Open Data and Privacy

Chapter editor: James Lowry and Anna Sexton
Chapter contributing authors: James Lowry and Anna Sexton

Summary
This review looks at the regulatory environment for privacy in the open data environment in the United Kingdom, and civil society work on privacy in the same context. The temporal coverage of the review is 2011, when the open data movement began to accelerate in the UK, to 2019. The review begins by acknowledging the political nature of data, framing the discussion in terms of data politics and notions of open societies and environments. The review then surveys the privacy laws, regulations, policies and resources issued by the state ('privacy from above') before looking at the resources and campaigns for privacy coming out of civil society ('privacy from below'). The review suggests that civil society action is less concerned with data release than with methods of data collection and sharing between public and private sector actors.

Key words: open data, openness, open government, privacy, data protection, surveillance, dataveillance

Introduction

Defining 'data politics', Ruppert, Isin and Bigo wrote that data politics is concerned 'with not only political struggles around data collection and its deployments, but how data is generative of new forms of power relations and politics at different and interconnected scales'(Ruppert et al, p.2).One clear thread in data politics is openness, with notions of open societies and open environments sharing a dependency on access to information; the former for informed participation and the latter for data control. These affordances of data are often viewed as being in tension in government openness and individual privacy, where the data is neutral but its uses are political. Mindful that 'raw data is an oxymoron' (Gitelman, 2013) – that data, like archives and records, are never neutral - this survey takes a high level look at data protection and data reuse policy and activism in the UK in the context of open data to identify where and how privacy and openness connect.

The social and political significance of this topic cannot be overstated, as the recent difficulties of the Open Society Foundations (OSF) show. OSF's work on information and digital rights seeks to 'curb overly broad and unaccountable surveillance, make major internet platforms more accountable to the public, and expose and challenge problems caused by algorithmic decision-making…'(Open Society Foundations, n.d.). Post-2011, OSF has been banned in Russia, shut down in Pakistan and driven out of Hungary and Turkey under government pressure and interference, demonstrating that information activism around privacy and access is perceived by some governments as a threat to their hegemony.

The political will behind the open data movement in the United Kingdom was chiefly commercially motivated, with the Cameron government citing innovation as a driver for the foundation of the Open Data Institute in 2011. In the same year, the UK co-founded the Open Government Partnership, an international organisation seeking to promote transparency and public participation in government. 2011, then, marks an important moment in Britain's open data movement, and our study of the literature therefore begins at this date. This literature review will focus on British sources, rather than European sources more generally. While this is primarily due to the limits of space, we recognise that

we are writing as Britain moves towards Brexit, and the benefits of European work on privacy, and other areas of information policy and human rights, that have been experienced in Britain may soon fall subject to the agendas of domestic political actors. With this in mind, we have looked at privacy 'from above', in the sense of laws, regulations and policies instigated by UK central government, and privacy 'from below', in the sense of information activism from British civil society. The chapter draws on the *Open Government Data Literature Review* (EU02) by James Lowry and Anna Sexton's work on the *Recordkeeping, Open Government and Data Privacy Literature Review* (EU21).

Privacy from Above

According to Bates, the open government data (OGD) agenda in the UK rests on the notion that non-personal data 'produced by public bodies should be opened for all to re-use, free of charge, and without discrimination' (Bates, 2014, p.389). Since the election of the coalition Government in 2010 in the UK, there has been a marked political focus on the potential to generate income from opening up public sector information, in part as a reaction to the global financial downturn and the introduction of austerity measures. This included, in 2011, a £10 million pledge by the Government, to be delivered over five years, for the establishment of the Open Data Initiative. The Chancellor of the Exchequer gave this pledge in his Autumn 2011 statement to parliament with justifications that were tied into catalysing 'new markets and innovative products and services'. In a speech in December 2011, the prime minister employed a subtly different rhetoric which spoke to notions of collective action, solidarity and citizen participation. Despite this glaze, it is clear from the Chancellor's earlier positioning that the UK's OGD agenda is as much connected to what Keen et al describe as 'practical neo-liberalism' as it is to participatory citizenship. In 'practical neo-liberalism' it is the relationship between the State and the private sector that takes precedence, and which is ultimately reinforced (Keen et al, 2013, p.229).

