Original Research Article

BIG DATA & SOCIETY

Big Data & Society
January–June 2018: 1–12

DOI: 10.1177/2053951718765021
journals.sagepub.com/home/bds
SAGE

Doing data differently? Developing personal data tactics and strategies amongst young mobile media users

Neil Selwyn[1] and Luci Pangrazio[2]

Abstract

Large amounts of personal data are generated through young people's engagements with mobile media, with these data increasingly (re)used by advertisers, content developers and other third parties to profile, predict and position individuals. This has prompted growing concerns over the ability of mobile media users to develop informed stances towards how and why their data is being used, i.e. to build 'conscious' and/or 'resistant' forms of 'data agency'. This paper explores ways of developing the critical consciousness and resistant practices of young mobile media users towards personal data. Drawing on research with 27 young people (aged 13–17 years), the paper describes efforts to make representations of third party use of personal data openly available as a basis from which to develop data-savvy tactics and strategies. The results of these interventions – while only partially successful – offer valuable insights into the technical, social and cultural issues that shape young people's engagement with personal data. The paper concludes by considering how concerns over data agency might be better aligned with the realities of young people's mobile media use.

Keywords

Personal data, data literacies, data obfuscation, mobile media, teenagers

Introduction

The proliferation of mobile devices and social media platforms has led to rapid growth in the generation of 'personal data' relating to individual users. These data range from profile details and platform interactions, through to the content of all posts, photos, videos and associated technical details. Personal data is also drawn from online activity external to social media platforms through social plug-ins and cookies, information gathered offline from data brokers, as well as demographic and psychographic information generated from sources as diverse as government censuses to supermarket loyalty schemes (Bodle, 2016). In addition, these data points 'contain metadata as well as unstructured and finely granular information, i.e. emotional expressions or affective exchanges' (Peacock, 2014: 2). While users consciously volunteer personal data, many forms of data are generated without an individual's awareness or understanding of where, how or why the data is being collected and re-appropriated.

The digital marketing industry that uses these data is opaque and complex, meaning that the (re)usage, collection and analysis of personal data by other parties has many aspects and dimensions that are unknown to users. In a technical sense, data that is attributable to individual users is a necessary operational element of social media platforms. Collaborative filtering algorithms, for example, process personal data to classify users, make suggestions and recommendations, and 'personalise' the platform (Chun, 2016). Such instances of personalisation, however, are distinct from profiling. Profiling uses personal information and data points to create identities on behalf of individuals that can be

[1]Monash University, Australia
[2]Deakin University, Australia

Corresponding author:
Neil Selwyn, Faculty of Education, Monash University, Wellington Road, Clayton, Melbourne, VIC 3800, Australia.
Email: neil.selwyn@monash.edu

used for marketing, management and risk assessment purposes (Bechmann, 2013: 75). Facebook, for example, offers third party advertisers options to target particular audiences and demographics by sharing a user's profile data specifying location, age, gender and languages. This data can also be accompanied by 'detailed information' on what a user shared on their timelines, the apps they use, the advertisements they click on, as well as applications and activities they engage with, such as their purchase history (Facebook, 2017). Application programming interfaces (APIs) and software development kits mean social media platforms enable connection with an array of other parties, such as 'businesses and institutions, ad publishers, ad intermediaries, third-party content developers, and users' (Helmond et al., 2017: 1).

In addition to these platform-specific data, data is facilitated by mobile devices. The rise of mobile media enables real-time tracking allowing the targeting of across multiple geographical locations and devices. Marketers and advertisers have welcomed this 'precise' targeting as it yields considerably greater returns on investment (Turow, 2011). Supported by predictive analytics, these detailed data profiles now lead to recommendations and advertisements that can appear uncannily accurate and prescient to the individual recipient. When replicated on a mass scale, these developments constitute a pervasive form of corporate surveillance (Bodle, 2016). Indeed, these data are being increasingly recirculated and reused in ways that have future consequences for the individuals concerned – from the advertising that they encounter, to various ratings and profiling used to determine social and economic outcomes. With commercial and government actors now relying on personal data to profile, predict and position individuals, concerns are being raised over the extent to which these processes are understood amongst the general population.

In light of this, academics from a variety of disciplines are now beginning to address the problem of how to best support individuals to adopt informed and critical stances towards the (re)use of their data. As such, a first step to developing critical data practices is to develop understandings of how data is processed. While these issues apply to all technology users, they are seen as particularly pertinent to young people aged between 13 and 17 years. This 'teenage' age group constitutes some of the most voracious but vulnerable users of mobile media. On one hand, it is widely accepted that 'smart' self-management of personal data can enhance young people's use of digital technology. However, European and North American research has highlighted a rising sense of powerlessness and/or apathy amongst teenagers with regards to personal data and their control over data privacy and security (Donovan, 2013; Pybus et al., 2015). Thus, growing efforts are now being made to support the development of data awareness and data literacy amongst young people in this age group.

Making sense of digital data agency – Strategies and tactics

The present paper addresses these issues from the emergent perspective of 'critical data studies' and associated academic work that seeks to advance accounts of how digital data is implicit in the operation of power in contemporary everyday life. Recent writing and research in this vein has highlighted the need to develop understandings of the politics of personal digital data (e.g., Boyd and Crawford, 2012; Kitchin and Lauriault, 2018; Van Dijck, 2013). As Dalton et al. (2016: 1) contend:

> Critical Data Studies calls attention to subject formation within these data regimes, for a critical examination of where the interpellation of the individual emerges in algorithmic culture and, through that, where the cracks and seams, the spaces for resistance and alternatives, might be found.

Such concerns have underpinned regular calls in this journal (and elsewhere) for researchers to address issues of data agency, i.e. to explore alternative ways 'in which power and participation [might be] constructed and enacted' in individual's data practices (Couldry and Powell, 2014: 1). Thus, it is reasoned that academic critiques of the disempowering nature of much data arising from technology use need to be balanced by explorations of how data might be repurposed to enhance individual agency, i.e. 'feeding such data back to users, enabling them to orient themselves in the world' (Kennedy et al., 2015: 1). Amidst this interest in 'citizen agency' with regards to digital data, Kennedy et al. (2015) point to the need for further research on users who might be classed as 'conscious' or 'resisting' agents. As they ask: 'can ordinary people do the same things with their data as corporations and organisations?' (p. 6).

