Data & Policy (2020), 2: e8
doi:10.1017/dap.2020.8

COMMENTARY

The role of technology in governance: The example of Privacy Enhancing Technologies

Natasha McCarthy and Franck Fourniol

Science Policy Section, The Royal Society, London, United Kingdom
*Corresponding author. Email: natasha.mccarthy@royalsociety.org

This paper is a commentary piece based on and drawing from the Royal Society report: Protecting privacy in practice—the current use, development and limits of Privacy Enhancing Technologies in data analysis (The Royal Society, 2019).

Received: 29 August 2019; **Revised:** 12 March 2020; **Accepted:** 29 April 2020

Keywords: data management and use; differential privacy; governance; homomorphic encryption; personal data stores; Privacy Enhancing Technologies; secure multi-party computation; trusted execution environments

Abstract

The collection of data, its analysis, and the publication of insights from data promise a range of benefits, but can carry risks for individuals and organizations. This paper sets out considerations regarding the potential role for technologies in governance of data use, and some key limitations. The paper examines the potential of Privacy Enhancing Technologies (PETs) to support organizations and institutions that handle data in governing data use, and considers their role based on their current state of development and the trajectory of technological development. This involves consideration both of how these technologies can potentially enable governments and others to unlock the value of data, and also recognition of both contingent and in principle limitations on the role of PETs in ensuring well-governed use of data.

Policy Significance Statement

If we are to unlock the benefits of data for policy, balancing the use of technologies with the right organizational structures, institutions, and skilled users is important to ensure human flourishing in a data-enabled society. In particular, to enable wider and well-informed use of technologies in the governance of data use, we need to create and support a community of intelligent users—who know what the technologies can and cannot deliver both technically and in terms of meeting ethical requirements. This can also inform future research.

Abbreviations

ICO, Information Commissioner's Office; MPC, secure multi-party computation; PDS, personal data stores; PETs, Privacy Enhancing Technologies, TEE, trusted execution environment.

Background and Introduction

The amount of data generated from the world around us has reached levels that were previously unimaginable. The use of data-enabled technologies promises significant benefits, from improving healthcare provision and treatment discovery, to better managing critical infrastructure such as transport and energy. However, the collection of data, its analysis, and the publication of insights from data can all carry risks for individuals and organizations.

The British Academy and Royal Society report *Data Management and Use: Governance in the 21st Century* (The British Academy and The Royal Society, 2017), published in June 2017, highlighted a series of such tensions between benefits and risks—or between competing benefits—in the use of data. These tensions include:

1. Using data relating to individuals and communities to provide more effective public and commercial services, while not limiting the information and choices available.
2. Promoting and distributing the benefits of data use fairly across society while ensuring acceptable levels of risk for individuals and communities.
3. Promoting and encouraging innovation, while ensuring that it addresses societal needs and reflects public interest.
4. Making use of the data gathered through daily interaction to provide more efficient services and security, while respecting the presence of spheres of privacy.

The Royal Society has continued this work on the governance of data use by considering the role of Privacy Enhancing Technologies (PETs) in enabling well-governed use of data. The PETs project examined the role of technologies in enabling data analysis and extracting value while preserving personal or sensitive information. Thus, a high-level aim of the project was to assess the extent to which there is a role for technology in addressing the tensions set out in the *Data Management and Use: Governance in the 21st Century* report, and to understand the specific roles and limitations of PETs in enabling data users—including those in the public sector—to steer a course through these tensions.

The aims of the project were to explore the interplay between the following questions in relation to PETs:

1. What are the ethical and social issues at stake in the use of these technologies?
2. What is mathematically possible and what is technically feasible in their development and use?
3. What business models and incentive systems can deliver these technologies?

It addressed these questions by exploring the underlying principles, current state of development, and use cases for the following technologies, considering them within the wider context of business systems and governance frameworks influencing data use:

1. Homomorphic encryption.
2. Differential privacy.
3. Secure multi-party computation.
4. Trusted execution environments.
5. Personal data stores.

These are five interrelated and heterogeneous approaches within a broad field and there was no intention to suggest that these particular technologies will develop earlier or get more uptake than others. The particular technologies were selected following a series of interviews with researchers and practitioners during the project scoping. It was carried out by gathering evidence through a series of cross-sector expert workshops and by developing case studies of these technologies and approaches in practice.

https://doi.org/10.1017/dap.2020.8 Published online by Cambridge University Press

The Role of PETs in Data Governance—How can PETs Enable Well-Governed use of Data?