Despite central government drives to open up data as a reusable asset, in reality there is a series of stumbling blocks to any realisation of exploiting citizen-state data held in publicly maintained systems through open data initiatives. There are fundamental questions on usability and usefulness that are linked to the quality of the underlying records from which the data to be opened is drawn, as well as the extent to which data can maintain its authenticity and integrity during any process of extraction (Lowry, 2014). Keen et al contend that datasets generated from public sector records are generally both incomplete and inaccurate. There is also a fundamental problem with any assumption that the State has the right to decide the 'ifs, how, and when' in relation to opening up data derived from citizen interaction with state services. The assumption that they *do* have this right runs counter to growing trends of public feeling in the UK that emphasise citizen rights to control access to their data (Keen et al, 2013, p.229).

To be published as wholly open data without restrictions, datasets must be anonymised (de-identified). Anonymisation is a process that 'prevents all parties from singling out an individual in a dataset, from linking two records within a dataset (or between two separate datasets) and from inferring any information in such a dataset' (Article 29 Working Party, 2007). It might be assumed on the surface that this then solves the problem of citizen control: if individuals are no longer identifiable, then the data is surely no longer 'theirs'. This is an assumption that is reinforced in data protection law, as data protection is only applicable to *identifiable* data, with no data subject rights over data that has been de-identified. Yet the simple acceptance that anonymisation (de-identification) solves any issues that the citizen might have with the creation of open datasets that are derived from their interaction with the

state is problematic. It is simply not possible to make anonymity an intrinsic property within an individual level dataset because identifiability is context dependent and depends on what other data is available to the individual seeking to make an identification. Data derived from citizen-state interaction is in fact always inextricably connected to the participating citizen and the community from which they derive, and therefore those that have participated in the creation of the data retain a deeply vested interest in its ongoing use. However, the notion that they should have a say in supposedly anonymised open data reuse is not currently supported in law, policy or regulation around open data.

Controlling the levels of detail (the granularity) in the data is one relatively effective way to manage the risk of identification, but the less detailed the data, the less commercially valuable, or otherwise useful (i.e. to researchers), the dataset becomes. Keen et al suggest that it is 'not clear' if or how 'the circle of data protection and commercially valuable publication can be squared' (Keen et al, 2013, p.238). Proponents of the OGD agenda often frame open data as a direct benefit for the citizen. As taxpayers, citizens should have access to data relating to the services that they help to pay for, to re-use with as few restrictions as possible. Yet clearly, as the discussion above begins to tease out, positing open data as a 'citizen's right' can be in direct tension with the protection of the citizen's more fundamental rights, freedoms and interests. For these reasons alone, the aspirations of the 'open government agenda' are contentious.

While *sharing* data may lie at the heart of the OGD agenda, from a privacy perspective, the *limitation* of sharing personal information is not only seen as positive, it is cast as a fundamental human right. However, its reach is viewed in law as 'non-absolute' and its application is therefore weighed against its functioning in society. A number of high level overlapping legal measures exist to protect privacy including privacy rights, which guarantee freedom from interference; rules of data protection, which control the processing of personal data; and duties of confidentiality, which protect against unauthorised or unreasonable breaches of confidence (Nuffield Council, 2014). Across these legal measures a balance is sought between privacy and public interest, including where the boundary of privacy lies in relation to other fundamental human rights and interests.

