023

Privacy

Teresa Scassa

Key points

- Privacy concerns are increasingly at the forefront of debates about data, and publishers of open data are struggling with identifying and addressing potential privacy issues.
- Privacy rights are complex and are not absolute. There is often a balance to strike between transparency and privacy when government information about individuals is involved.
- Striking this balance requires training, resources, and combined commitments to both respecting privacy and advancing openness.

Introduction

Open data programmes urge the release of government datasets in reusable formats under open licences. They also seek to make data findable and datasets interoperable with a view to maximising their reuse both alone and in combination with other datasets. Open data is meant to serve a broad range of purposes, including increasing transparency, enhancing government efficiency, empowering citizens, and stimulating innovation.[1] However, many government datasets also include data about identifiable individuals. Further, some of the most valuable government data is that which relates to citizens and their use of government services.[2] Privacy is, therefore, an important open data issue.

Privacy is treated as a human right in many countries, as well as under several international conventions, including the Charter of Fundamental Rights of the European Union,[3] the Universal Declaration of Human Rights,[4] and the American Convention of Human Rights.[5] Nevertheless, the legal protection available for privacy can vary significantly from one country to another.[6] Some countries have no data protection laws in place.[7] There is also a gap in terms of global data protection frameworks.[8]

Privacy is a broad concept and its normative content may vary from one country to another. Even within individual nations, concepts of privacy may vary considerably among different

segments of the population and in different contexts. In the case of information, privacy is often viewed as a right to exercise some form of control over information about one's self.[9]

While the concept of privacy in the abstract may be difficult to encapsulate, many countries have laws that specifically address the obligation of governments to protect the personal information they collect from citizens. Borgesius et al. (2015) observe that around one hundred countries have some form of data privacy law that adopts fair information principles.[10] The General Data Protection Regulation (GDPR),[11] which took effect in the European Union (EU) in May 2018, provides a comprehensive framework for privacy across public and private sectors and may have an impact on privacy protection beyond EU borders.

Data protection laws aim to protect individuals from a range of different harms. These may vary depending on the nature and extent of the disclosure of personal information. A dataset containing information that links an individual to a particular location, workplace, or income bracket could expose that individual to security risks. The release of sensitive personal data (e.g. financial or health information) may have impacts on an individual's ability to gain employment, secure insurance, or other benefits. The disclosure of this type of data may result in more direct and more easily quantifiable harms than the release of less sensitive data.

An example: Gun permits in the United States

Following the tragic school shooting in Newtown, Connecticut, a newspaper used public registry data to create online interactive maps that showed the names and addresses of all registered gun owners in two New York counties.[12] Many individuals expressed outrage either at being identified as living in a household for which a gun permit had been issued or at being identified as one for which no permit had been issued. While the information had been acceptably public when contained in a registry accessible only through a government office or an access to information request, it was considered unacceptably public when represented on an online interactive map.

It is important to note, however, that privacy rights are not absolute, and they are balanced against other competing public interests. One of these is transparency. In many countries, "right to know" or "access to information" laws mandate the release of information in the hands of government, yet also contain limitations on disclosure that serve to protect privacy. In other words, there is a long-standing acknowledgement that there is a balance to be struck between the right to access government information and the privacy rights of citizens.[13] National/state laws may reflect different visions of privacy or may strike a balance between privacy and transparency differently according to prevailing values. The consequence may be that in a context of global, interoperable, government open datasets, the citizens of some countries may find their personal information more exposed than those in other countries (see Figure 1).

