 2018 and 2019 of the Inquiry. Their evidence evaluated all 79 parliamentary submissions (from Phase 1) on how to combat fake news. It concluded that politicians should focus on the propagandistic and commercial causes of online disinformation spread by advertisers, public relations practitioners, digital intermediaries, mainstream media, intelligence agencies and the public and to prepare for technological changes that use AI to propagate disinformation. Bakir and McStay's recommendations were clearly reflected in the Inquiry Interim Report **[5.3]**. Bakir was one of only three academics subsequently invited to give oral testimony on user targeting, misinformation and AI-enhanced fake news **[5.4]**. The Inquiry's Interim Report included Bakir's recommendation on the establishment of a working group to monitor developments in the spread of false information in light of rapidly changing technology because 'what is around the corner may be much more worrying than what we have experienced to date' **[5.3]**. This Inquiry has been globally influential in raising awareness of the connection between digital surveillance and disinformation. It formed an 'International Grand Committee', 2018-2020, with representatives from the legislatures and governments of Argentina, Belgium, Brazil, Canada, France, Ireland, Latvia, Singapore and the UK to ensure that fundamental rights and safeguards of their citizens are not undermined by unchecked technology. It also led to the UK Government's Centre on Data Ethics & Innovation, established in late 2018, and tasked with guarding against digital disinformation.

b) *Advising on disinformation for wider UK/EU/global policymakers and regulators*. As a result of their expert advisory roles for the Fake News and Disinformation Inquiry, 2017-2019, Bakir and McStay have been invited to participate in disinformation and digital campaigning events, including the German and French Embassies, British-German Jurist's Association, DCMS Select Committee, Cabinet Office, Electoral Commission, Electoral Reform Society, Fair Vote, Information Commissioner's Office, and FoJo in Sweden. In 2018, they were key contributors to the European Commission White Paper on the internet's impact on echo chambers, fake news and populism, thereby defining a work programme of H2020 and FP9 research **[5.5]**. Their influential journal paper **[3.3]** was cited in UNESCO's Journalism Education and Training handbook, *Journalism, Fake News and Disinformation* (2018). In 2019, they submitted evidence to the All-Party Parliamentary Group (APPG) on Electoral Campaigning Transparency directly

informing its report **[5.6]**. By offering further advice on digital literacy and emotional profiling via an invited briefing paper they influenced the APPG's next steps in helping to restore electoral transparency to the parliamentary agenda for 2020. In 2019, Bakir and McStay submitted invited evidence to the House of Lords Select Committee on Democracy and Digital Technologies recommending greater transparency, explainability of algorithms, informativeness and civility in digital campaigns, and better media literacy for voters. Their insights were published in the Select Committee's Final Report **[5.7]**, which makes an urgent case for reform of electoral law as well as our overwhelming need to become a digitally literate society. In 2019, Bakir gave a keynote on solutions to digital disinformation to FoJo, an international gathering in Sweden of fact-checkers with subsequent coverage on *Sverige Radio*, Sweden's national public service radio.

Mutual watching, privacy and possibilities for resistance

a) *Citation of Bangor University authors in Supreme and High Courts in India, Jamaica, South Africa judgements affecting over 1,400,000,000 people*. Bakir's (2015) concept of 'veillant panoptic assemblage' was applied by McDermott (2017) to a legal context on data protection and consent in the information age, clarifying the nature of contemporary, ubiquitous 'veillance' and its privacy impacts. This research was cited by India's Supreme Court in ruling on a mandatory national identification system that informational privacy is a constitutional right that should be protected as part of the right to life and personal liberty. The ruling stated: *'There is what is now described as 'veillant panoptic assemblage', where data gathered through the ordinary citizen's Veillance practices finds its way to state surveillance mechanisms, through the corporations that hold that data' …The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection'* **[5.8]**. The ruling, including McDermott's work, was subsequently cited by Jamaica's Supreme Court in its 2019 declaration that a mandatory identification system is unconstitutional and a breach of privacy **[5.9]**. Bakir's (2015) work on veillant panoptic assemblage was cited in South African High Court case no. 25978/2017 regarding the constitutionality of the regime for state surveillance of private communications between members of the South African public **[5.10]**; accordingly, on 16 September 2019, the Court declared that bulk interception by the South African National Communications Centre is unlawful and invalid.

Bangor's work has achieved global media coverage through wide public engagement contributing to greater understanding of the need for public accountability of intelligence elites, problems with commercial data surveillance and its links to disinformation, and privacy implications of mutual watching and possibilities for resistance. It has been referenced 2 times in media with global reach; *BBC.com* and *al-Jazeera.com*, together reaching 700,000,000 people in over 100 countries. In addition Bangor University's work has received coverage in: *Vecer* (Slovenia, online readership 25,000 daily), *Business Daily* (Kenya, Africa's leading daily business publication), *Sverige Radio* (Sweden's public service radio, over 7,000,000 weekly listeners), The Indian Express (India, circulation 309,252 daily), *The Hindu.com* (16,350,000 average daily readers), *Gauri Lankesh News* (India, circulation 15,000) and *Spring News Online* (Thailand, over 2,000,000 Facebook followers). Bangor University's work is covered in 4 specialist publications in the UK and USA: *New Scientist* (circulation 124,000 weekly), *The Drum* (10,000 readers in Europe, North America, Asia-Pacific), *Adweek* (6,000,000 marketing professional online subscribers), and *Open Democracy* (3,500,000 unique yearly views largely from activists, journalists and policy influencers).