An examination of the complexity of how these balances have been translated into the legal framework around data sharing can be opened up through a consideration of practices around more granular, person-level data generated through citizen-state interaction. This kind of data is often made accessible by government departments not as fully open data but as pseudonymised data. In these instances, artificial identifiers replace personal identifiers in a way that still enables the tracking of an individual across linked datasets. Pseudonymised data of this kind does fall under the Data Protection Act, however the procedural mechanisms and possibilities surrounding its reuse is also controlled by an overlapping web of more specific and context dependent laws and regulations. In exploring the extent to which the consent of the data subject plays a role in the release and reuse of government administrative data, Sexton et al (2018) examined processes for data release by UK government departments in relation to health, education, transport and energy. This study revealed that while the General Data Protection Regulation and related UK Data Protection Act uphold the consent of the data subject as the primary procedural mechanism underpinning the fair and lawful processing of personal data, it is by no means the only permissible mechanism for authorising data release. In place of explicit consent, it is possible for researchers and data providers to rely on alternative legal gateways, on privacy notices, and on offering opt-outs to data subjects.

The primary influencing factor on the centrality (or otherwise) of consent of the data subject is the specificities of the legislative framework governing the collection and processing of the data. For example, school data collection is made mandatory under specific legislation and regulation including the Education Act and the Children's Act. In line with provisions made in this legislation, collection and reuse of school data relies on the display of privacy notices in schools and on local authority websites, with only limited opt-out arrangements. School data is therefore routinely aggregated into a large dataset known as the National Pupil Dataset, which is made available by the Department for Education in varying degrees of granularity and identifiability. While scrutiny by a panel, and various other safeguards are in place to control the release and reuse of this dataset, the consent of pupils or parents is not a component in the governance model.

In understanding the legislative framework underpinning the open government agenda, it is also necessary to highlight the impact of the EU's Re-use of Public Sector Information Directive 2013/37/EU, which has been transposed, in the English context, into the Re-Use of Public Sector Information Regulations 2015. For the purposes of the Regulations, public sector information is defined as any information (content) whatever its medium (form) – including print, digital or electronic, and sound recordings – produced, held or disseminated by a public sector body, with a public body defined as being both central and local government or any other public body including cultural sector bodies.

In the UK context, The National Archives is the principal body offering guidance on the implementation of the regulations, which includes best practice on standard licences, datasets and charging for re-use. Documents holding personal data are not excluded from re-use under regulations, but such reuse has to be in accordance with the EU and national rules on the processing of personal data. This means that data may be derived, for example, from medical records or from patient interactions with services and made available for re-use as long as disclosure risk is effectively safeguarded through robust anonymisation.

As explored by Janssen (2011), in January 2010 the web portal data.gov.uk was launched to provide a single access point to open data varying from information about school locations, house prices, and tax receipts, to commuting statistics and public transport routes and timetables. The UK push towards open data and re-use has also finally been cemented by the introduction of a 'right to data' by the Protection of Freedoms Bill, amending the Freedom of Information Act, 2000, to include an obligation for public bodies to publish datasets available for re-use in a re-usable format either in response to a request or through their publication schemes.

The UK PSI Regulations are designed to enforce mandatory re-use permission for all information produced, held or disseminated within the course of a public task unless re-use is otherwise restricted or excluded (with some exceptions for the cultural sector). The aim is to ensure that as much public sector information is made available for reuse as possible under transparent and unrestrictive conditions and at marginal cost. To ensure compliance public bodies must, among other things, be proactively aiming to make information and metadata open and machine readable, under open licenses and for free where possible.