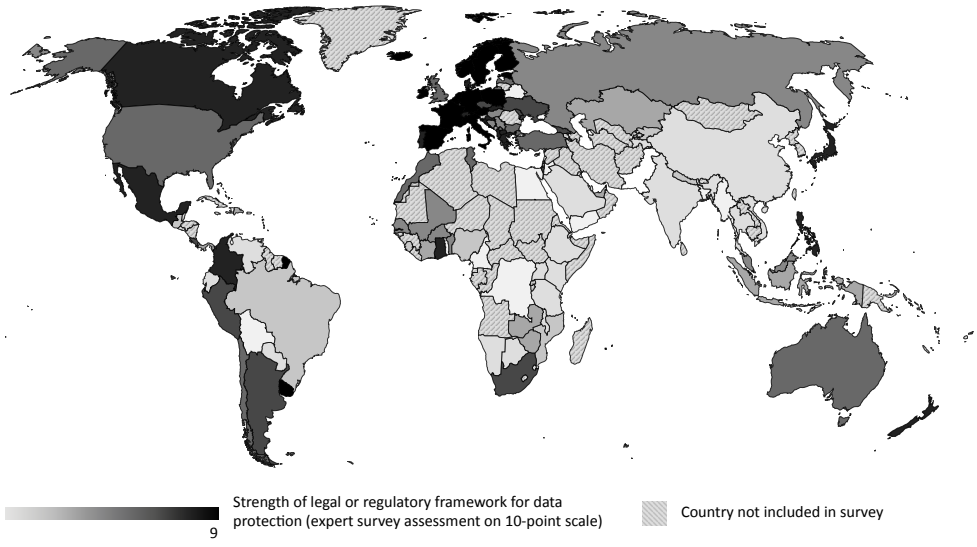

Figure 1: The Open Data Barometer asks about the presence of robust legal or regulatory frameworks for data protection as part of assessing open data readiness. The results illustrate a global divide in the presence of suitable laws and regulations.
Source: https://opendatabarometer.org/?_year=2017&indicator=ODB

The shifting context for open data and privacy

Privacy concerns are at the forefront of the current context for big data analytics, artificial intelligence, and machine learning, all of which are technologies fuelled by data. Open government data can be used in these new technologies and processes,[14] making privacy concerns more acute. While the loss of control over one's personal information is on its own a harm, in our contemporary big data environment, the potential consequences of this loss of control are magnified. A very broad range of other data that can be associated with individuals through analytics could have impacts on decisions made about those individuals or the opportunities that are offered, or never offered, to them.[15] Adding to the privacy harms that may arise if open datasets inappropriately contain personal information, concerns over privacy could lead citizens to seek to share less data with governments.[16]

The 2013 G8 Open Data Charter[17] did not mention privacy, perhaps because earlier views on open data were that it involved only non-personal data, and therefore, did not raise privacy issues. The potential for reidentification of individuals from deidentified datasets using data from multiple sources (the mosaic effect) sharpened concerns about privacy and open data. The International Open Data Charter of 2015[18] specifically acknowledges that open data by default must involve appropriate anonymisation.

In addition to the issues about how data is used in the context of big data and artificial intelligence, it is important to note that governments are poised to collect even greater volumes of personal information as cities become increasingly sensor-laden and networked. The smart cities context also presents privacy challenges when the release of smart city sensor data is contemplated.[19]

While the focus of this paper is on open government data, it is important to keep in mind that the concept of open data is now broader than just government data. Open data now comes from many different sources, including open scientific data and data voluntarily published by various organisations. Still other data is open in the sense that it is published online and capable of being scraped or otherwise extracted (such as social media platform data).[20] The availability of all of this data contributes to the issues of identifiability of individuals as a result of the release of open government datasets, even in anonymised forms, because of the potential for combining these different sources of data to achieve reidentification. The combined use of data from all of these sources of "open" data in big data analytics and machine learning raises compelling privacy issues, as well as issues that go beyond privacy to social justice and equality.[21]

Key issues

The definition of personal information

Privacy in open government data tends to be addressed through a consideration of whether datasets identified for release contain personal information. As most public sector data protection laws deal with government treatment of personal information, this focus is not surprising. Therefore, the scope of privacy protection in open data depends on the definition of "personal information". Unique identifiers (i.e. names or numbers on official identification documents) are clearly personal information. Some approaches to open data simply consider this type of information to be unsuitable for release as open data. In other words, open data is, by definition, data that does not include personal information.[22] Nevertheless, the obligation to protect privacy generally goes beyond merely declining to release datasets that contain unique personal identifiers, such as names or identity numbers. Privacy is generally defined for data protection purposes as "information about an identifiable individual" or "personally identifiable information". Identifiability has been interpreted broadly by many data protection authorities. Thus, if an individual can be identified from a dataset when it is combined with other available data, regardless of the source of that data, then the dataset is said to contain personal information.[23] Notorious examples involving supposedly deidentified or anonymised private sector data include the reidentification of individuals from anonymised datasets of Netflix viewing habits,[24] or, more recently, from anonymised data used to create Strava heat maps.[25] As data analytics become more sophisticated, and as the volume of available "other" data grows exponentially, reidentification risks in anonymised datasets may be extremely high.[26] Ohm cautions that in a big data era, the effectiveness of anonymisation techniques may be considerably undermined.[27] If taken to a logical extreme, reidentification risks could lead to decisions not to release any government data that might be linked to identifiable individuals. This would significantly reduce the stock of

available open data. Some researchers insist that remote and intangible risks should not drive policies around open data in light of strong anonymisation techniques, and they have designed and proposed anonymisation tools and techniques to support the release of useful data.[28]

