A Framework for Public Bodies for Managing the Secure and Appropriate Release of Open Source Data

Jane Henriksen-Bulmer
Bournemouth University
Talbot Campus
Poole
UK
http://staffprofiles.bournemouth.ac.uk/display/jhenriksenbulmer
jhenriksenbulmer@bournemouth.ac.uk

This paper outlines current research in progress for the creation of a set of privacy heuristics, incorporated into a framework for privacy preserving open source publishing of public body information. It explains how HCI may result in privacy being compromised if information is published without first considering what privacy implications such publication might have. The paper then goes on to explain the meaning of open government and open government data publishing. This is followed by a brief overview of the UK statutory landscape that any publication has to conform to. An outline is also provided of existing guidance available to public bodies, together with an explanation of the research approach and methodology utilised in conducting the research. Initial findings show that statutory constraints may get in the way of workflow and that no formal quality checks are currently in place to support open source publishing of public data in the UK.

Open Source Publishing; Open Government; Open Government Data; Privacy

1. BACKGROUND

Over the last decade or so, there has been a shift in how data is accessed, used and published. This has brought about an increase in the type and amount of data that is now publicly available, including large amounts of public data.

This paper looks at the open source publishing landscape from a public body perspective and the obstacles currently encountered by those who are involved in releasing data open source. The aim of the research is to create a framework, including a set of privacy heuristics, that will allow public bodies to publish data in a manner that manages the tension between maintaining data utility and privacy. This will then allow researchers and others to benefit from the release, whilst preserving the privacy of any individuals whose data may be included.

Historically data was collected, maintained, stored and controlled at a local level. Organisations and individuals would collect data pertaining to their business or interest and hold this in paper or electronic format. With the event of more and more automation in data management and analytics, a shift has occurred in how data is accessed, used and published. Data has become 'the new oil' and, as such, big business (Van't Spijker, 2014). The main difference arises from how data is shared and published. Data is now collected, stored, analysed and shared at a velocity and in quantities beyond imagination just a few years ago, this is often referred to as big data (Sicular, 2013).

On the face of it, the release of such data is a positive move, it enhances transparency and supports openness, particularly with public data. However, it also raises serious concerns over the privacy implications such data releases might bring. Many examples can be found in the literature of anonymised data being released, only to find that, despite this, individuals were still re-identifiable (Henriksen-Bulmer, 2015). For example, when AOL released data containing users search queries, Barbaro and Zeller were quick to expose how easy finding individuals from anonymised data could be (Barbaro et al., 2006). This shows that, the human computer interaction (HCI), and how data is interpreted and used, is unpredictable, thus introduces unforeseen privacy risks, making it

© *The Authors. Published by BISL.*

imperative that privacy has already been preserved prior to publication.

The revolution in data publishing is not limited to individuals or private organisations, public bodies are also entering the world of online presence and publishing. Increasingly, public bodies now offer access to data ranging from enabling the public to access information through web portals through to providing data open source.

In the UK, it is estimated that UK public sector information is worth 1.8 billion annually (Department for Business Innovation and Skills, 2013). This brings with it the potential for individuals and organisations to profit from analysing and/or re-using the information in ways previously unimaginable, with access to data and re-use of data being strongly encouraged by the UK government (Shakespeare, 2013). To this end, the UK Government are, in an attempt to be more transparent, implementing a strategy called 'seizing the data opportunity' which, among other things, seeks to allow open access to government datasets (Department for Business Innovation and Skills, 2013). At the time of writing this article (February 2016), there are 23,194 datasets available to freely download on the government's open data website (data.gov.uk), with more datasets being published all the time. Similarly, in the United States (US), the data.gov website boast availability of just under 195,000 datasets from 78 different government agencies (Data.gov, 2016).

Whilst a dataset might not, by itself, raise concerns over processing of personal data, a further risk arises when data mining results are combined with results from other datasets (Sweeney, 1997). These combined dataset can provide data miners with detailed insights into their customers affairs, likes and preferences, as well as potentially, their ailments, and thus, prove very valuable indeed. This gives rise to potential issues and raises questions over, for example, who has access to what personal data and what inferences can be drawn from the data. Moreover, how do data analysts use, share and/or re-use the results of their data mining efforts? Do they have permission to use and/or re-use that data and in what format?