Navigating the tensions created by new uses of data, set out above and in the *Data Management and Use: Governance in the 21st Century* report, requires appropriate governance mechanisms, from codes of conduct and ethics to regulation. However, in some cases, technological solutions can help diffuse dilemmas between making use of data and protecting both the individuals and organizations that generate or are subjects within datasets. PETs as a category comprises a broad suite of technologies and approaches—from a piece of tape masking a webcam to advanced cryptographic techniques. While some are focused on protecting private communications, the report explored a subset of five PETs identified during the scoping of the project as being particularly promising to enable privacy-aware data collection, analysis, and dissemination of results.

The key question of this paper is whether, according to the current state of development and the trajectory of technological development, we can utilize PETs in addressing social and ethical tensions in data use, and thereby use them as tools for governing the ways that data is used. This will involve consideration both of how these technologies can potentially enable governments and others to unlock the value of data, while also recognizing both contingent and in principle limitations on the role of PETs in ensuring well-governed use of data.

The Technologies

There is currently no technology that is applicable to every single situation of privacy-preserving data analysis. Different PETs can be used to achieve distinct aims, such as:

1. Securely providing access to private datasets.
2. Enabling joint analysis on private data held by several organizations.
3. Securely out-sourcing to the cloud computations on private data.
4. De-centralizing services that rely on user data.

One way to understand the technologies set out in the report and their potential role in governance of data use is by relating them to the social and ethical tensions set out in *Data Management and Use,* which they might help to resolve. To note again that we were primarily looking at privacy protection for big data analysis—but with the exception of personal data stores (PDS) which present a slightly different approach.

Tension 1: **Making use of the data** gathered through daily interaction to provide more efficient services and security, while respecting the presence of **spheres of privacy**.

Tension 2: Providing ways to **exercise reasonable control over data** relating to individuals while **encouraging data sharing** for private and public benefit.

Public and commercial organizations routinely collect data by users of their services. These data can be used to improve the service—but can also be revealing of individuals' and groups' everyday behavior, creating the tensions above. Thus, a means is needed to enable this use while protecting this sensitive information.

Homomorphic encryption

Homomorphic encryption is a form of encryption that allows certain computations on encrypted data, generating an encrypted result which, when decrypted, matches the result of the same operations performed on the data before encryption (Player, 2018).

Homomorphic encryption can be used to analyze data in circumstances where all or part of the computational environment is not trusted, and sensitive data should not be accessible. It is currently applicable where the computation required is known and relatively simple. Homomorphic encryption provides confidentiality and can be used to address the risk of revealing sensitive attributes related to individuals or organizations, in a dataset or output.

https://doi.org/10.1017/dap.2020.8 Published online by Cambridge University Press

Trusted execution environments

A trusted execution environment (TEE) is a secure area inside a main processor (see e.g., Anati et al., 2013). TEEs are isolated from the rest of the system, so that the operating system cannot read the code in the TEE. However, TEEs can access memory outside. TEEs can also protect data "at rest," when it is not being analyzed, through encryption.

Like homomorphic encryption, TEEs might be used to securely outsource computations on sensitive data to the cloud. Instead of a cryptographic solution, TEEs offer a hardware-based way to ensure data and code cannot be learnt by a server to which computation is outsourced. Unlike homomorphic encryption, current TEEs are widespread and permit the computation of virtually any operations.

Tension 3: **Incentivising innovative** uses of data while ensuring that such data can be **traded and transferred** in mutually beneficial ways.

Commercial organizations, for example, face this tension when there is value in learning from the practices and performance of competitors but accessing relevant data would reveal commercially sensitive information. Certain cryptographic techniques can enable different organizations to analyze and derive insights from data without pooling it or sharing it with each other. This opens up the potential for companies to learn from each other without giving away trade secrets.

Multi-party computation

Secure multi-party computation (MPC) is a subfield of cryptography concerned with enabling private distributed computations. MPC protocols allow computation or analysis on combined data without the different parties revealing their own private input. In particular, it may be used when two or more parties want to carry out analyses on their combined data but, for legal or other reasons, they cannot share data with one another (Archer et al., 2018).