As noted by Janssen, in its 2010 Digital Agenda, the European Commission 'emphasised the importance of the availability of public sector data for stimulating markets for online content' (2011, p.446). In its Introductory Guide to the Amended PSI Directive, the National Archives UK also connects this ethos of economic benefits and employment opportunities across Europe by stating that

‘Re-use of public sector information stimulates the development of innovative new information products and services in the UK and across Europe, thus boosting the information industry’ (The National Archives, 2019). Janssen describes the PSI directive ‘as a direct result of the European Commission's concern about the underdevelopment of the European information market and its inability to compete with the United States’, a concern fuelled by the Commission’s view that federal level data was widely available across the US at low cost (2011, p.447). The purpose of the Directive was therefore two fold: ‘on the one hand, enabling the availability of public sector data to third parties at low prices and unrestrictive conditions, and on the other hand, ensuring a level playing field between public bodies that operate in the information market in competition with the private information industry’ (Janseen, 2011, p.447). However, in relation to exploitation of commercial value, the push towards openness at no (or marginal) cost effectively prevents the public sector itself from profiting from the information industry that it feeds. The promotion of openness necessarily entails a loss of control, and the negative implications are therefore felt by those who profited from the control mechanisms that were originally in place. The PSI Directive’s attempts to ‘level the playing field’ are actually designed to ensure that the private sector is not at a disadvantage to the public sector. Janssen summarises how the directive is in fact designed to prevent public sector bodies from locking ‘their data in exclusive deals with one private company or to maximise short term revenues by abusing their market power as monopolists’ (2011, p.448). The directive is also designed to mitigate any ‘risk that public sector bodies fund (part of) their market activities with public tax money in order to keep their market prices low, and in this way use cross-subsidisation to distort the market’. This is achieved through the insistence that the re-use of public sector information has to be non-discriminatory for comparable categories of re-use’.(Janssen, 2011, p.448). The underpinnings of the regulations are therefore more in favour of enabling the private sector to profit from public sector information, than protecting the public sector’s ability to monetise the information it holds. Mustill also explores the processes of capital accumulation associated with the release of open data and interrogates how open government data has become a ‘means by which public wealth can be transferred to private capital’ through what he describes as ‘non rivalrous enclosure’ where the guise of openness obfuscates the reality that the usability of the data is ‘restricted at any given time to those in possession of the necessary tools’ (2019, p.18).

This reinforces the point that ‘openness’ is not wholly ‘good’ for all sections of society, all of the time. It is argued by those who see OGD as a form of neo-liberalism that the private sector in fact stands to benefit over and above both the citizen and the public sector. In regards to the citizen, commercial exploitation raises strongly felt privacy and security concerns, as well as concerns over unfair treatment realised through biases in how data is both created and then reused. Can either the private sector (or indeed the public sector) be trusted to act in the citizen’s best interest? And for all citizens fairly, without marginalisations occurring? Rumours that the insurance industry may have used data released by the HSCIC’s predecessor body to fix the costs of insurance provides plenty of fodder for the notion that the citizen, the public sector and the private sector often have competing interests, with OGD placing the balance most firmly in the hands of the latter.

Coming back to the question of how privacy and openness interconnect in national legislation, regulation and policy; the rules on re-use of public sector information must be applied in full compliance with data protection legislation and this is made explicit in the text of the regulation. However, a 2018 impact assessment commissioned by the European Commission on the implementation of the EU PSI Directive by member states draws out that while the importance of compliance with GDPR and national

data protection legislation as a precedent over the re-use of information is well understood, there has been uncertainty across member states on facilitating re-use while ensuring data protection compliance in cases where public registers or datasets also contain personal data (e.g. car registration databases or hospital records). Significantly, the impact assessment reveals that concerns were raised by member state representatives around the 'suitability of techniques that can be used for anonymization or ways by which purpose limitation can be ensured' (European Commission, 2018). This highlights how, despite the drive towards open data, and the introduction of legislation to both force and support data sharing, the fundamental tensions between privacy and openness are still seen by implementers as difficult to resolve.