The rest of the paper is organised as follows; section two presents an outline of the research objectives and questions. In section three, the key points of the literature review provide an overview of how HCI and privacy considerations are applicable in open source publishing. It then goes on to explain some of the terminology around public body publishing including; open government and open source publishing of public information, together with an outline of the regulatory framework currently in place in the UK that underpins the publishing of public information. This is followed by an overview of what guidance is currently available for public bodies on publishing open source.

Section four sets out the problem statement, whilst section five presents the research approach and methodology. Section six provides a short review of initial findings and section seven details the main contributions of this research.

2. RESEARCH OBJECTIVES AND QUESTIONS

The objective of this research is to investigate how public bodies can manage the potential privacy risks and security concerns that arise from HCI and open source publication with the benefits of making data publicly available whilst retaining data utility so that researchers and others can benefit from the release.

The question the PhD will seek to answer is:

How do public bodies manage the tension between allowing access to information whilst retaining competitive advantage and user confidentiality?

3. KEY POINTS OF LITERATURE REVIEW

The literature review will look at the open source publishing landscape from a variety of perspectives including; privacy and HCI; open government; open government data; statutory requirements in the UK; privacy; and any existing guidance available to aid public bodies in publication. A brief overview of each perspective has been provided in this paper.

3.1. Privacy

Privacy in relation to HCI is most often thought about in terms of how rules and constraints within the software can be used to preserve privacy. This implies that privacy is a static subject that can be regulating by simply setting some rules and boundaries around the information. In reality; regulating privacy is "a dynamic, dialectic, negotiate affair", that may be destabilised by technology Palen and Dourish (2003).

Privacy encompasses all aspects of our lives and most people expect that their privacy will be preserved when dealing with public body organisations, some might say that privacy is "a fundamental right to our democracy" (Janssen and van den Hoven, 2015). To this end, the law provides some privacy protection, through data protection legislation, in the UK, the Data Protection Act 1998 (DPA). These regulations however, protect privacy in regard to how data is processed or shared by those

who process it. This means that data protection is viewed and enforced from the perspective of what the data processor (i.e. the person who processes the information) can or cannot do with the data, rather than from the perspective of the individual about whom the information pertains (the data subject).

From a corporate perspective, privacy in protected through fair information practices (FIP) which are underpinned by regulatory constraints such as the DPA in the UK (and similar regulations around the world). FIP in this context means ensuring that individuals (data subjects) are given notice of any intended disclosure and being asked to consent to data use (Bamberger and Mulligan (2015).

Despite this protection, the reality is that, at the point of human computer interaction, such as when users access the information or services, the statutory protection does not hold. For example, a recent study by Borghi et al. (2013), showed that EU compliant informed consent is not obtained in the majority of cases, with only a third of websites in the UK found to respect the privacy of the data subject. There are also a number of other considerations that will need to be taken into account when considering how privacy can best be incorporated into the open source publishing process including context, tolerance and coverage.

Privacy needs to be placed in the right context, that is to say, each dataset will need to be considered in light of the likely HCI and its surrounding circumstances. It is not just the nature or value of the information, it is also the context of the data release, who it is to be released to and the ethical, moral and political implications such release might bring and that will need to be considered (Nissenbaum, 2010). Early research conducted in the US proved that it was possible to uniquely re-identify 97 percent of voters in Cambridge, Massachusetts from publicly available datasets by combining data from multiple sources (Sweeney, 1997). Since then, research shows that data linking is the most common method used in re-identification (Henriksen-Bulmer (2015)).

Further, different Countries will have different tolerance levels for privacy (Janssen and van den Hoven, 2015) as indeed, will different users of that information once it has been published. Therefore, there is no guarantee that those who download the information will process the data in accordance with any constraints that may have been placed on the data or that the information will not be used for re-identification or data matching purposes.

Moreover, any data that is published open source will be available globally and thus, any re-use purpose may span multiple countries. This means that any privacy implications will need to be considered not just at local or national level, but globally. Therefore, each dataset will need to be evaluated for privacy implications in light of these concerns prior to publication.

3.2. Open Government

The main drivers behind open government vary between countries, but for most the concept incorporates accountability, transparency, participation, collaboration and, of course, access to information (United Nations, 2013); (Abu-Shanab, 2015). Underlying this are a number of drivers including encouraging economic growth through providing opportunities for the public, researchers and organisations to re-use the information published. Worldwide, 69 Countries have joined the open government partnership, committing to implementing open government reform so far (Open Government Partnership, 2016b).