Not all personal information necessarily has the same level of sensitivity. Some categories, such as health data or data about religious or ethnic identity, may be considered more sensitive than others.[29] The level of sensitivity may determine the degree of anonymisation required before a dataset can be released as open data.

Although not strictly personal information, "demographically identifiable information" (DII) or "community identifiable information" (CII) may also be sensitive information. DII is defined as "data that can be used to identify a community or distinct group, whether geographic, ethnic, religious, economic, or political".[30]

The privacy/transparency balance

When it comes to the relationship between citizens and the state, privacy is not an absolute. In many instances, privacy is balanced with transparency, permitting the public disclosure of some forms of personal information (e.g. political donations, permit applications, land titles registration, etc.). In some cases, this balance is defined within specific legislative instruments that determine how particular kinds of information are to be dealt with. In other cases, general principles are found in access to information/right to know laws. As Borgesius et al. (2015) note, the privacy/transparency balance was negotiated in the context of such laws for decades prior to the open data movement.[31]

It is sometimes difficult to separate information about institutions from information about individuals.[32] The balance between privacy and transparency may be struck differently in different countries, depending upon political and social contexts. For example, in some countries, battling corruption may be seen as a more urgent priority than protecting privacy. This does not mean that privacy is not respected, but it may mean that there is less privacy with respect to some kinds of information that is shared with government. Greater transparency may also serve goals of equity by exposing biases and inequality. Principles of transparency may mandate the disclosure of considerable amounts of quite personal information. For example, open court principles require trials to be open to the public, and mandate the publication of court and tribunal decisions.[33] Some governments require the publication of the salaries of public servants, identified by name and position. While it is possible to treat some of this information as open information and not open data (i.e. publishing it in tabular form on a website, rather than as a downloadable dataset), the technological reality is that once it is published in either form, it is available for extraction and reuse. Thus, although there is a distinction between open data and open information, it may be largely meaningless from a privacy perspective.

In cases where such data is shared publicly, their transparency value is considered to outweigh any privacy concerns. In many cases, however, these assessments may have been made in a pre-digital era or at least prior to our big data era. Where this is the case, the privacy impacts of the release of such data may have changed and may require reassessment.[34] Assessing privacy impacts throughout the life of a dataset, and not just upon its release, is now an open data best practice.[35] Recent struggles in Canada with the exploitation of personal information contained in court and tribunal decisions published online highlight these challenges.[36]

As noted earlier, different countries may set the balance between privacy and transparency differently, and open data is available without geographic restrictions. Its users may be found anywhere in the world. Therefore, while the transparency benefits of open data tend to be experienced within the jurisdiction releasing the data, the privacy risks may be global.

An example: Court decisions in Canada

Court and administrative tribunal decisions in Canada are published on the websites of the specific courts and tribunals, as well as on CanLII, a portal that aggregates and provides open access to these documents. These decisions often contain personal information, some of which might be quite sensitive. To balance the open court principle with privacy rights, the court, tribunal, and CanLII websites do not permit indexing by search engines. In 2013, the Office of the Privacy Commissioner of Canada began receiving complaints that a Romanian-based entity was scraping decisions from these websites and posting the decisions on its own fully indexed website. Individuals who complained to the Romanian website about the publication of their personal information were offered the option to pay in order to have this information deleted. A court case brought in Canada ruled that the Romanian site breached Canadian data protection law, ordering the site to remove all Canadian court and tribunal decisions that contained personal information.