These ongoing concerns resonate with previous debates in media and cultural studies with regards to issues of citizen resistance and empowerment. One useful frame of reference is Michel de Certeau's writing on resistance, subversion and re-appropriation in everyday life. In particular, de Certeau's (1984) *The Practice of Everyday Life* continues to offer insights into how people work with (and against) the 'formal structure of practice' in their everyday actions. Of particular significance is de Certeau's well-known distinction between strategies and tactics. Here, 'strategies' are described

as the ways in which powerful actors and dominant institutions get to define official practices and knowledge by encouraging people to engage with structures in ways that reaffirm the 'constructed order' of the city. In contrast, many people's everyday lives involve working around official structures by *not* relying on these official strategies and resorting instead to political practices and forms of knowledge that subvert, usurp and undermine official norms and 'ways of doing' – what de Certeau termed 'tactics'.

While the relevance of de Certeau's writing to the digital era can be questioned (e.g., Poster, 2006), this notion of strategies and tactics has continued potency when addressing issues of digital agency and resistance. These distinctions are certainly reflected in the practices currently being promoted by state, civil and commercial authorities as ways of improving young people's stewardship of their personal data. In de Certeau's terms, these tend to be strategies of making 'better' use of social media, i.e. engaging more carefully, thoughtfully and critically with organising procedures and protocols. For example, such strategies are implicit in calls for users to engage with 'cybersafety', 'internet awareness' and 'data privacy self-management'. Recommended practices here include developing users' awareness of the 'Terms Of Service' associated with social media platforms. They also include encouraging users to reconfigure settings, permissions and parameters of social media accounts; to block unwanted incursions; and generally pay attention to the permissions that they consent to be granted through platforms. These strategies therefore tend to demand individuals to become more vigilant of the risks implicit in engaging with digital devices and platforms.

The notion of personal data 'tactics', however, fits with a number of oppositional approaches towards digital media that have taken various forms during the past 30 years. For example, oppositional behaviour, subversion and resistance have long underpinned philosophies of the computer 'hacking' movement (Ross, 1991) as well as the rise of 'tactical media' during the 1990s and 2000s. Most recently have been calls for 'data obfuscation'. As Brunton and Nissenbaum (2015) detail, these are tactics of 'data disobedience' intended to mitigate, evade or perhaps sabotage dominant structures of data reuse and recirculation. In these terms, 'obfuscation is the deliberate addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection' (Brunton and Nissenbaum, 2015: 1).

So how might these concerns with strategies and tactics fit with the personal data practices of young mobile media users? The remainder of this paper reports on research exploring the capacity of young mobile media users to engage in such personal data strategies and tactics. In particular, the paper addresses the following research questions:

- What forms of engagement with personal data strategies do young people see as appropriate and/or attainable in terms of enhancing their engagement with mobile media?
- What forms of personal data tactics do young people see as appropriate and/or attainable in terms of enhancing their engagement with mobile media?
- To what extent (and with what outcomes) are young people able to develop new personal data strategies and/or tactics?

Research questions and methods

These questions were addressed through a 12-month research study that sought to work with groups of young people (aged 13–17 years) to cultivate their capacity to develop and implement critical personal data practices. Specifically, the project sought to explore personal data generation on mobile media devices. The project ran from July 2016 through June 2017, working with five groups (27 participants in total) in the Melbourne metropolitan area of Australia (see Appendix 1). These young people were recruited through local schools and engaged in the project activities during non-examination periods of the school calendar. In contrast to previous work by Pybus et al. (2015), most of the young people in the project had no particular background in computer programming and/or digital technology. Instead, they engaged in the project through the invitation to take part in 'workshops to explore practical strategies and techniques for protecting your personal data and privacy in online spaces'.

The project aimed to make use of social and computational science approaches to render processes of 'making data' and 'data mining' more accessible to ordinary users (Kennedy and Moss, 2015; Pybus et al., 2015). This was achieved through a combination of 'co-design' workshops (Bødker et al., 1993) and what Benjamin Haber (2016: 153) describes as code-based 'active experimentation with the forms and formulas of digital media'. In this spirit, a series of workshops were carried out with the young people over the course of the study. These workshops supported participants' engagement with a mobile app designed to give users insight into how their personal data was processed by industry-standard data analytics and profiling tools (in the form of three commercial APIs). This focus on APIs was deliberate. As Boyd and Crawford (2012: 674) put it: 'wrangling APIs, scraping, and analysing big swathes of data is a skill set generally restricted to those with a computational background'.

In total, the research was conducted over four distinct phases. The first phase of investigation involved exploring the young people's current understandings of personal data, and therefore establishing the types of mobile media practices and associated personal data which participants could then analyse and reflect upon during subsequent phases of the research. A second phase saw the researchers working with a software developer to build an Android smartphone app (titled 'PDQ' – an abbreviation of 'Personal Data Questions'). In Australia mobile phones are the most commonly used digital device, with 90% of teenagers using one daily and 79% using one for more than 3 hours a day (Australian Psychological Society (APS), 2017). PDQ took the form of a simple chat app to coincide with teenagers' most common digital practices. PDQ was capable of aggregating individual's personal data and then demonstrating to each participant how text, image and geolocation data would be processed by various APIs. In full, this involved:

- The use of natural language processing to extract metadata from chat logs (using the Cloud Language API);
- The use of shared images to extract metadata on the user, including sentiment analysis of faces and object recognition (using the Cloud Vision API);
- The use of GPS co-ordinates from participants' Android devices to map user whereabouts and reverse geo-coding to create user location metadata (using Google Maps API).