Tension 4: **Promoting and distributing the benefits** of data use fairly across society while ensuring **acceptable levels of risk** for individuals and communities.

And also *Tension 1*: **Making use of the data** gathered through daily interaction to provide more efficient services and security, while respecting the presence of **spheres of privacy**.

Here, large organizations might face this tension as they might want to enable different parties (internal or external) to access and use a derived dataset or statistics, while limiting the risk to reveal information about any specific individual or entity.

Differential privacy

Differential privacy is a slightly different PET in that it is not a technology per se. It is a security definition which means that, when a derived insight is released, it should not give much more information about a particular individual than if that individual had not been included in the dataset used to produce that insight—and this amount is referred to as "privacy budget" and can be quantified (Nissim et al., 2018). By fixing a privacy budget for a given set of information released, an institution can reason mathematically about the risk of disclosure of information relating to a specific individual. It is achieved by a central trusted authority altering a fraction of the data (e.g., by adding noise), either at point of collection or at point of disclosure of the output of an analysis.

An alternative way of addressing *Tension 2* above is by providing individuals with more control over how data related to them gets used. Organizations, for example, might want to use citizen data for public good while, to build trust, they might want to support individuals in "exercising reasonable control."

Personal data stores

PDS are again not a technology as such, but they are ways of enabling better control of data so that people can access data-driven services without giving away their data to an external server.

https://doi.org/10.1017/dap.2020.8 Published online by Cambridge University Press

Unlike the other four PETs covered in the report, which are tools for privacy-preserving computation and are used by organizations analyzing data, PDS are citizen- or consumer-facing apps and services (World Economic Forum, 2013) which can be supported by different kinds of PETs. They provide an example of one of the goals for PETs—enabling people to have more control over data.

PDSs are a way to enable a distributed system, where the data can be stored and processed at the "edge" of the system, rather than centralized. It is possible, for instance, to send machine learning algorithms to the data, rather than the data to the algorithms. Distributing out the data and computing addresses a number of issues such as the "honeypot" issue—whereby an organization holding millions of records constitutes a "honeypot" that is economically attractive to hack.

These different technologies and approaches are used to varying degrees depending on their level of maturity. There are some examples of current pilots and well-established use.

Use Cases: What Can Work in Practice

How far are these technologies able to underpin the ways that data use is governed in practice? The field of PETs development is moving quickly, and the Royal Society report captures a moment in time where the technologies are maturing and opportunities to use these technologies are beginning to emerge. It may be that some of the technologies surveyed in our report do not achieve their promise in the near term, or that the costs of adoption prove prohibitive, or that other technologies not explored in depth might leapfrog them. However, there are a number of areas where PETs are already in use which were set out in case studies in the report, with examples summarized here.

There are many examples of current uses of these technologies. For example, TEEs are used in mobile phones to process "touch ID" data (Hoffman et al., 2018). They are also an integral part of secure clouds. The following are some specific examples of where organizations have made use of, or promoted, PETs.

For secure MPC, the first real-world application of Sharemind—which uses MPC—was the analysis of key performance indicators for the Estonian Association of Information Technology and Telecommunications (ITL). The ITL proposed collecting certain financial metrics and analyzing them to gain insights into the state of the sector. The member companies expressed concerns over the confidentiality of the metrics, as they would be handing them out to competitors.

This prompted the use of MPC, with Sharemind developing a solution that was deployed in 2011 (Archer et al., 2018). Seventeen participating companies acted as the input parties who uploaded their financial metrics to three computing parties with the capability to host the Sharemind platform. ITL management acted as the result party, leading the processing and dissemination of results.

Differential privacy has been put into practice by a number of organizations handling large amounts of data, to assess and limit the risk to individuals' privacy. For example, in 2017, the U.S. Census Bureau announced that it would be using differential privacy as the privacy protection mechanism for the 2020 decennial census (Garfinkel et al., 2018). This is having already implemented differential privacy for other services: for example, onTheMap, 2008, an online application developed in partnership with 50 U.S. states, for creating workforce related maps, demographic profiles, and reports. By incorporating formal privacy protection techniques, the Census Bureau will be able to publish a specific, higher number of tables of statistics with more granular information than previously. By fixing a privacy budget for that given set of released publications, the institution can reason mathematically about the risk of disclosure of information relating to a specific individual.