Open data challenges

There are some features of open data that present particular challenges when it comes to addressing privacy issues. For example, the ideal of open data is data that "can be freely used, modified, and shared by anyone for any purpose".[37] This includes commercial purposes. The commercial reuse of open data, particularly in a big data environment, may increase privacy risks.[38] As noted earlier, some of the most useful and important datasets are ones that relate to citizen activities and their consumption of public services.[39] Data may, therefore, be more useful if it contains personal information.[40] It may also be less useful if anonymisation techniques substantially impact the data for certain purposes.[41]

Other challenges exist at the operational level. Identifying datasets that contain personal information and preparing them for release through anonymisation can be time and resource intensive. In some cases, available government resources may not be sufficient for the task.[42] Further, deciding whether datasets contain information capable of leading to the reidentification of individuals can be challenging, as can determinations of whether the anonymisation techniques applied are adequate, depending on the degree of sensitivity of the data. In many cases, civil servants are left to make judgement calls about whether certain datasets should be released. This can lead to variance from one government department to another in terms of willingness to release certain types of datasets. Further, a risk-averse government culture may lean toward non-release where any doubts arise.[43] Some have argued that open data requires a cultural shift within governments to overcome such barriers and hesitations.[44] In the case of privacy, that cultural shift might mean accepting some level of reidentification risk.

Privacy issues and preparing open data for release

A considerable amount of work has gone into the design and development of guidance for governments around how to open data while addressing privacy concerns. Some of this work has been led by governments involved in the release of open data and some by academics. Considerable attention has been paid to the development of tools, analytical frameworks, and other guidance documents.[45] These are meant to provide practical guidance to those who must decide whether a dataset that contains personal information should be opened, and then, if so, decide how the dataset should be dealt with in order to protect privacy.

One important privacy-protective measure is greater government awareness of the importance of limiting the collection of personal information to only that which is truly necessary.[46] Another measure is to conduct risk/benefit analyses or privacy impact assessments with respect to the release of datasets that may raise privacy concerns.[47] Given the rapidly changing technology and big data context, it is also advisable that privacy issues be considered at every stage of a dataset's life cycle and not just at the point leading up to its publication as open data.[48] Attention must also be paid to the various techniques that are available for removing personal information, including pseudonymisation (replacing names with unique identifiers) or anonymisation. Various anonymisation techniques exist, including aggregation and randomisation.[49]

Some have argued that the release of datasets that raise potential privacy issues might call for a different kind of licensing.[50] In other words, such datasets might be subject to licences that restrict their reuse to only certain contexts (e.g. non-commercial) or that prohibit activities aimed at reidentification. However, privacy protection through licensing terms depends on the licensor's ability to track and monitor reuse, as well as their willingness to take legal action in case of breach of terms.

Some now argue for a more nuanced approach to "open". For example, the Open Data Institute (ODI) proposes a spectrum of openness with different levels of access to data depending upon its nature, the identity of the user, and the proposed use (see Figure 2, overleaf).

Conclusion

There is no doubt that privacy is a key issue for open data. Not only does citizen trust depend on governments' abilities to appropriately protect the personal information that is shared with them, individuals can be exposed to privacy harms if personal information is inappropriately shared. Nevertheless, privacy rights are not an absolute. The need to balance privacy with transparency in relation to government information and data predates the open data movement. In some cases, public interest in transparency may justify the disclosure of personal information as open data. Privacy is a concept that can vary from one country to another and among subgroups within a given country. In addition, the privacy/transparency balance may be struck differently in different countries depending on the relative importance of either goal. It is important to note, however, that privacy impacts may now be experienced on a global scale.