The concept of Open Government in its current format became popular after President Obama released a Memorandum for the Heads of Executive Departments and Agencies in March 2009, and since then other countries have also adopted the phrase, creating their own Open Government agendas including Australia, UK, New Zealand, Russia, China and the European Union (EC) (Wirtz and Birkmeyer, 2015). That is not to say that none of these countries had transparency or data access agendas prior to this date, that may well have been the case as indeed it was in the UK.

There has been a number of papers written by scholars in recent years relating to open government covering; transparency (CONROY and SCASSA, 2015); (Harrisona and Djoko Sigit, 2014); policy (Carrasco and Sobrepere, 2015); democracy (Hellberg and Hedström, 2015); and citizen participation (Potra et al., 2015). Further, much research has been conducted into open government and data.

3.3. Open Government data

Open Government is seen by some as an extension or subset of e-government (Attard et al., 2015). However, whilst it may be true that open government can be seen as the progression of e-government, e-government was about inter-agency and inter-department sharing of data and access to services, whereas open government is about, among other things, access to information and thus, the two are quite distinct from each other.

Access to information has become an integral part of open government, providing the means of facilitating access to and the re-use of public body information,

and enabling collaboration with citizens, in the hope that this will encourage wider participation and convey government's commitment to transparency (Goda, 2011). Moreover, as citzens pay for public services, it has been argued that such access to information should be made available free and open source (Shakespeare, 2013); (Fishenden and Thompson, 2013).

To this end, many governments have embraced the open source publishing concept and started making data available to freely download from data.country sites such as the data.gov site in the US and the data.gov.uk site in the UK. Across the world there are, according to the Open Knowledge Foundation (a UK not for profit agency), currently 122 countries that provide some degree of public body data open source (up from 97 countries in 2014) (Open Knowledge, 2016). Thus, it is clear that the open public data movement is going global and appears to be continuing to grow.

What is not clear, is whether these portals are meeting the open government objectives of accountability, transparency, participation and collaboration. A recent survey of seven prominent data.country websites found that, whilst these support the perception of participation and transparency, there is no consistency in data format, availability or how comprehensive, timely or accurate the published information is, nor are there any consistent quality checks carried out on the data. Rather, the portals merely function as "data repositories" with little evidence that the open government objectives of transparency and accountability are actually being achieved (Lourenço, 2015). Furthermore, studies on citizen participation also suggest that public participation and re-usability of the data published is also questionable (Janssen et al., 2012); (Hellberg and Hedström, 2015); (Attard et al., 2015).

3.4. The UK Regulatory Framework

In the UK, the regulatory framework consists of a combination of UK legislation and EU regulations enacted into UK law.

The regulations pertinent to the release of information are; the Data Protection Act 1998 (DPA); the Freedom of Information Act 2000 (FOI); The Re-Use of Public Sector Information Regulations 2015 (ROPSIR); the Environmental Information Regulations 2004 and the Infrastructure for Spatial Information in the European Community regulations 2012 (INSPIRE).

The DPA applies to any personal information and controls the use, maintenance, storing, publishing and sharing of data containing personal information. It also enables individuals to obtain details of any personal information a public authority holds about them upon request.

FOI concerns access to information held by a public body with some exceptions. Anyone can make a request for information under FOI. Furthermore, FOI also places an obligation on public bodies to implement a publication scheme under which public bodies are required to proactively publish a range of data including expenditure, policies, procedures and how decisions are made (section 19 (Information Commissioners Office, 2015). In 2012 the FOI publishing scheme was extended to also make any information released through a FOI request available for re-use (s. 11(1)(a), Protection of Freedoms Act 2012). The act requires that this publication scheme be created and approved by the Information Commissioners Office (ICO) (s. 19).

ROPSIR places an obligation on public bodies to publish information and make this available for re-use for alternative purposes. Public bodies are not obliged to adapt any dataset or extract from it in order to make it available for re-use (section 6). They are however, expected to make the full dataset, including its metadata, available in machine readable and open format "as far as is reasonably practicable" (section 11). Moreover, they may impose license conditions on the re-use, so long as this does not unnecessarily restrict how the information is re-used (section 12) and is non-discriminatory (section 13).