Rather than replicating any specific existing app, PDQ was deliberately generic in design in order to support tactics and strategies that could be easily translated to the various platforms the young people were making everyday use of. Once the app was fully developed and beta tested, participants then used PDQ (either on their own phones or from researcher-supplied phones for those without Android devices) to generate a sample of personal data over a designated seven-day period.

Using this personal data, the third phase of the study saw the groups engage in a series of workshops that focused on making better sense of their personal data practices, data trails and traces, as well as developing understandings of feasible personal data strategies and tactics. This phase of workshops involved researchers and participants engaging in a series of iterative activities that led each group towards co-operatively designing possible tactics and ways of engaging with strategies that might mitigate 'real world' problems that the young people identified from the processing of their data. Each workshop group worked towards the goal of producing what they considered to be feasible personal data 'challenges' that outlined possible alternate 'data savvy' ways of engaging with social media. One of the tools used in these workshops was the browser add-on Lightbeam in order to reveal third parties who were tracking data. In addition, using Lightbeam helped the young people develop a sense of the targeting parameters of the digital platform they were using (i.e. the second party) for sharing with third parties, such as marketing agencies.

The final (fourth) phase of the investigation then involved participants using mobile media and/or the PDQ app for another seven-day period where they attempted to enact one (or more) of the groups' data challenges. A concluding workshop was held to compare the differences between the initial and final sets of personal data generated from these uses of PDQ, thereby prompting further reflection on participants' ability to engage with social media in alternate critical ways. In all these latter workshops, participants' data traces were shared within groups only after individuals had been given an opportunity to review and approve the materials to be shared.

Findings

(i) *Personal data practices and (non)concerns*

The first phase of the research centred on making sense of the young people's current understandings of personal data. Most participants were frequent and eclectic users of social media encompassing a familiar range of platforms (Instagram, Snapchat and YouTube), albeit with little conformity across the groups. The only notable norm across the groups was a common wariness (if not rejection) of Facebook. This was justified on various grounds of generational difference ('for the oldies' (Sinead), 'a mum social media thing' (Jane)), needless features ('Facebook is way more complicated than it needs to be' (Sinead)) and a general irrelevance: 'no one uses Facebook… I was born in 2004' (Chelsea).

Most participants considered themselves to be making relatively 'safe' use of social media. This is a generation whose exposure to 'cybersafety' education throughout school was reflected in their social media habits. Tellingly, these quite deliberate practices contrasted with non-specific concerns about social media. Many participants expressed a vague unease over what might still be visible even after activating one's privacy settings ('you just don't know what other people can see of what you post, or what you're doing' (Jacob)). There was also uncertainty over the permanence of what was posted online. For example, one participant questioned the likelihood of data actually being 'deleted':

'everything that happens is recorded... like what goes online stays online' (Mia). Yet when pressed, there was little awareness of specific third parties beyond mention of 'malicious people' (Frank), 'someone creepy' (Phoenix), 'a master hacker or something' (Jade) or 'the government' (Ty).

Once the groups had used the PDQ app over a seven-day period, the next phase of workshops involved examining and making sense of the data generated from their activities. Of the three main types of personal data generated through the app, the young people's most immediate concerns related to the generation of geolocation data. While the workshops had discussed at length the rationale (and likely consequences) of permitting location tracking through PDQ, participants were nevertheless unnerved by subsequent analyses of their geolocational traces over the seven days of app usage. This was illustrated by our presentation of one user's data that highlighted visits to vegan/vegetarian restaurants and health food shops that were punctuated by visits to McDonalds outlets:

> **Researcher: So the app has identified a user here who is vegetarian and also goes to Maccas**...
> Chris: [cutting in] That's me! Yeah... I went to Westfield Maccas twice.
> Lachlan: Wait... the app can track us like that?
> **Researcher: Yes, if you activated the tracking option. You guys use heaps of apps that do exactly the same thing.**
> Veronica: That's kind of creepy.

Geolocation data was perceived as 'unsettling' (Nick) due to the accuracy of the API's analysis: 'it shows genuinely where I was' (Nick). A few participants expressed surprise that their location remained traceable: 'I didn't even have data on my phone so I do not know how that was tracking me' (Bree). Further reflection on the fact that PDQ was designed to analyse geolocation data had prompted one boy to decide to opt out of using the app outside of the school premises:

> Mac: I didn't use it because I knew you were tracking me
> **Researcher: But don't all the apps you use track you?**
> Mac: Yes... but that's always going on. Because I know you were tracking it, it felt different... it put me off using it.

In this sense, a main concern conveyed by participants was an indeterminate sense of 'creepy-ness'. Terms used here included: 'untrustworthy', 'annoying', 'frustrating', 'invaded'. As one participant put it: 'Well I was kind of aware that it tracks you, it's kind of just creepy... it's unexplained, so you just lead to assumptions and it's a kind of unknowingness and then your brain starts to jump to conclusions' (Mia). These discussions also raised uncertainties over 'who' was behind the mobile media platforms that young people were using. One set of discussions explored speculations whether 'people work for Instagram?' (Sinead), and if they could 'see everything that you do' (Rachel). All told, few conclusions were reached beyond the observation that 'it's a bit murky' (Frank). In contrast, the groups were considerably less unsettled by the API's text sentiment and image analyses – primarily due to the relative (in)accuracy of these results. For example, the API's emotional and personality analyses of participants' selfies had proven only sporadically credible (e.g., misidentifying faces as 'joyful', 'angry', 'male' or 'female').