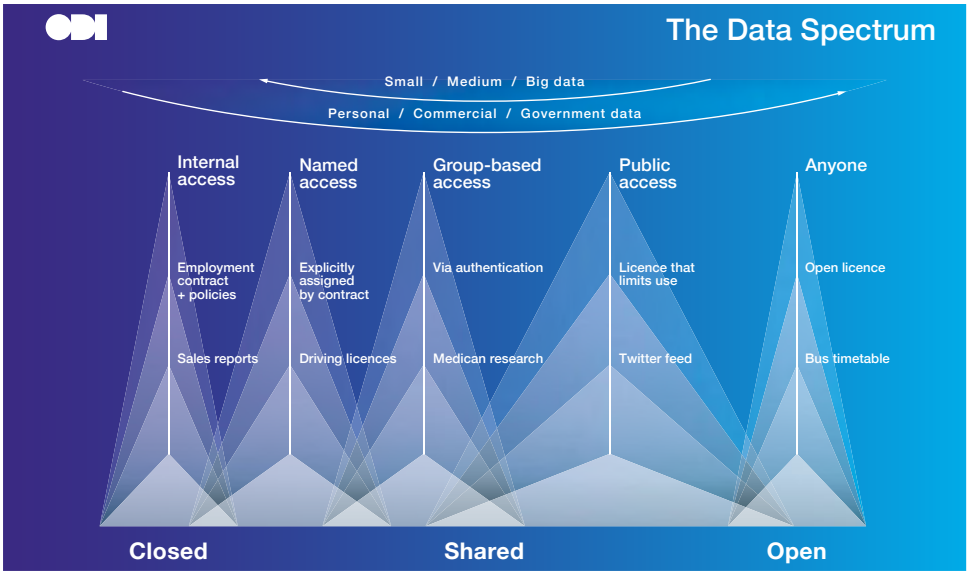

Figure 2: The Open Data Spectrum was published in 2016, consolidating a growing understanding in the open data field that ideas of "open by default" must be considered alongside a recognition of legitimate access control for some datasets.
Source: https://theodi.org/about-the-odi/the-data-spectrum/

The rapidly evolving era of big data and artificial intelligence has given rise to new uses for open government data. These technologies also increase the risk of reidentification of individuals through the matching of anonymised data from multiple different sources. This increased reidentification risk poses challenges for the release of useful open data, and requires a carefully balanced approach. Some reidentification risk may be acceptable, depending on the nature and value of the data at issue. Over the last few years, there has been a proliferation of tools to provide guidance to government agencies and departments struggling with open data privacy issues. These tools will be useful to those who want to open up data in other contexts as well.

At the same time as the publishers of open data struggle with identifying and addressing potential privacy issues, a large volume of often highly personal information is routinely published by governments based on policies developed prior to the big data era, and, in some cases, even prior to the internet. Publicly available personal information is found in multiple government registries, as well as in court and tribunal decisions, and it is published under various transparency laws and policies related to elections, procurement, public sector salaries, etc. The impacts of the digital environment and of big data on privacy in relation to these categories of government data will require a reassessment of how such data is made publicly available.

Balancing privacy and transparency in the release of open data will require training and resources, and the commitment of governments to provide these resources will have a significant impact on how the balance is struck. When datasets contain personal information, a simple refusal to disclose the datasets will limit access to the data for reuse. Instead, what is required is a process for determining whether the data can be adequately anonymised to protect privacy while furthering the release of open data.

Further reading

Borgesius, F.Z., Gray, J., & Van Eechoud, M. (2015). Open data, privacy, and fair information principles: Towards a balancing framework. *Berkeley Technology Law Journal*, *30(3)*, 2073–2130. http://btlj.org/data/articles2015/vol30/30_3/2073-2132%20Borgesius.pdf

Finkle, E. (2016). *Resources: Open data release toolkit*. Version 1.2. San Francisco, CA: Data SF. https://datasf.org/resources/open-data-release-toolkit/

Floridi, L. (2014). Open data, data protection, and group privacy. *Philosophy and Technology*, *27(1)*, 1–3. https://link.springer.com/article/10.1007/s13347-014-0157-8

Garfinkel, S.L. (2016). *De-identifying government datasets*. DRAFT NIST Special Publication 800-188. Washington, DC: US Department of Commerce, National Institute of Standards and Technology. https://csrc.nist.gov/csrc/media/publications/sp/800-188/archive/2016-08-25/documents/sp800_188_draft.pdf

Green, B., Cunningham, G., Ekblaw, A., Kominers, P., Linzer, A., & Crawford, S. (2017). *Open data privacy*. Cambridge, MA: Berkman Klein Center for Internet & Society Research Publication. https://cyber.harvard.edu/publications/2017/02/opendataprivacyplaybook

ODI (Open Data Institute). (n.d.). The data spectrum. https://theodi.org/about-the-odi/the-data-spectrum/

About the author

Teresa Scassa is the Canada Research Chair in Information Law and Policy at the University of Ottawa. She teaches and researches in the area of information law, including intellectual property and privacy law. More information about Teresa is available at https://www.teresascassa.ca.