The Environmental Information Regulations 2004 places a duty on public bodies to make environmental information available on request; and, INSPIRE obliges public bodies to publish geographical data concerning the environment open source.

3.5. Existing guidance on Publishing Data Open Source

There are a number of guidelines that have been produced to aid government bodies in publishing data open source. However, most only provide high level guidance. For example, the Open Government Partnership link to a number of existing open data standards and open data guidelines in their open government data section (Open Government Partnership, 2016a), such as the 10 principles of open government data developed by the Open Government Working Group (Open Government Working Group, 2007) and updated by Sunlight Foundation in 2010 (Sunlight Foundation, 2010). The original 8 principles state that, to be considered open, the data published should be: Complete; Primary; Timely; Accessible; Machine Processable; Non-discriminatory; Non-proprietary and License free.

Another example, is the United Nations (UN) Guidelines on open government data for citizen engagement, produced for open government programmes and aimed primarily at transparency and public engagement, yet there is a small section on open access to information included. These refer to the following principles for open data which, they recommend public bodies should publish in publishing data open source (United Nations, 2013):

- Harmonise open data publishing policy with existing regulatory frameworks;
- Make the raw (or primary) data available, discoverable and downloadable in open source and machine readable format;
- Rate the data published following Tim Berners-Lee 5 Star (5*) scheme for linked open data (Berners-Lee, 2006).

In the UK, a series of guidelines also exist, aimed primarily at the regulatory obligations that public bodies must adhere to. Some of these guidelines are quite comprehensive, e.g. ICO have produced a series of FOI publication scheme guidance notes which provides quite detailed information on the types of information that should be published, how this should be classed and the types of information that may fall under each class (Information Commissioners Office, 2016). The guidance does not however, provide any guidance on process or selecting or preparing the information for publication.

In other areas the regulations themselves provide very detailed and prescriptive technical guidelines including data specifications requirements. For example, INSPIRE regulations require EU countries to collaborate and make spatial (mapping) data available at local, regional, national and international level. The regulations provide publishers with detailed technical specifications on required data format and standards, e.g. the INSPIRE annexes (European Commission, 2014). However, in other areas, particularly those involving publishing data open source, the guidance provide little detail on technical requirements or implementation strategies.

Thus, whilst there is a number of guidance documents available, none are comprehensive, nor do they explain or suggest what steps public bodies should undertake to determine suitability or prepare the information for publication.

4. PROBLEM STATEMENT

Releasing information increases transparency, availability and access to information which in turn encourages entrepreneurship and innovative new uses for the data. For example, businesses may use the data for market research, consumer tracking and business analytics, whilst individuals and entrepreneurs may use the data for information gathering, research and new business ventures (Kimble and Milolidakis, 2015); (Daley, 2016).

The flip side of these benefits however, are that security and privacy may be compromised as a result. Examples of privacy and security breaches is regularly highlighted in the news with the press quick to pick up any juicy scandals, whether this is from published or otherwise obtained data (Farrell, 2015).

Once data has been released it is very difficult, if not impossible, to retract. Thus, ensuring the data released is secure and that privacy is preserved prior to HCI taking place (download) is paramount. From the perspective of a public body, this is perhaps more important as any breach of data security or privacy is likely to result in loss of public trust and confidence, a core value of public service provision.

5. RESEARCH APPROACH AND METHODOLOGY

The methodology to be followed will be in three phases.

In phase one, a detailed literature review to identify existing studies covering the release of open source data will be carried out. This will be followed by a series of contextual interviews with key stakeholders involved in open source publishing.

To ensure broad coverage from within the public sector, interviews will be held with key stakeholders from three different public sector groups; local authorities, universities and the police to harvest different perspectives on how each sector currently approach the release of open source data. Furthermore, two different aspects of public sector open source publishing within each group will also be explored to determine what existing processes are in place and whether these processes differ either between agencies and/or internally between departments.

The information gathered will be analysed and coded using Corbin and Strauss (2008) grounded theory framework, to create a model of pertinent concepts. From this a hypotheses for a set of privacy heuristics will be developed, that will be suitable for incorporating into a open source

publishing framework. Simultaneously, the process data collected will be used to create a set of process maps, mapping the current publishing processes within each department/public sector body. These two sets of data will then be compared and consolidated to create a consolidated series of privacy heuristics for the framework.

Phase two will involve verifying and validating the privacy heuristics created in phase one through a series of surveys, contextual interviews and workshops or focus groups designed to discuss and evaluate the proposed privacy heuristics.