Thus, many of the young people expressed an ambivalence towards these reappropriations of their personal data. Aside from geolocation data, most participants' concerns appeared assuaged by the lack of accuracy of the data analyses. Providing that misattributions did not cause obvious disadvantage, then most participants seemed unperturbed by the APIs labelling them as having 'visited Portugal', being British rather than Australian or 'interested in beauty products':

> I feel that if it isn't going to affect me in a negative way it doesn't really bother me. When it says that I am British then I'd just go 'Well, no I'm not'. So little things like don't really bother me. But, if it was to say things that could potentially get me into trouble then I'd probably care a bit more. (Ricky)

Participants seemed comforted by the fact that '[the apps] are guessing and they don't actually have something that can tell you how I was feeling that day. Because that would be creepy' (Simone). Some young people were happy to simply dismiss the API analysis as 'fake' (Shanya). As another participant reacted to some of his personal characteristics being diagnosed inaccurately by the text sentiment analysis processing:

> I don't take it personally... it's more like it's funny... it funny that they tried so hard to work out what I wanted or who I was and then got it so wrong... it's just the computer getting it wrong, so 'Ha ha... nice try!' (Ljudevit)

Throughout these discussions, it was notable how nearly all the young people remained non-plussed by PDQ's demonstrations of how advertisers use personal data. The use of data for targeted advertising was felt to be an acceptable element of mobile media use. As different participants reasoned: 'What's so bad about advertising anyway? Because if you don't want it, you

don't buy it. And if you do, then it just helps you, so it's a good thing' (Dom). In this sense, having personal data tracked and analysed by third parties such as marketing agencies was seen an acceptable aspect of contemporary digital technology use. It was also felt that 'Terms of Service' agreements could not be engaged within an agentic manner: 'Yeah, because if you ''Disagree'' they won't let you [use the app]. So you have to agree' (Olivia); 'It's all the same…it's not really signing, it's just clicking ''Agree''' (David). In this sense, rather than seeing the appropriation of personal data as cause for concern, many instances of the PDQ analysis were judged to be relatively unproblematic: 'That's just the way of the world… it's the way things are these days. It's not a drama. You know about it, but there's not much you can really do' (Matt).

(ii) *Doing data differently? Adoption of strategies and tactics*

The final phase of the project was designed to address these emerging understandings and to explore possibilities for alternate practices and actions. Most participants initially found it difficult to articulate what they had gleaned from using PDQ. A few participants maintained that they 'really don't care' (Lachlan), with many reasoning that they 'cared… but not enough to do anything' (Matt), for example:

> Ty: It's something that I think we're all aware of but we don't really do… I mean I just can't be bothered to turn off my microphone or my GPS or whatever.
> Simone: Yeah. When you go into Snapchat you don't think someone's going to record me doing this.
> Shayna: I don't know… I mean, what's the worst that's going to happen?

Yet as the workshop discussions progressed, most of the groups became more interested in exploring possible ways of feeling more 'positive' (Dom), 'safe' (Rachel) and less 'weirded out' (Bree) with regards to the (re)use of personal data. Despite this increased interest, it nevertheless proved difficult to develop tangible ideas for what was collectively framed as 'Doing Data Differently'. Indeed, the initial design workgroups around this theme struggled to move beyond exaggerated forms of counter-practice, e.g. persuading people to 'delete every app now' (Ljudevit), 'less use of it' (Sara) or 'getting onto the deep web' (Matt). However, after discussing a range of 'data safety' strategies and 'data obfuscation' tactics, four of the groups designed simple protocols based around the following 'challenges':

- Strategic challenge: 'Investigating the Terms Of Service'
- Strategic challenge: 'Doing ''due diligence'' on platform companies'
- Tactical challenge: 'Running ad-blocking, tracking and geo-spoofing software'
- Tactical challenge: 'Selfie obfuscation'

Participants then chose one (or sometimes two) of these 'challenges' to pursue over a second seven-day period – the results of which are now described in more detail:

a. *Investigating the Terms of Service*

The most popular 'challenge' was researching and reporting back on the 'Terms Of Service' of popular mobile media platforms. Two groups were formed: one researching Skype and the other researching Instagram. None of the young people could recall having read more than a few lines of any of the Terms of Service before. As it transpired, this challenge was more difficult than it first appeared with only a couple of girls in the Instagram group managing to read fully through the platform's Terms of Service. Even these young people felt that they remained relatively uninformed. The overriding sense was of the obtuse nature of the text – 'it takes pages and pages' (Jade); 'just so they can hide stuff in there that you might not like' (Mac). The group was especially struck by the nature of the language:

> The language they use is really misleading. The Instagram ones phrased things in a way that if you read it quickly or skimmed it then it sounds like it's OK. But if you go back over it then its worded in a way that's like 'IF you do this… THEN there's a chance'. It's kind of like hiding it even if you do read it. (Mia)

The consensus from these investigations was that the Terms of Service could easily be truncated into 'summarised versions' of a couple of sentences (Mia). Moreover, none of the group felt motivated to read through full Terms of Service in the future.

The group scrutinising Skype's Terms of Service also identified areas of contention. For example, the regular mention of 'accordance with the Microsoft Services Agreement' raised the issue of Skype's ownership by Microsoft. This led to reflections on which third parties might conceivably come under Skype's terms of sharing data with 'Microsoft-controlled affiliates and subsidiaries, [and] vendors working on our behalf'. As the group discussion continued:

> **Researcher: So who are these 'Affiliates and subsidiaries'?**
> Olivia: Heaps!

Veronica: If you use a Windows computer.
Matt: Xbox.
David: Minecraft.
Rachel: Even the Windows store or people that sell Microsoft stuff?

The group was also taken with the subsequent stipulation of data being 'shared' by Skype 'when required by law or to respond to legal process; to protect our customers; to protect lives'. Nevertheless, the Skype Terms were judged as an acceptable way for Microsoft to absolve themselves of responsibility for illegal use of their service: 'I guess it sort of stops them getting sued, so it's a money-saving thing on their part' (Mac). Most agreed that this was also a laudable, civic-minded justification for sharing data:

Matt: Back when Skype first came out it wasn't really scanned at all. So that why a lot of illegal activity happened over messages and that. So that's why they started the scanning.
Ljudevit: It's not particularly shocking.

b. ***Doing 'due diligence' on platform companies***

Another popular co-designed 'challenge' was researching and reporting back on the commercial background of popular social media platforms – what was termed 'doing due diligence'. The most productive investigations were from a group of three boys who were keen users of the Discord app. Discord had been described in effusive terms during the initial workshops as an alternative 'grass roots' form of social media. In these initial descriptions, the boys described the app as a 'Skype-buster' (Frank) that had been set up by gamer communities as a controllable means of communicating via video and text in small groups – 'It's just like us four and a few other people that we know' (Ljudevit). These boys' use of Discord was presented as a way of not having to 'use any mainstream social media' (Frank):

Ljudevit: Discord is just a very niche thing, pretty much for people who use video games.
Frank: Mostly for the games market.
Researcher: So who owns Discord? Is it owned by Facebook?
Ljudevit: No, I think it's just run by itself. It's its own company.