How to cite this chapter

Scassa, T. (2019). Issues in open data: Privacy. In T. Davies, S. Walker, M. Rubinstein, & F. Perini (Eds.), *The state of open data: Histories and horizons* (pp. 339–350). Cape Town and Ottawa: African Minds and International Development Research Centre. http://stateofopendata.od4d.net

Endnotes

1 Davies, T.G. (2014). Open data policies and practice: An international comparison. *SSRN* [Article], 5 September. http://dx.doi.org/10.2139/ssrn.2492520

2 Simperl, E., O'Hara, K., & Gomer, R. (2016). *Analytical report 3: Open data and privacy*. Luxembourg: European Data Portal. https://www.europeandataportal.eu/sites/default/files/open_data_and_privacy_v1_final_clean.pdf

3 EU. (2000). *Charter of Fundamental Rights of the European Union*, 2000/C 364/01. Brussels, Belgium: European Union Parliament. http://www.europarl.europa.eu/charter/pdf/text_en.pdf

4 UN. (1948). *Universal Declaration of Human Rights*. General Assembly Resolution 217A. New York, NY: United Nations. http://www.un.org/en/universal-declaration-human-rights/

5 OAS. (1969). *American Convention on Human Rights*. Washington, DC: Organization of American States. https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm

6 See, for example, DLA Piper. (2018). Data protection laws of the world. https://www.dlapiperdataprotection.com/

7 UNCTAD (United Nations Conference on Trade and Development). (n.d.). Summary of adoption of e-commerce legislation worldwide. New York, NY: United Nations. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx

8 UNCTAD (United Nations Conference on Trade and Development). (2016). *Data protection regulations and international data flows: Implications for trade and development*. New York, NY: United Nations. http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

9 Nissenbaum, H. (2016). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford Law Books; Solove, D.J. (2008). *Understanding privacy*. Cambridge, MA: Harvard University Press.

10 Borgesius, F.Z., Gray, J., & Van Eeechoud, M. (2015). Open data, privacy, and fair information principles: Towards a balancing framework. *Berkeley Technology Law Journal*, *30(3)*, 2073–2130.

11 GDPR (General Data Protection Regulation). (2018). Regulation (EU) 2016/679, *OJ* L 119, 04.05.2016; cor. *OJ* L 127, 23.5.2018. Strasbourg: European Parliament and Council of the European Union. https://gdpr-info.eu/

12 Worley, D.R. (2012). *The gun owner next door: What you don't know about the weapons in your neighbourhood*. http://people.sju.edu/~ggrevera/se/privacyIssues/JournalNews-The-gun-owner-next-door.pdf

13 Janssen, K. (2012). Open government and the right to information: Opportunities and obstacles. *Journal of Community Informatics*, *8(2)*, 1–11.

14 Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures & their consequences*. London: SAGE Publications Ltd.

15 Borgesius, F.Z., Gray, J., & Van Eechoud, M. (2015). Open data, privacy, and fair information principles: Towards a balancing framework. *Berkeley Technology Law Journal*, *30(3)*, 2073–2130; Citron, D.K. & Pasquale, F.A. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, *89*, 1–34. https://ssrn.com/abstract=2376209

16 Borgesius, F.Z., Gray, J., & Van Eechoud, M. (2015). Open data, privacy, and fair information principles: Towards a balancing framework. *Berkeley Technology Law Journal*, *30(3)*, 2073–2130.

17 https://www.gov.uk/government/publications/open-data-charter/g8-open-data-charter-and-technical-annex

18 https://opendatacharter.net/

19 Borgesius, F.Z., Gray, J., & Van Eechoud, M. (2015). Open data, privacy, and fair information principles: Towards a balancing framework. *Berkeley Technology Law Journal*, *30(3)*, 2073–2130.

20 Scassa, T. (2017). Sharing data in the platform economy: A public interest argument for access to platform data. *University of British Columbia Law Review*, *50(4)*, 1017–1071. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3077996

21 Citron, D.K. & Pasquale, F.A. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, *89*, 1–34. https://ssrn.com/abstract=2376209; Kim, P.T. (2017). Auditing algorithms for discrimination. *University of Pennsylvania Law Rev*iew, *166*, 189–203.

22 Open Knowledge International. (n.d.). What is open data? In *The open data handbook*. Cambridge, UK: Open Knowledge International. http://opendatahandbook.org/guide/en/what-is-open-data/

23 Scassa, T. (2010). Geographic information as personal information. *Oxford University Commonwealth Law Journal*, *10(2)*, 185–214.