5. Sources to corroborate the impact

5.1 **National Union of Journalists (NUJ) website** hosting Journalism post-Snowden: a simple guide to protecting your information and contacts, generated by Bakir and Lashmar. The first NUJ-endorsed plain English guidance for journalists on how to avoid surveillance by Intelligence Elites. The full version is behind NUJ membership wall, but an abridged version is at:
http://intel-elites.bangor.ac.uk/douments/NUJ%20GUIDE%20Abridged%202019.pdf

5.2 CAGE **(2015) External Review Report**. A critical report in kickstarting scrutiny of media strategies for Intelligence Elites in which Bakir is the only academic cited.
https://docs.google.com/viewerng/viewer?url=https://www.cage.ngo/wp-content/uploads/free-downloads-files/temp-files/00856859100.pdf

5.3 Digital, Culture, Media & Sport Committee **(2018) Disinformation and 'fake news': Interim Report**. House of Commons 363. pp.24-25. Bakir recommends creating a working group to monitor developments in false information circulation given rapidly changing technology, leading to the establishment of a UK Government Centre to monitor such developments.
https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf
For parliamentary links to **Bakir & McStay's written evidence** where they propose attending to digital behavioural advertising's role in incentivising and combating fake news:
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/culture-media-and-sport-committee/fake-news/written/48101.html
For **Bakir and McStay's assessment of the Fake News Inquiry's 79 written submissions** from Phase One, distilling insights that shape Phase Two of the Inquiry:
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/written/71533.html
5.4 Parliament TV **(2018) Televised oral evidence of DCMS Committee, House of Commons Inquiry into Disinformation and Fake News**. Bakir is one of 3 academics answering questions on user targeting and misinformation, and the only academic on AI-enhanced fake news. (Evidence submitted is a screenshot; video on file; available on request).
http://www.parliamentlive.tv/Event/Index/63e3c7bd-97f8-4209-b2b1-50086390f377
5.5 Taylor, S. et al. **(2018) Opinion Forming in the Digital Age: Fake News, Echo Chambers and Populism - Key Themes, Concerns & Recommendations for European Research and Innovation**. European Commission. Bakir and McStay's contributions to this consensus report White Paper helped the European Commission define a work programme of research (H2020, FP9) on fake news, echo chambers and populism.
https://research.bangor.ac.uk/portal/files/22190899/Opinion_Forming_in_the_Digital_Age_Public_Recommendations_v1.0.pdf
5.6 All-Party Parliamentary Group (APPG) on Electoral Campaigning Transparency **(2020) Defending our Democracy in the Digital Age: Reforming Rules, Strengthening Institutions, Restoring Trust**. UK parliamentary report urging greater electoral campaigning transparency.
https://fairvote.uk/wp-content/uploads/2020/01/Defending-our-Democracy-in-the-Digital-Age-APPG-ECT-Report-Jan-2020.pdf
Appendix of APPG Report (containing Bakir & McStay's evidence) recommends concrete incentives for digital political campaigners to act more transparently, pp.245-258:
https://1u5lpf242yxl2669iu2mp449-wpengine.netdna-ssl.com/wp-content/uploads/2020/01/Defending-our-Democracy-in-the-Digital-Age-APPG-ECT-Report-Appendices-Jan-2020.pdf
5.7 House of Lords Select Committee on Democracy and Digital Technologies **(2020) Digital Technology and the Resurrection of Trust,** p,91, p.104, p.139. Urges electoral law reform and greater digital literacy.
https://committees.parliament.uk/publications/1634/documents/17731/default/
For parliamentary link to **Bakir & McStay's evidence** recommending greater transparency, explainability, informativeness and civility in digital campaigns and better media literacy, see:
https://committees.parliament.uk/writtenevidence/352/html/
5.8 India Supreme Court Judgment **(2017) IN THE SUPREME COURT OF INDIA CIVIL ORIGINAL JURISDICTION WRIT PETITION (CIVIL) NO 494 OF 2012,** pp.251-2, pp.264-5. Cites McDermott's application to a legal context of Bakir's concept of 'veillant panoptic assemblage', shaping a ruling that affects the whole of India (1,339,000,000 people).
https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf
5.9 Jamaica Supreme Court **(2019) JMFC Full 04,** para. 175, p.151, pp.116-117. Cites McDermott's application to a legal context of Bakir's concept of 'veillant panoptic assemblage', shaping a ruling that affects the whole of Jamaica (3,000,000 people).
https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf
5.10 High Court of South Africa, Gauteng Division, Pretoria **(2019) Case No: 25978/17,** p.9. Cites Bakir's work on the 'veillant panoptic assemblage', shaping a ruling that affects the whole of South Africa (58,000,000 people).
https://amabhungane.org/wp-content/uploads/2019/06/190212_amaB-heads-of-argument.pdf