After these initial conversations the boys decided to research Discord further, exploring questions of privacy and the app's business model. In terms of privacy, the group inferred that Discord's 'niche' origins ensured that data sharing was not a core feature of the site; 'Discord is relatively private. The only other people that could see what we've written down are the people who run it' (Frank).

In terms of its commercial basis, an initial presumption was that the site had been established through 'crowdfunding maybe?' (Frank). This was amended with the discovery of an optional 'subscription service you can do'. All told, the ownership of the site by a company that was not a recognisable technology corporation was seen to lend it a degree of credibility and trustworthiness: 'It's not actually owned by anything big like Facebook or Google' (Ljudevit). That said, during one of the final workshops we guided the boys through different sections of the Discord website that detailed the company's background, its major backers (Time Warner and Tencent), $30 million raised 'from top VCs in the valley' and its 'HypeSquad' model of paying teams of users to recruit friends to subscribe to the service. As well as exploring the app's Terms of Service we also encouraged the group to use Lightbeam to trace the App's data sharing with other parties. Having completed these investigations, the boys nevertheless presented essentially the same overview of Discord at the final session:

Researcher: So what did you find?
Frank: It's pretty much Skype but its focused for gamers, for that particular niche.
Ljudevit: Its very bog standard. Interestingly the Terms and Conditions are not particularly long. They basically say 'Don't do a naughty and you'll be good'.
Frank: There was an interesting thing where it had a thing called 'Your Data'. It was a thing that basically said... 'Yeah, well we SORT of collect your data but it is your own. We don't really do anything with you and it's your fault if anything happens to it!
Researcher: Who owns it?
Frank: It's just standalone company... it's not like Facebook... it's like Skype when it first started, there's just a few people who own it and that's it.

c. ***Running ad-blocking, tracking and geo-spoofing software***

A third 'challenge' related to blocking, tracking and spoofing software designed to give users more control over their personal data. A small number of participants volunteered to test ad-blocking software, although none eventually downloaded or used any applications. The reasons given for not following through on this challenge related to a set of general concerns. Having found some programs, a couple of

participants remained unconvinced that blocking software would be effective – an assumption based on their shared 'scary' experiences of continuing to receive targeted advertising even after 'turning cookies off' (Jade). Another participant did not want to compromise the security of his device: 'I worry to download those things because I don't want to get viruses on my computer... So I don't like downloading ad blocks or antiviruses' (Mac).

This lack of actual implementation also extended to the various data-tracking plug-ins and apps that participants were introduced to in the workshops. Having seen Lightbeam, participants were initially enthused. However, none of this group made use of the application outside of the workshops. Some participants had found it too difficult to work out how to install and run the applications. A few participants also raised doubts over the actual effectiveness of tracking apps:

> I feel like we're fighting a losing battle at the end of the day. Like, you know Chrome? There's a thing called Incognito, but Google Ads I think are still able to track you even if you're using Incognito... because Google made Incognito. (Mac)

One participant, who self-styled himself as a 'hacker', made grand plans to deploy geo-spoofing software and fool the PDQ app into 'thinking that I am the leader of a small African state' (Mac). However, by the time of the final session he had not done this, claiming a lack of time while also alluding to the difficulty of actually doing this in practice. By the time of the final workshop only one member of the group had been prompted to take action – altering the privacy settings on her Firefox browser to put 'tracking protection on' (Olivia). She had been prepared to do this because it was on 'the official, like, Firefox website, the official thing that Firefox has approved'.

d. *Photo obfuscation*

The final 'challenge' detailed various obfuscation tactics related to the APIs' photo analysis and facial recognition features. Three participants researched a range of tactics including 'CV Dazzle' make-up, stealth clothing, asymmetrical haircuts and facial jewellery. Eventually two participants attempted to alter 'selfie' photographs in an effort to mislead the Vision API. Despite their interest in the obfuscation options, neither of the participants opted for altering hairstyles or experimenting with make-up. At best, one of the boys did allow his photo to be digitally altered to give the appearance of wearing the camouflage-like 'Dazzle' makeup designed to disrupt automatic facial recognition analysis. One tactic that was deployed was to take 'ugly selfies'. These were of limited effectiveness, although one participant opted to lowlight his profile and look away from the camera – thereby misleading the Image API into analysing the image as non-human. Despite their amusement with the concept, no participant saw this as a viable future practice:

> Chang[ing] haircut would be too difficult for most people ... a lot of people care a fair bit about how their hair looks, so I don't think they would change it just so [third parties] can't see what you look like. (Ricky)

(iii) **Reflections and future intentions**

These co-designed challenges were intended to support, provoke and/or cajole participants into reflecting on their personal data practices. The relative lack of success highlights the complex relationships that young people have with digital technology use and personal data practices. Even when cognisant of the issues and options, most participants were not compelled to act differently. This inertia related to doubts over the effectiveness of any alternative actions coupled with understandable issues of lack of time and expertise. It was also telling that greater numbers of participants opted to pursue the strategic 'challenges' of becoming better informed, rather than the tactical 'challenges' of downloading tracking/blocking software or obfuscating images. Only a few participants reckoned that these activities might influence their future practices: 'Having the thought in the back of your head that [third parties] can get more specific things might prompt me to be more careful and cautious when it asks for location or things like that' (Ricky). In contrast, a few others remained staunchly indifferent – maintaining that 'I'm really too busy to care. I guess so many people use [social media], and it doesn't really bother me' (Lachlan); 'It's not like it's life or death or whatever' (Dom). Others reported feeling more unsettled and 'overwhelmed' (Jane).