In order to share NHS data securely with multiple teams, while maintaining as much as possible the potential usefulness of the data, NHS Digital have been using a de-identification service employing homomorphic encryption (The Royal Society, 2019). For security reasons, data is de-identified in different "pseudonymization domains" for each different part of an organization. Within one domain, all data with the same base value is replaced with the same "token" (a nonidentifying value). Across domains, the same base value receives different token. Usually, transferring data between domains requires to remove the encryption for the first domain and replace it with the second domain encryption. However, using consistent "tokenization" and partially homomorphic encryption by Privitar Publisher, it

https://doi.org/10.1017/dap.2020.8 Published online by Cambridge University Press

is possible to transform data items between any two domains without revealing the base value, even if they have been de-identified by two instances of the de-identification service using different encryption keys.

This methodology allows the de-identification tool set to be deployed to multiple locations across the NHS and makes any data de-identified by any tool from the de-identification tool set potentially linkable with any other data de-identified by any other tool from the tool set.

In an effort to empower consumers, the UK government promoted midata, a Personal Data Store (World Economic Forum, 2013). Launched in 2011, in partnership with multiple organization, the online portal was designed to provide citizens with access and control over data about them. For example, individuals can access the transactional data for their current account, which they can upload to third party price comparison websites to compare and identify the best value.

Constraints: What are the Technical Limitations of PETs in Practice?

When using PETs, there are trade-offs. Privacy engineers say that PETs incur a cost in terms of "utility." In the context of different technologies, the cost in utility might be of a different nature. It is also important to bear in mind that a number of these technologies are still in a research phase, and technical limitations might therefore evolve in time. For example, with differential privacy adding noise to a dataset entails a loss of some useful information so there is a cost in terms of accuracy. The first organizations that successfully implemented differential privacy have been able to do so because they are handling large amounts of data, and the effect of noise then is less severe in terms of loss of information. At the opposite end of the scale, when handing control over to individual users, one technical challenge is to design user interfaces that are engaging enough and convey the right level of information for citizens to use them effectively.

In the case of PETs where computation happens on encrypted data, such as homomorphic encryption and secure MPC, the main cost to utility is in terms of computation resources (time and computing power) (von Maltitz and Carle, 2018). Encryption can entail a substantial increase in data size, which can cause a major bandwidth problem—this is the subject of ongoing research (Brakerski et al., 2011).

The use of secure hardware has its own technical limitations. In particular, there are questions around the trustworthiness of the hardware. Many "side-channel" attacks are possible, especially on the cloud which is a shared environment (side-channels include caches, memory, disk, etc.). There are side-channels based on speculative execution, affecting certain processors (e.g., Spectre attacks) (Kocher et al., 2018).

In order to negotiate these trade-offs, users need to have a clear idea of what information or value they are trying to protect, and they need to determine the potential benefits and costs of different PETs so that systems can be optimized for this. It is, for example, important to consider the financial cost associated with enforcing a given trust model, in particular if a trusted authority needs to be appointed.

Limitations: How Far Can PETs Deliver Ethical Use of Data?

The key consideration in the use of PETs as a tool for governing the use of data, is that their use does not in itself automatically make an analysis legal, ethical, or trustworthy. There are a range of risks posed by data analysis, some can be addressed by PETs, others not.

When making use of PETs, we might consider in particular the following kinds of risks posed by data analysis:

1. How much does the analysis reveal about the whole population or group from which the data used for the analysis originated? (This might raise concerns relating fairness and discrimination, or to the privacy of individuals in the population).
2. Does the analysis reveal whether someone or a specific entity is included in the dataset that was used to conduct the analysis?
3. How much does an analysis reveal about sensitive attributes about specific individuals or entities in the dataset?

https://doi.org/10.1017/dap.2020.8 Published online by Cambridge University Press

4. To whom is information revealed and what might they do with it?
5. How sensitive are the input, intermediate values and output of an analysis?