Privacy from Below

In this setting, where law, regulation and policy, together with technical and procedural issues of data management and curation, continue to be contested, privacy activism within UK civil society is energetic. This activism is led by a handful of organisations, chiefly Privacy International, Big Brother Watch, Liberty, and the Open Rights Group. Though state funded, the Open Data Institute has also supported privacy activism, providing a base for the UK's OGP civil society forum, fostering research and leading projects on topics such as data ethics, policy design and standardisation. Privacy figures in the ODI's data ethics work, including its Data Ethics Canvas (Open Data Institute, 2019) , which is a tool designed to help users design and run data projects that are ethical and have positive impacts. Although the term 'privacy' does not feature in the Canvas itself, the supporting documentation shows that ODI evolved its tool with reference to pre-existing data ethics frameworks including privacy frameworks. The following summary of civil society priorities around privacy illuminates the range of ways in which privacy is threatened in the open environment, but also shows that much privacy activism is not directly concerned with privacy in public sector information reuse as envisaged by government advocates of OGD. Instead, covert data collection and opaque practices with closed and shared data appear to be the primary concerns.

Privacy International (PI) is a UK registered charity that exists to 'promote the human right of privacy throughout the world' (Privacy International, n.d.). It does this through advocacy and policy work, legal action, technical analysis, investigation and research and by fostering an 'international privacy movement'. Its current campaigns focus on a range of topics including advertising technologies, secret global surveillance networks, critiquing identity systems, monitoring the role of the Internet of Things in court cases, and protecting migrants at borders. PI produces a range of resources, including 'long reads', case studies, 'explainers' (illustrated FAQs), advocacy documents and videos. PI has also produced numerous reports, some of which focus on particular countries or regions, others of which have a wider scope. Reports of the latter type include *The Global Surveillance Industry*, which traces the history of the development of surveillance technologies and looks at their international trade (Privacy International, 2016). In 2018, with the International Committee of the Red Cross, PI published *The Humanitarian Metadata Problem - Doing No Harm in the Digital Era*, which is intended to inform humanitarian workers about the data risks associated with certain technologies, and discusses the 'do no harm' principle in this context (Privacy International and the International Committee of the Red Cross, 2018). Also in 2018, PI published *Digital stop and search: how the UK police can secretly download everything from your mobile phone*, which responds to the potentially unlawful use of mobile phone extraction tools by UK police, and argues for changes such as an independent review of the practice and the development of new official guidance (Privacy International, 2018). PI also participated in the UK's OGP civil society forum that drafted commitments for the national action plan.

Big Brother Watch describes itself as a 'cross–party, non-party, independent non-profit organisation leading the protection of privacy and civil liberties in the UK' (Big Brother Watch, 2019:2). Its

campaigns include Face Off, which opposes the use of facial recognition technology in public surveillance, and Free Speech Online, which is concerned with the haphazard censorship of online speech by social media companies, as well as the possibility of government regulations to control speech over social media. Much of Big Brother Watch's online content is about mobilising the public, but it also publishes briefing notes, blogs, opinion pieces and factsheets. The organisation has produced parliamentary briefings and evidence, submissions and letters, which it makes available on its website. Its research reports cover topics such as classroom management software, body-worn cameras, and police access to digital evidence. Its most recent report, *Digital Strip Searches: The Police's Data Investigations of Victims*, discusses the seizure of digital information from crime victims' phones, police use of artificial intelligence to analyse the data, and these practices in relation to current laws and the legal concept of consent (Big Brother Watch, 2019:1). Importantly, the report surfaces victims' experiences, and includes a section written by the director of the Centre for Women's Justice. Big Brother Watch's 2018 State of Surveillance report covers a range of current issues, including the effect of surveillance on the right to freedom of assembly, blacklisting practices, the impact of state surveillance on investigative journalism, accountability in school surveillance and data-sharing and immigration enforcement (Big Brother Watch, 2018).

Liberty is an independent membership organisation that was established in 1934 to help defend human rights in the UK (Liberty, n.d.). The membership consists of campaigners, lawyers and policy experts who work to defend rights through public campaigning, test case litigation, Parliamentary work, policy analysis, information sharing and the provision of free legal advice. Of its seven current campaigns, four are explicitly about privacy, with campaigns around facial recognition software in public places, data sharing in immigration enforcement, mass surveillance and police spying. Though Liberty does produce reports, much of its written output is in the form of written evidence and policy briefings. In relation to information issues, these briefings cover the use of algorithms in the justice system, official secrecy and freedom of expression in universities, etc.