Perhaps the most revealing feeling was one of annoyance. Here it was reasoned that the responsibility for action should not fall onto individual users. Instead, any change of behaviour should come from the platform providers and third parties:

> It's kind of annoying because you can be in control, but there are so many steps you have to take in order to do that. (Frank)
>
> I feel like you shouldn't have to do all of these complicated and very time-consuming steps. I feel like there should be a better way to do it. (Chelsea)

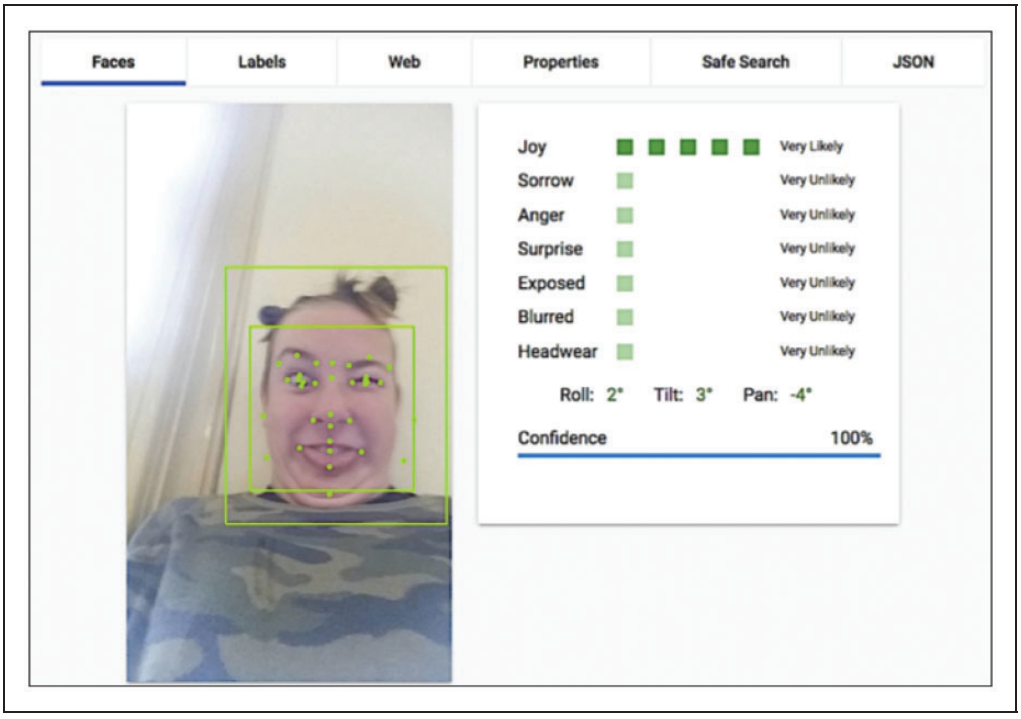

Figure 1. 'Selfie obfuscation' and resulting API emotion analysis.

> I think it's both the users' fault but also the people who own Instagram and stuff like that. (Mia)

Discussion and conclusions

This paper contributes to a growing literature seeking to explore data agency amongst ordinary users – seeking to mitigate what Beer (2009) terms the 'technological unconscious' in favour of moving towards the 'conscious user' (Kennedy et al., 2015: 6). Our study was limited in scope and timing and requires refinement and extension in other settings. Nevertheless, it offers initial insight into the complex nature of these young people's personal data practices, as well as providing further insights into current academic enthusiasm for data agency. In short, while our research was successful in (temporarily) making young people 'conscious' of the personal data implications of social media use, it was less successful in supporting their actions as 'resisting agents' (Kennedy et al., 2015). So how should we make sense of this disarticulation between personal data awareness and personal data actions?

It is important to first acknowledge the young people's levels of interest in (and concerns about) these issues. Throughout the research we found our participants to be interested in (and occasionally intrigued by) the 'politics of data'. They could quickly comprehend connotations of their personal data flows and recirculations and developed a range of insightful responses to the re-articulation of data generated by their (seemingly) innocuous engagements with social media. Personal data privacy was a matter of concern for the young people in our study (Boyd, 2014), albeit in rather under-defined terms. Indeed, most saw the sharing of data with advertisers as an acceptable trade-off: 'seeing more value in being active and sharing information on [social media] than protecting their information' (Suh and Hargittai, 2015: 9). Reaching such compromises appeared to be a way for the young people to counter feelings of being 'overwhelmed' with a reassurance that they were 'in control' (at least in terms of their data exchanges with known others).

Yet regardless of this understanding and awareness we remained a long way from achieving our goal of supporting the development of personal data practices amongst young social media users that might result in heightened engagement with the politics of personal data. Indeed, the majority of participants remained notably nonplussed by the range of counter-practices that might result from these enhanced understandings. There was some interest in tentatively engaging with a couple of the information-based strategies that were foregrounded in the workshops. For example, there was some interest in better engaging with the 'Terms of Service' of popular platforms and asking questions of underpinning business models. Yet, as de Certeau (1984) reminds us, such strategies essentially act to

maintain the status quo – establishing boundaries and relations between 'producers' and 'consumers', and often justified on the grounds of technical rationality and the general maintenance of order. Conversely, there was little sustained interest in pursuing any of the more involved social media tactics – what de Certeau (1984: 37) describes as transgressive forms of 'trickery' in the face of the plans of organising authorities. Despite initial intrigue, these social media tactics were seen as too time consuming and impractical to be of genuine use.