The explanations of the technologies above indicate how the technologies might address these specific kinds of risks. However, many ethical questions arise through the data analysis pipeline, which are not grouped within these particular kinds of questions. In assessing whether data analysis is ethical, we might consider broader concerns, for example, whether the purpose of data use is socially beneficial, whether it might result in disadvantages for certain individuals or groups, whether the data has been collected appropriately, and so on. Implementing PETs can ensure that the methods by which data is used include protection against specific privacy risks, but it has a less direct relationship to these broader ethical concerns, and often involve certain ethical or governance questions being settled in advance of their being used.

For example, a key question in governance of data use is, should we be collecting this data at all in the first place? One of the things PETs may help with is to provide extra scrutiny of this question. Given that the use of a PET incurs certain costs, as set out above, there has to be a significant benefit to collecting and using data, if you intend to use PETs to ensure that analysis of that data is privacy-preserving. So, one of the key questions might concern, not how we use the technologies to protect the data through collection and analysis, but rather focus on whether there is any pragmatic (and also ethical) purpose for getting the data at all.

Moving on to data analysis, use of some of the PETs actively require certain ethical and social questions to have been settled in advance of their being used. For example, when using differential privacy a "privacy budget" has to be set which establishes the acceptable risk that an individual might be identifiable in the output of an analysis—for example, if a specific person could be identified through the statistics published by the U.S. Census Bureau in the example above (Garfinkel et al., 2018). This cannot be set by technology alone and is itself an act of decision making and may be subject to governance. Legal requirements might mean that organizations will have to observe a "minimum" privacy aim, and guidance from regulators might help improve understanding of this.

Furthermore, PETs have the potential to actively enable unethical use of data, by virtue of potentially enabling computation in private. For example, PETs such as MPC might enable companies to misbehave and to form collusions, for example, to set prices or other aspects; some research is addressing this threat (Alwen et al., 2009).

All of this means that there are, in principle, limits to the role of these technologies in governing the use of data, or requirements that certain questions about governing uses of data be addressed separately to the technologies being utilized. They are not a "solution" to a "problem" posed by the need to balance risks and benefits of data-enabled technologies, but they are a tool to be used to put governance in place. As such, there is a need for skilled users and the right business environment and governance frameworks to achieve the desired outcome.

The Road to Adoption: Steps in Enabling Appropriate Uptake and Development of PETs

How do we create these skilled users and good environments? Our report made a number of recommendations about the route to appropriate adoption of PETs. These are set out below, drawing from the original text in the report.

Accelerate Research and Encourage Development and Adoption

First, there is a challenge of developing the technologies in order to address limits created by the current stage of technology development. One way of focusing research is by funders, government, industry, and the third sector working together to articulate and support the development of cross-sector research challenges. Alongside providing continued support for fundamental research on PETs, this can potentially support development of PETs so that they can be applied in instances where there are particular governance needs relating to the ways that data is used, for example, due to particular sensitivities relating to the data.

https://doi.org/10.1017/dap.2020.8 Published online by Cambridge University Press

Government can be an important early adopter, using PETs and being open about their use so that others can learn from their experience. Government departments should consider what existing processing might be performed more safely with PETs and how PETs could unlock new opportunities for data analysis, including opening up the analysis of sensitive datasets to a wider pool of experts while fully addressing privacy and confidentiality concerns.

Supporting Intelligent Users

To enable wider and well-informed adoption, we need to create and support a community of intelligent users—who know what the technologies can and cannot deliver both technically and in terms of meeting ethical requirements.

There is a need for government, public bodies and regulators to raise awareness further and provide guidelines about how PETs can mitigate privacy risks and address regulations such as GDPR. For example, the Information Commissioner's office (ICO) could have a role in providing guidance about the use of suitably mature PETs to help U.K. organizations minimize risks to data protection, and this should be part of the ICO's Data Protection Impact Assessment guidelines. Such guidance would need to cover how PETs fit within an organization's overall infrastructure for governing data use, since the use of PETs in isolation is unlikely to be sufficient.

To give public sector organizations, in particular, the level of expertise and assurance they need to implement new technological applications, a centralized approach to due diligence would be beneficial and help assure quality across the board.

The National Cyber Security Center could act as a source of advice and guidance on the use of suitably mature PETs, as part of a network of expert organizations. Such a network of expertise would support the development and evolution of best practices and also provide access to advice on specific cases of data use or sharing. Ultimately, this could also serve as a point of engagement for academics and industry bodies working in the space and provide a portal from which private sector organizations interested in learning about PETs could access information on existing case studies.