The Open Rights Group (ORG) is a UK-wide campaigning organisation with two stated aims: to challenge 1) threats to 'privacy by both the government through the surveillance of our personal communications and private companies, who use our personal data to increase their profits' and 2) threats to 'free speech through the criminalisation of online speech, online censorship and restrictive copyright laws' (Open Rights Group, n.d.). The group's current campaigns related to privacy target the hoarding of personal data by political parties for the purposes of targeted advertising, involve GDPR complaints about adtech, push back on age verification technologies on the basis that they breach rights to privacy, and consider the implications of Brexit for privacy. The ORG claims several legal victories in its efforts to push back on state surveillance, including a successful challenge (with Privacy International and others) in the European Court of Human Rights to the UK's mass surveillance programmes exposed by the Snowden leaks, and their involvement in the UK Court of Appeal challenge to the 'Snooper's Charter' provisions found in the Data Retention and Investigatory Powers Act 2014. ORG also develops tools to support the right to privacy, most notably the Data Rights Finder, developed with the Information Commissioner's Office and Projects by If, which allows users to access jargon-free explanations of organisations' privacy policies.

ORG works on a number of privacy policy issues, but of most relevance to this review, ORG is the only civil society actor in this space to focus directly, rather than incidentally, on open data. It finds a number of problems with the UK government's move to 'open by default', seeing privacy as the most contentious 'especially in the area of healthcare, where pharmaceutical companies want access to patient health data to aid research. Claims that such personal and sensitive data can be successfully "anonymised" ignore evidence of the very real threats that individual records can be reidentified' (Maguire, 2012). ORG states that it works on open data through the OGP and groups across Europe, and has had three initiatives relevant to the scope of this survey. Firstly, it worked to against government plans to privatise aspects of data creation and management in the areas of weather, land and mapping as part of the formation of a Public Data Corporation, which worked under several names before being folded into a board within the Department for Business, Innovation and Skills. Secondly, ORG works to identify privacy risks around the commercialisation of "anonymised" public

services data. Finally, ORG has been concerned with historic data and in particular opening it to the family history 'sector' in a programme called 'Open Genealogy'(Open Rights Group, n.d.).

With this important exception, this survey has shown that in the activist space, there is very little overt connection between open data and privacy. Instead, there is a clear concern for data gathering (particularly in relation to covert techniques) and cross-agency data sharing. The involvement of organisations like Privacy International and the ORG in the UK's Open Government Partnership civil society forum shows that the relevant actors are alert to the privacy issues connected with open data and open government more broadly, but, outside of ORG's work, the problems and corrective efforts appear to concern data collection and opaque sharing practices, rather than publication and redaction. Gray has suggested that an

> …ambitious politics of data would have to move beyond programmes to make data public or keep data private through various attendant technical, policy and legal systems that facilitate or inhibit the flows of data in society... This would entail opening up spaces for democratic deliberation and social participation around the creation of data and around processes of datafication (Gray, 2016).

Arguably this is the direction in which civil society actors are trying to drive the privacy regime, so that individual agency is not necessarily focused on preventing dataveillance, but is instead fully informed and empowered to co-create (or not) data for civic purposes.

Conclusion

The InterPARES research in this space and the relevant literature since 2011 demonstrate the complex and contentious interactions of the privacy and openness agendas in the UK. Law, regulation and policy behind OGD have been driven by neo-liberal aspirations to data-fuelled economic growth as well as by concerns for government transparency and participatory governance. Privacy in this context is not simply diametrically opposed to government openness; the two are entangled together, together with private sector interests, technological developments and community concerns. Yet, with the notable exception of ORG, UK privacy activists are rarely directly concerned with open government data, and more often concerned with data gathering practices and sharing across government bodies and private sector actors.