This is not to say that the young people lacked the ability to engage in tactical counter-practices. The groups made a range of imaginative choices when it came to identifying possible tactics and ways of engaging with strategies. While some struggled to download blocking and tracking software, others demonstrated a creative capacity to produce cryptic messages and ugly selfies. Yet even after our series of interventions, the young people in our study were not particularly motivated to interact in a resistant manner with unknown third parties or relatively remote advertisers. As Brunton and Nissembaum (2015: 7) describe: 'obfuscation is contingent, shaped by the problems we seek to address and the adversaries we hope to foil or delay'. If third party use of personal data is not seen as a problem, and if platforms and advertisers are not seen as adversaries, then there is little/no motivation to act in an obfuscatory manner.

Perhaps most telling was some participants' 'annoyance' of having to engage in resistant and obfuscatory practices. In part, this annoyance related to what was described in various ways throughout the workshops as a hindrance of time, e.g. the 'time consuming' nature of counter-practices, feeling 'too busy to care' and so on. This suggests that engaging differently with social media was *not* perceived by the young people as something that could be a contingent, 'just-in-time' action, i.e. something that is 'seized "on the wing"' (de Certeau, 1984: xix). As noted in studies of everyday uses of digital media, social media use is predicated upon the development of habits to ensure ongoing connection to networked cultures (Chun, 2016). In this sense, it is understandable that the idea of any sort of break in social media routines might be perceived initially as a substantial, time-consuming undertaking, thereby leaving users feeling reluctant to move beyond a state of 'inter-passive' acceptance of the status quo (Davis, 2013). Thus, it might be that progression of critical data practices is a long-term proposition for many individuals. These, perhaps, are not ideas that can be quickly encountered, accommodated and then acted upon. Any impact of our short-term inventions on the digital practices of these young people might well be deferred and gradually realised over years rather than months. These issues of temporality certainly need to be foregrounded in future research design with this age demographic.

Another facet of the participants' annoyance was their sense that personal data privacy should be the responsibility of platform providers. While this could be seen as an optimistic reading of the for-profit agendas of social media platforms, it could also signal the beginnings of a political consciousness that insist powerful actors be regulated to protect individual's data rights. Indeed, a strand of critical data scholarship (Andrejevic, 2014; Boyd and Crawford, 2012; Fuchs, 2014) makes a similar argument that while individualised agency is to be encouraged, powerful actors, like platform operators and governments, also need to address the problematic information asymmetry that drives the data economy. So while these young people did not exude an innate willingness to take on the additional effort involved in online tactics of resistance or obfuscation, they might be more inclined to advocate for collective action and regulation.

While these latter sentiments are understandable, we would argue that the need remains to continue considering ways of supporting young people to be actively agentic in the (re)use of their personal data. While engagement with 'Terms of Service' and altering default platform settings is a start, such strategies do little to address power relations between social media providers and users. These are actions that maintain conformity with the 'proper' dominant ordering of platforms such as Instagram and Snapchat, and distract attention from the wider socio-technical systems within which data practices are situated. Indeed, critical learning about digital systems cannot result solely from an increased commitment from providers to act in more 'transparent' or 'accountable' ways, i.e. through the detailing of Terms of Service, financial information and business models, or providing access to code and algorithms. As Ananny and Crawford (2017) reason, having everything made visible and comprehensible does not lead to critical understanding. Instead, critical understanding is likely to result from active engagement with a system.

Yet the notion (advanced by the young people in our research) that active engagement with personal data can (or should) not be driven by the individual is an important issue to consider. All of the strategies and tactics explored in our study place considerable demands on the individual user. Even 'fully' reading terms of service or running Lightbeam involves significant amounts of sense-making work and expectations of rational decision-making on the part of each individual user – 'plac[ing] a tremendous burden on individuals to seek out information about a system, to interpret that system, and determine its significance' (Ananny and Crawford, 2017: 7). Thus, it is perhaps

unsurprising that our participants remained unenthusiastic about the 'agentic' choices that we were attempting to support them in making. Their non-committal reactions to the strategic and tactical challenges conveyed a strong sense that 'informed resistance' is even more of a challenge than 'informed consent'.

This all suggests a need to further explore the degree of agency that 'ordinary' users are practically able to exercise over personal data. To return to the writing of de Certeau (1984: xx), our research appears to confirm that the social media landscape is 'too tightly woven for [users] to escape from'. These young people certainly seemed to be have been disciplined into 'the formal structure of [social media] practice' (de Certeau, 1984: xv), and therefore displayed a reticence to transgress. Thus, on the basis of our study we might conclude that young people cannot be expected to face these challenges on their own. The development of personal data tactics is perhaps better approached along collective lines. Indeed, de Certeau (1984: xi) was keen to stress that tactics 'does not imply a return to individuality'. It would seem sensible to presume that tactical engagement with social media might be more effective if carried out by groups and collectives rather than individuals.

Unfortunately this conclusion does not lead to any neat recommendations or solutions. One obvious set of stakeholders to be involved in working out ways forward are the social media platforms, data brokers and internet service providers. As some of the young people in our study concluded, it makes sense that these commercial concerns play a more active role in ensuring that young people are protected (or at least given meaningful choices) when it comes to the appropriation of personal data by third parties. Yet it is perhaps unrealistic to expect for-profit actors to self-regulate and/or reform conditions under which personal user data is generated and recirculated. As Peacock (2014: 7) asserts: 'online corporations operating in a dysfunctional information market do not self-regulate because it puts them at an economic disadvantage'. Another obvious set of stakeholders is the state and government actors – yet here it also remains unclear whether vested interests preclude the will to alter current conditions. Moreover, in light of the Snowden revelations, it could be argued that there are few reasons to expect sustained interest amongst most governments to alter the use of personal data within their jurisdictions (Obar, 2015).