24 Porter, C.C. (2008). De-identified data and third party data mining: The risk of re-identification of personal information. *Shidler J.L. Com. & Tech*, *5(1)*. http://www.lctjournal.washington.edu/Vol5/a03Porter.html

25 Hsu, J. (2018). The Strava Heat Map and the end of secrets. *Wired*, 29 January. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

26 Green, B., Cunningham, G., Ekblaw, A., Kominers, P., Linzer, A., & Crawford, S. (2017). *Open data privacy*. Cambridge, MA: Berkman Klein Center for Internet & Society Research Publication. https://cyber.harvard.edu/publications/2017/02/opendataprivacyplaybook; Ohm, P. (2017). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Rev*, *57*, 1701–1777; Sweeney, L. (2010). k-Anonymity: A model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems*, *10(5)*, 557–570. https://epic.org/privacy/reidentification/Sweeney_Article.pdf

27 Ohm, P. (2017). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Rev*, *57*, 1701–1777.

28 See, for example, El Emam, K. (2013). *Guide to the de-identification of personal health information*. Boca Raton, FA: CRC Press.

29 ICO (Information Commissioner's Office). (n.d.). Special category data. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

30 NRC. (2017*). 510 Data Responsibility Policy*. Version 2.0, 8 November. The Hague: Netherlands Red Cross . https://www.510.global/wp-content/uploads/2017/11/510_Data_Responsibility_Policy_V.2_PUBLIC-1.pdf

31 Borgesius, F.Z., Gray, J., & Van Eechoud, M. (2015). Open data, privacy, and fair information principles: Towards a balancing framework. *Berkeley Technology Law Journal*, *30(3)*, 2073–2130.

32 Simperl, E., O'Hara, K., & Gomer, R. (2016). *Analytical report 3: Open data and privacy*. Luxembourg: European Data Portal. https://www.europeandataportal.eu/sites/default/files/open_data_and_privacy_v1_final_clean.pdf

33 Scassa, T. (2014). Privacy and open government. *Future Internet*, *6*, 397–413. www.mdpi.com/1999-5903/6/2/397/pdf

34 Ibid.; Borgesius, F.Z., Gray, J., & Van Eechoud, M. (2015). Open data, privacy, and fair information principles: Towards a balancing framework. *Berkeley Technology Law Journal*, *30(3)*, 2073–2130.

35 Green, B., Cunningham, G., Ekblaw, A., Kominers, P., Linzer, A., & Crawford, S. (2017). *Open data privacy*. Cambridge, MA: Berkman Klein Center for Internet & Society Research Publication. https://cyber.harvard.edu/publications/2017/02/opendataprivacyplaybook

36 Dobby, C. (2015). Canadians upset with Romanian website that exposes court case details. *The Globe and Mail*, 4 January. http://www.theglobeandmail.com/report-on-business/industry-news/the-law-page/canadians-upset-over-romanian-website-that-exposes-court-case-details/article22284367/; *A.T. v. Globe24h.com*, 2017 FC 114 (CanLII). http://canlii.ca/t/gx6bl

37 Open Knowledge International. (n.d.). The Open Definition. Cambridge, UK: Open Knowledge International. http://opendefinition.org; Ubaldi, B. (2013). *Open government data: Towards empirical analysis of open government data initiatives*. OECD Working Papers on Public Governance 22, p. 6. Paris: Organisation for Economic Co-operation and Development Publishing. http://dx.doi.org/10.1787/5k46bj4f03s7-en

38 Simperl, E., O'Hara, K., & Gomer, R. (2016). *Analytical report 3: Open data and privacy*. Luxembourg: European Data Portal. https://www.europeandataportal.eu/sites/default/files/open_data_and_privacy_v1_final_clean.pdf

39 Simperl, E., O'Hara, K., & Gomer, R. (2016). *Analytical report 3: Open data and privacy*. Luxembourg: European Data Portal. https://www.europeandataportal.eu/sites/default/files/open_data_and_privacy_v1_final_clean.pdf

40 Green, B., Cunningham, G., Ekblaw, A., Kominers, P., Linzer, A., & Crawford, S. (2017). *Open data privacy*. Cambridge, MA: Berkman Klein Center for Internet & Society Research Publication. https://cyber.harvard.edu/publications/2017/02/opendataprivacyplaybook

41 Garfinkel, S.L. (2016). *De-identifying government datasets*. DRAFT NIST Special Publication 800-188. Washington, DC: US Department of Commerce, National Institute of Standards and Technology. https://csrc.nist.gov/csrc/media/publications/sp/800-188/archive/2016-08-25/documents/sp800_188_draft.pdf