It is interesting to note a recent development in data activism in the United States. A 'manifest-no' has been built from a feminist standpoint perspective ultlising the power of 'no' to make a series of refusal statements on data sharing and reuse. These statements challenge the assumption that the harm associated with data practices are the same for everyone, when historic and systemic patterns of exploitation produce differential vulnerabilities for communities. The statements also highlight how current data practices are normalizing a drive to both monetize and hyper-individualize the human experience. Thus the manifest-no acts as a form of resistance to this status quo by instead centering collective forms of life as a means to exceed neoliberal logic (Cifor et al, 2019). Such ways of thinking, conceptualising and practising data are important to draw in here because they provide a means to not only question but begin to actively refuse the logic bound up in high level policy, regulation and law at the intersection of openness and privacy. This is a kind of communal statement of data politics not yet seen in the UK.

References

Article 29 Working Party. (2007). Working Document on the processing of personal data relating to health in electronic health records (EHR). https://ec.europa.eu/justice/article-29/press-material/public-consultation/ehr/2007_ehr/ms-national/dept_health_and_children_ie_en.pdf

Bates, J. (2014). The strategic importance of information policy for the contemporary neoliberal state: The case of Open Government Data in the United Kingdom. Government Information Quarterly, 31(3), 388-395. http://dx.doi.org/10.1016/j.giq.2014.02.009.

Big Brother Watch (2018) 'The State of Surveillance in 2018' https://bigbrotherwatch.org.uk/wp-content/uploads/2018/09/The-State-of-Surveillance-in-2018.pdf [accessed 3 November 2019]

Big Brother Watch (2019: 1) 'Digital Strip Searches: The Police's Data Investigations of Victims' https://bigbrotherwatch.org.uk/wp-content/uploads/2019/07/Digital-Strip-Searches-Final.pdf [accessed 4 November 2019]

Big Brother Watch (2019:2) 'Big Brother Watch's written evidence to the Joint Committee on Human Rights on The Right to Privacy (Article 8) and the Digital Revolution inquiry' https://bigbrotherwatch.org.uk/wp-content/uploads/2019/06/Big-Brother-Watch-written-evidence-to-JCHR-The-Right-to-Privacy-and-the-Digital-Revolution-Inquiry-Feb-2019-II.pdf [accessed 2 November 2019]

Cifor, M., Garcia, P., Cowan, T.L., Rault, J., Sutherland, T., Chan, A., Rode, J., Hoffmann, A.L., Salehi, N., Nakamura, L. (2019). Feminist Data Manifest-No. https://www.manifestno.com/.

European Commission, (2018). Working Document, Impact Assessment. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018SC0127&rid=4

Gitelman, Lisa (ed.) (2013) Raw Data is an Oxymoron, MIT Press.

Gray, Jonathan (2016) 'Datafication and democracy: Recalibrating digital information systems to address societal interests' https://www.ippr.org/juncture/datafication-and-democracy [accessed 29 October 2019].

Janssen, K. (2011). The influence of the PSI directive on open government data: An overview of recent developments. Government Information Quarterly, 28(4), 446-456.. https://doi.org/10.1016/j.giq.2011.01.004.

Keen, J., Calinescu, R., Paige, R. and Rooksby, J. (2013), Big data + politics = open data: The case of health care data in England. Policy & Internet, 5, 228–243. https://doi.org/10.1002/1944-2866.

Liberty (n.d.) https://www.libertyhumanrights.org.uk [accessed 26 October 2019]

Lowry, J. (2014). 'Opening Government: Open Data and Access to Information'. In Lowry, J. and Wamukoya, J. (eds.) *Integrity in Government Through Records Management* (pp.161-171). Ashgate.