Perhaps the most fruitful suggestions relate to encouraging non-official actions and practices. Yet this will be no easy task. Indeed, this paper has highlighted the difficulties of non-official attempts to encourage and support the development of 'critical' data practices amongst young mobile media users. This is not to suggest that we give up completely on the idea of working to foster increased data agency amongst young people. There is clearly a need to continue exploring the complex, challenging nature of the task. Above all, this paper points to the need to further refine understandings of the broader context of young people's everyday lives and data practices. These young people were neither locked into using the same social media platforms, nor particularly perturbed by the intrusion of advertising or commercial interests in their lives. Yet these *were* young people who recognised their uncertainties regarding personal data. In light of this, it seems prudent to continue work towards involving young people in the cultivation of critical (but realistic) discourses around personal data.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received financial support for the research, authorship, and/or publication of this article: This paper is based on research funded by the auDA Foundation (2016-2017 grants scheme).

ORCID iD

Neil Selwyn http://orcid.org/0000-0001-9489-2692
Luci Pangrazio http://orcid.org/0000-0002-7346-1313

References

Ananny M and Crawford K (2017) Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media and Society*. Epub ahead of print. DOI: 1461444816676645.

Andrejevic M (2014) The big data divide. *International Journal of Communication* 8: 1673–1689.

Australian Psychological Society (APS) (2017) *Digital Me*. Melbourne: Australian Psychological Society. Available at: http://compassforlife.org.au/digital-me-survey/ (accessed 7 March 2018).

Bechmann A (2013) Internet profiling. *Medie Kultur* 55: 72–91.

Beer D (2009) Power through the algorithm? *New Media and Society* 11(6): 985–1002.

Bødker S, Grønbæk K and Kyng M (1993) Cooperative design. In: Schuler D and Namioka A (eds) *Participatory Design*. Hillsdale, NJ: Lawrence Erlbaum Associates, pp. 157–175.

Bodle R (2016) A critical theory of advertising as surveillance. In: Hamilton J, Bodle R and Korin E (eds) *Explorations in Critical Studies of Advertising*. London: Routledge, pp. 138–152.

Boyd D (2014) *It's Complicated*. New Haven, CT: Yale University Press.

Boyd D and Crawford K (2012) Critical questions for big data. *Information, Communication and Society* 15(5): 662–679.
Brunton F and Nissenbaum H (2015) *Obfuscation*. Cambridge: MIT Press.
Chun W (2016) *Updating to Remain the Same*. Cambridge: The MIT Press.
Couldry N and Powell A (2014) Big data from the bottom up. *Big Data & Society* 1(2). DOI: 10.1177/2053951714539277.
Dalton C, Taylor L and Thatcher J (2016) Critical data studies. *Big Data & Society* 3(1): 1–9. DOI: 10.1177/2053951716648346.
Davis M (2013) Hurried lives. *Thesis Eleven* 118(1): 7–18.
de Certeau M (1984) *The Practice of Everyday Life*. Translated by Steven Rendell. Berkeley: University of California Press.
Donovan G (2013) *My Digital footprint.org*. Doctoral Thesis, Faculty of Psychology, CUNY, New York.
Facebook (2017) About ad targeting. *Facebook Business*. Available at: https://www.facebook.com/business/help/717368264947302 (accessed 7 March 2018).
Fuchs C (2014) *Social Media*. London: Sage.
Haber B (2016) The queer ontology of digital method. *Women's Studies Quarterly* 44(3): 150–169.
Helmond A, Nieborg D and van der List F (2017) The political economy of social data. *Association for Computing Machinery, #SMSociety'17*. Epub ahead of print 2017. DOI: 10.1145/3097286.3097324. Available at: https://dl.acm.org/citation.cfm?id=3097324.
Kennedy H and Moss G (2015) Known or knowing publics? Social media data mining and the question of public agency. *Big Data & Society* 2(2): 1–11. DOI: 10.1177/2053951715611145.
Kennedy H, Poell T and van Dijck J (2015) Data and agency. *Big Data & Society* 2(2): 1–7. DOI: 10.1177/2053951715621569.
Kitchin R and Lauriault T (2017) Towards critical data studies. In: Thatcher J, Shears A and Eckert J (eds) *Thinking Big Data in Geography: New Regimes, New Research*. Lincoln, NE: University of Nebraska Press, pp.3–20.
Obar J (2015) Big Data and The Phantom Public: Walter Lippmann and the fallacy of data privacy self-management. *Big Data & Society* 2(2): 1–16. DOI: 10.1177/2053951715608876.
Peacock SE (2014) How web tracking changes user agency in the age of Big Data: The used user. *Big Data & Society* 1(2): 1–11. DOI: 10.1177/2053951714564228.
Poster M (2006) *Information Please*. Durham, NC: Duke University Press.
Pybus J, Cote M and Blanke T (2015) Hacking the social life of Big Data. *Big Data & Society* 2(2): 1–10. DOI: 10.1177/2053951715616649.
Ross A (1991) Hacking away at the counterculture. In: Penley C and Ross A (eds) *Technoculture*. Minneapolis: University of Minnesota, pp. 107–134.
Suh J and Hargittai E (2015) Privacy management on Facebook: Do Device Type and Location of Posting Matter? *Social Media + Society* 1(2): 1–11. DOI: 10.1177/2056305115612783.
Turow J (2011) *The Daily You*. New Haven, CT: Yale University Press.
van Dijck J (2013) You have one identity. *Media, Culture and Society* 35(2): 199–215.

Appendix 1

NOTE

Gender and age characteristics of the quoted participants

Bree	Female, 13 years
Chelsea	Non-binary, 13 years
Chris	Male, 15 years
David	Male, 14 years
Dom	Male, 14 years
Frank	Male, 14 years
Jacob	Male, 16 years
Jade	Female, 13 years
Jane	Female, 14 years
Jordan	Male, 13 years
Lachlan	Male, 14 years
Ljudevit	Male, 14 years
Mac	Male, 14 years
Matt	Male, 15 years
Mia	Female, 14 years
Nick	Male, 17 years
Oliva	Female, 15 years
Phoenix	Male, 15 years
Rachel	Female, 15 years
Ricky	Male, 17 years
Sara	Female, 13 years
Shanya	Female, 14 years
Simone	Female, 14 years
Sinead	Female, 14 years
Ty	Male, 13 years
Veronica	Female, 14 years