To assist with this and to aid validation, personas will be created from the grounded theory model, that stimulate realistic scenarios depicting how privacy may be compromised when publishing data open source. These personas will then be used as an additional tool to encourage wider discussion and help ”kickstart analysis” within the workshops, thus validating the model and helping to identify where amendments need to be made Faily and Fléchais (2010).

In phase three, the data gathered will again be coded and analysed following Corbin & Strauss (2008) methodology, to generate an outline set of requirements that will, together with the privacy heuristics, form the basis for the framework. From this, a set of guidelines will be produced that can be applied universally across all public bodies for the safe and secure release of open data. These guidelines will be validated through a series of case studies asking participants from previous phases to apply the proposed framework in practice. This will facilitate a thorough evaluation returning to the original sample groups to harvest feedback and criticism of the framework.

6. INITIAL RESULTS

Having conducted some contextual interviews with local authorities in the UK, initial findings support the fact that public bodies have little or no guidance in regards to open source publishing. As a result, some feel they are embark on this journey individually, with multiple approaches adopted. Indications are that a consistent approach and streamline guidance on how to approach this would be useful and welcomed by practitioners.

The findings also suggests that legislation may get in the way of workflow in the area of open source publishing. For example, FOI prescribes that details of every expenditure incurred in excess of 500 pounds is to be published as part of LA publication scheme. ROPSIR requires LAs to publish the raw dataset, but they are not obliged to modify the underlying information to comply with a request for re-use (ROPSIR s. 11). The research showed that financial officers make notes in the original dataset sometimes containing sensitive detail. This means that publication officers cannot publish the data in it’s ’raw’ format in accordance with ROPSIR, they must process the data to remove any such notations. Thus, in view of the additional workload required to ensure compliance, there is a real chance that statutory requirements may not be adhered to as to do so will impede workflow.

Further, quality checks are not incorporated into the publication of public data as standard. Research showed that currently, when public authorities submit data to the data.gov.uk site for publication, there are no specified quality checks that must be carried out prior to publication, nor does the portal itself conduct any quality and/or privacy checks on any data uploaded prior to publication.

7. MAIN CONTRIBUTIONS

A framework for managing the secure and appropriate release of public body information will enable public bodies to publish data open source, safely and securely, whist preserving privacy. Once adopted, the framework will provide practitioners with consistent advise and guidance, where previously they had none or only, at best, ad-hoc or high level guidance. At the same time, users confidence will increase as they will be able to download same format data from multiple locations and public bodies, knowing practitioners have adhered to the same heuristics and guidelines in preparing the data for publication.

The proposed privacy heuristics within this framework will be detailed enough to provide proper direction on how privacy preservation can be achieved, whilst retaining data utility so that published data can still be purposely re-used for alternative purposes.

Further, the research will provide a detailed insight into current publishing practices that can be used to inform future work. For example, this may form part of a collaborative research effort that may look into other areas such as the technical challenges and/or the legal and policy perspectives. Another possible extension of this will be to look at how the final framework and privacy heuristics may be expanded to provide direction to public agencies globally on how best to publish information open source. This would need to take into account international differences in the data, the law and attitudes. However, it could aid and encourage better privacy preserving open source publishing of information globally.

REFERENCES

Abu-Shanab, E. A. (2015). Reengineering the open government concept: An empirical support for a proposed model. *Government Information Quarterly*, 32(4):453 – 463.

Attard, J., Orlandi, F., Scerri, S., and Auer, S. (2015). A systematic review of open government data initiatives. *Government Information Quarterly*, 32(4):399 – 418.

Bamberger, K. A. and Mulligan, D. K. (2015). *Privacy on the Ground: Driving Corporate Behaviour in the United States and Europe*. the MIT Press: Mssachusetts Institute of Technology, London: England.

Barbaro, M., Zeller, T., and contributed reporting for this article Hansell, S. (2006). A face is exposed for aol searcher no. 4417749.

Berners-Lee, T. (2006). 5* open data.

Borghi, M., Ferretti, F., and Karapapa, S. (2013). Online data processing consent under eu law: A theoretical framework and empirical evidence from the uk [article]. *International Journal of Law and Information Technology*, 21(2):109.