Maguire, Lee (2012) 'Open Data' https://www.openrightsgroup.org/issues/opendata [accessed 24 October 2019]

Mustill, E. 2019. 'Understanding How Open Government Data is Used in Capital Accumulation: Towards a Theoretical Framework'. In Wood, S. E. Lowry. J., Lau, A. J (eds) Information/Control: Control in the Age of Post-Truth'. Special Issue. Journal of Critical library and Information Studies 2. 2. DOI: https://doi.org/10.24242/jclis.v2i2.63

Nuffield Council on Bioethics. (2014). The collection, linking and use of data in biomedical research and health care: ethical issues. https://www.nuffieldbioethics.org/publications/biological-and-health-data

Open Data Institute (2019) 'Data Ethics Canvas' https://theodi.org/article/data-ethics-canvas/ [accessed 24 October 2019]

Open Rights Group (n.d.) 'About' https://www.openrightsgroup.org/about/ [accessed 29 October 2019]

Open Society Foundations (n.d.) 'Our Work' https://www.opensocietyfoundations.org/what-we-do/themes/information-and-digital-rights [accessed 2 November 2019]

Privacy International (n.d.) 'About' https://privacyinternational.org/about [accessed 2 November 2019]

Privacy International (2016) 'The Global Surveillance Industry' https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf [accessed 8 November 2019]
Privacy International (2018) 'Digital stop and search: how the UK police can secretly download everything from your mobile phone' https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf [accessed 8 November 2019]
Privacy International and the International Committee of the Red Cross (2018) 'The Humanitarian Metadata Problem: 'Doing No Harm' in the Digital Era' https://privacyinternational.org/sites/default/files/2018-12/The%20Humanitarian%20Metadata%20Problem%20-%20Doing%20No%20Harm%20in%20the%20Digital%20Era.pdf [accessed 8 November 2019]
Ruppert, E., Isin, E., & Bigo, D. (2017). Data Politics. Big Data & Society, 4(2), 2053951717717749. https://doi.org/10.1177/2053951717717749
Sexton, A.K., Shepherd, E.J., Duke-Williams, O.W., and Eveleigh, A. (2018). The Role and Nature of Consent in Government Administrative Data. Big Data and Society, *5* (2). https://doi.org/10.1177/2053951718819560
The National Archives. 2019. Why PSI must be re-useable. https://www.nationalarchives.gov.uk/information-management/re-using-public-sector-information/about-psi/psi-must-re-usable/

CVs

Dr James Lowry is Co-Director of the Liverpool University Centre for Archive Studies. His research is concerned with information and governance, particularly in colonial, post-colonial and diasporic contexts. His current projects include *Displacements and Diasporas*, exploring the technical and theoretical problems connected with disputes and claims over displaced records. He is also collaborating with colleagues at Kings College London on the *Sudan Memory* project, to safeguard the documentary heritage of Sudan and the Sudanese diaspora, and the *Refugee Rights in Records* project based at the University of California, Los Angeles; that project seeks solutions to the informational problems experienced by displaced people. His recent publications include *Displaced Archives*, an edited collection published by Routledge in 2017.James is editor of the Routledge Studies in Archives book series. https://orcid.org/0000-0001-9970-3846

Dr Anna Sexton is a lecturer in the UCL Department of Information Studies on the MA in Archives & Records Management. She has held several practice-based roles in the recordkeeping field most recently as Head of Research at The National Archives (TNA). Her research experience includes developing participatory and community focused approaches to archives and records; documenting lived experience of mental health from a survivor perspective; using recordkeeping perspectives to examine the secondary re-use of government administrative data; examining the intersection between open data initiatives and the protection of personal information; and exploring the technical integration of XML encoding standards to develop platforms for users to view archives. She has a varied portfolio of public engagement projects including pilot work, funded by UCL's policy unit, to bring together care experienced members of the public with social workers and information professionals to co-develop a recordkeeping framework for social care records. Her current research interests include participatory and trauma informed approaches to archives and recordkeeping, as well as data equity and ethics, particularly in relation to personal health data. https://orcid.org/0000-0002-5557-2204