42 Johnson, P.A., Sieber, R.E., Scassa, T., Stephens, M., & Robinson, P.J. (2017). The cost(s) of geospatial open data. *Transactions in GIS*, *21*, 434–445. http://onlinelibrary.wiley.com/doi/10.1111/tgis.12283/full

43 Huijboom, N. & Van den Broek, T. (2011). Open data: An international comparison of strategies. *European Journal of ePractice*, *12*, 1–13. https://research.vu.nl/en/publications/open-data-an-international-comparison-of-strategies

44 See, for example, Davies, T. & Bawa, Z.A. (2012). The promises and perils of Open Government Data (OGD). *The Journal of Community Informatics*, *8(2)*. http://ci-journal.net/index.php/ciej/article/view/929/926

45 See, for example, Green, B., Cunningham, G., Ekblaw, A., Kominers, P., Linzer, A., & Crawford, S. (2017). *Open data privacy*. Cambridge, MA: Berkman Klein Center for Internet & Society Research Publication. https://cyber.harvard.edu/publications/2017/02/opendataprivacyplaybook; Borgesius, F.Z., Gray, J., & Van Eechoud, M. (2015). Open data, privacy, and fair information principles: Towards a balancing framework. *Berkeley Technology Law Journal*, *30(3)*, 2073–2130; Garfinkel, S.L. (2016). *De-identifying government datasets*. DRAFT NIST Special Publication 800-188. Washington, DC: US Department of Commerce, National Institute of Standards and Technology. https://csrc.nist.gov/csrc/media/publications/sp/800-188/archive/2016-08-25/documents/sp800_188_draft.pdf; Finkle, E. (2016). *Resources: Open data release toolkit*. Version 1.2. San Francisco, CA: Data SF. https://datasf.org/resources/open-data-release-toolkit/; Article 29 Data Protection Working Party. (2013). Opinion 06/2013 on open data and Public Sector Information ('PSI') reuse. http://www.gpdp.gov.mo/uploadfile/2014/0505/20140505062629657.pdf; Scassa, T. & Conroy, A. (2016). Strategies for protecting privacy in open data and proactive disclosure. *Canadian Journal of Law and Technology*, *14*, 215–262.

46 Scassa, T. & Conroy, A. (2016). Strategies for protecting privacy in open data and proactive disclosure. *Canadian Journal of Law and Technology*, *14*, 215–262; IPC. (2009). *Privacy and government 2.0: The implications of an open world*. Toronto: Information and Privacy Commissioner of Ontario. http://www.ontla.on.ca/library/repository/mon/23006/293152.pdf

47 Scassa, T. & Conroy, A. (2016). Strategies for protecting privacy in open data and proactive disclosure. *Canadian Journal of Law and Technology*, *14*, 215–262; Green, B., Cunningham, G., Ekblaw, A., Kominers, P., Linzer, A., & Crawford, S. (2017). *Open data privacy*. Cambridge, MA: Berkman Klein Center for Internet & Society Research Publication. https://cyber.harvard.edu/publications/2017/02/opendataprivacyplaybook

48 Simperl, E., O'Hara, K., & Gomer, R. (2016). *Analytical Report 3: Open data and privacy*. Luxembourg: European Data Portal. https://www.europeandataportal.eu/sites/default/files/open_data_and_privacy_v1_final_clean.pdf

49 See, for example, Garfinkel, S.L. (2016). *De-identifying government datasets*. DRAFT NIST Special Publication 800-188. Washington, DC: US Department of Commerce, National Institute of Standards and Technology. https://csrc.nist.gov/csrc/media/publications/sp/800-188/archive/2016-08-25/documents/sp800_188_draft.pdf; Finkle, E. (2016). *Resources: Open data release toolkit*. Version 1.2. San Francisco, CA: Data SF. https://datasf.org/resources/open-data-release-toolkit/; Scassa, T. & Conroy, A. (2016). Strategies for protecting privacy in open data and proactive disclosure. *Canadian Journal of Law and Technology*, *14*, 215–262.

50 Borgesius, F.Z., Gray, J., & Van Eechoud, M. (2015). Open data, privacy, and fair information principles: Towards a balancing framework. *Berkeley Technology Law Journal*, *30(3)*, 2073–2130; Scassa, T. & Conroy, A. (2016). Strategies for protecting privacy in open data and proactive disclosure. *Canadian Journal of Law and Technology*, *14*, 215–262.