Carrasco, C. and Sobrepere, X. (2015). Open government data: An assessment of the spanish municipal situation. *Social Science Computer Review*, 33(5):631 – 644.

CONROY, A. and SCASSA, T. (2015). Promoting transparency while protecting privacy in open government in canada. *Alberta Law Review*, 53(1):175 – 206.

Corbin, J. M. and Strauss, A. L. (2008). *Basics of qualitative research : techniques and procedures for developing grounded theory.* Los Angeles, Calif. ; London : SAGE, c2008.

Daley, J. (2016). Driven by data. *Entrepreneur*, 44(1):133 – 139.

Data.gov (2016). Data.gov: the home of the u.s. government's open data.

Department for Business Innovation and Skills (2013). Seizing the data opportunity: A strategy for uk data capability.

European Commission (2014). Inspire: Infrastructure for spatial information in the european community: Data specifications.

Faily, S. and Fléchais, I. (2010). Barry is not the weakest link: Eliciting secure system requirements with personas. In *Proceedings of the 24th BCS Interaction Specialist Group Conference*, BCS '10, pages 124–132, Swinton, UK, UK. British Computer Society.

Farrell, S. (2015). Nearly 157,000 had data breached in talktalk cyber-attack.

Fishenden, J. and Thompson, M. (2013). Digital government, open architecture, and innovation: Why public sector it will never be the same again. *Journal of Public Administration Research & Theory*, 23(4):977.

Goda, S. (2011). Open data and open government. *Informacios Tarsadalom*, 11(1-4):181 – 190.

Harrisona, T. M. and Djoko Sigit, S. (2014). Transparency, participation, and accountability practices in open government: A comparative study. *Government Information Quarterly*, 31(4):512 – 525.

Hellberg, A. and Hedström, K. (2015). The story of the sixth myth of open data and open government. *Transforming Government: People, Process and Policy*, 9(1):35–51.

Henriksen-Bulmer, J. (2015). Systematic literature review: Successful re-identification attacks. Master's thesis, Faculty of Science & Technology; Bournemouth University, Poole, UK.

Information Commissioners Office (2015). Model publication scheme, version 1.2.

Information Commissioners Office (2016). For organisations: Guide to freedom of information: What information do we need to publish?

Janssen, M., Charalabidis, Y., and Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. *Information Systems Management*, 29(4):258 – 268.

Janssen, M. and van den Hoven, J. (2015). Big and open linked data (BOLD) in govenment: A challenge to transparency and privacy. *Government Information Quarterly*, 32(4):363 – 368.

Kimble, C. and Milolidakis, G. (2015). Big data and business intelligence: Debunking the myths. *Global Business & Organizational Excellence*, 35(1):23 – 34.

Lourenço, R. P. (2015). An analysis of open government portals: A perspective of transparency for accountability. *Government Information Quarterly*, 32:323 – 332.

Nissenbaum, H. F. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford Law Books, Stanford: California.

Open Government Partnership (2016a). Open government guide: Open government data: Standards & guidance.

Open Government Partnership (2016b). Participating countries.

Open Government Working Group (2007). Open government working group meeting in sebastopol, ca.

Open Knowledge (2016). Open data index: Tracking the state of government open data.

Palen, L. and Dourish, P. (2003). Unpacking 'privacy' for a networked world. *CHI-Conference*, pages 129 – 136.

Potra, S., Branea, A., and Izvercian, M. (2015). How to foster prosumption for value co-creation? the open government development plan. [Serial on the internet], pages 239 – 245. Education Source, Ipswich, MA.

Shakespeare, S. (2013). Shakespeare review: An independent review of public sector information.

Sicular, S. (2013). Gartner's big data definition consists of three parts, not to be confused with three "V"s.

Sunlight Foundation (2010). Ten principles for opening up government information.

Sweeney, L. (1997). Weaving technology and policy together to maintain confidentiality. *The Journal Of Law, Medicine & Ethics: A Journal Of The American Society Of Law, Medicine & Ethics*, 25(2-3):98.

United Nations (2013). Guidelines on open government data for citizen engagement.

Van't Spijker, A. (2014). *The New Oil: Using Innovative Business Models to Turn Data Into Profit.* Technics Publications, Basking Ridge: NJ, e-book edition.

Wirtz, B. W. and Birkmeyer, S. (2015). Open government: Origin, development, and conceptual perspectives. *International Journal of Public Administration*, 38(5):381 – 396.