Standards and kitemarks can play a role in quality assurance and increasing "buyer confidence" in PETs. Currently, privacy standards are unclear and guidelines are scarce. Even though there is a lot of research on standards and processes, currently they are not mature enough for cross-sector agreement on best practice.

An Integrated Approach to Governance

Regulators and civil society need to consider how PETs could become part of the data stewardship infrastructure, underpinning governance tools such as "data trusts" and other initiatives for the governance of data use. In the United Kingdom, this means the Department for Digital, Culture, Media, and Sport (DCMS), the Center for Data Ethics and Innovation (CDEI), office for AI, and other bodies coming together to discuss the right role for these technologies as they develop further. If we are to unlock the benefits of data for policy, balancing the use of technologies with the right organizational structures, institutions, and skilled users is important to ensure human flourishing in a data-enabled society.

Acknowledgments. An earlier version of this article was made available for the Data for Policy 2019 Conference. The authors are grateful to the Chair and Working Group of experts who have led the Royal Society's Privacy Enhancing Technologies project and overseen the production of the report on which this article is based, and from which much of the content is drawn: Professor Alison Noble FRS FREng (Chair), Guy Cohen, Professor Jon Crowcroft FRS FREng, Dr Adria Gascon, Marion Oswald, and Professor Angela Sasse FREng. We are also grateful to reviewers for their helpful comments.

Funding Statement. This work received no specific grant from any funding agency, commercial, or not-for-profit sectors.

Competing Interests. The authors declare no competing interests exist.

Authorship Contributions. Conceptualization, N.M. and F.F.; Resources, N.M.; Supervision, N.M.; Writing-original draft, N.M. and F.F.; Writing-review & editing, F.F. and N.M.

https://doi.org/10.1017/dap.2020.8 Published online by Cambridge University Press

Data Availability Statement. Data availability is not applicable to this article as no new data were created or analyzed in this study.

References

Alwen Joël, **Katz Jonathan**, **Lindell Yehuda**, **Persiano Giuseppe**, **shelat abhi and Visconti Ivan** (2009) Collusion-free multiparty computation in the mediated model. In Halevi S (ed), *Advances in Cryptology – CRYPTO 2009. Lecture Notes in Computer Science*, vol. *5677*. Berlin and Heidelberg, Germany: Springer.

Anati Ittai, **Gueron Shay**, **Johnson Simon P and Scarlata Vincent R** (2013) Innovative technology for CPU based attestation and sealing. Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy, HASP 13.

Archer David W, **Bogdanov Dan**, **Lindell Yehuda**, **Kamm Liina**, **Nielsen Kurt**, **Pagter Jakob Illeborg**, **Smart Nigel P and Wright Rebecca N** (2018) From Keys to Databases – Real-World Applications of Secure Multi-Party Computation. Cryptology ePrint Archive: Report 2018/450. Available at https://eprint.iacr.org/2018/450 (accessed 3 May 2019).

Brakerski Zvika, **Gentry Craig and Vaikuntanathan Vinod** (2011) Fully Homomorphic Encryption without Bootstrapping. Available at https://eprint.iacr.org/2011/277.pdf (accessed 5 March 2020).

Garfinkel Simson L., **Abowd John M. and Powazek Sarah** (2018) Your Smartphone Has a Special Security Chip. Here's How It Works. Available at https://www.howtogeek.com/387934/yoursmartphone-has-a-special-security-chip.-heres-how-it-works/ (accessed 5 March 2020).

Hoffman Chris (2018) Your Smartphone Has a Special Security Chip. Here's How It Works. Available at https://www.howtogeek.com/387934/yoursmartphone-has-a-special-security-chip.-heres-how-it-works/ (accessed 5 March 2020).

Kocher Paul, **Genkin Daniel**, **Gruss Daniel**, **Haas Werner**, **Hamburg Mike**, **Lipp Moritz**, **Mangard Stefan**, **Prescher Thomas**, **Schwarz Michael and Yarom Yuval** (2018) Spectre Attacks: Exploiting Speculative Execution. Available at https://spectreattack.com/spectre.pdf (accessed 5 March 2020).

Nissim Kobbi, **Steinke Thomas**, **Wood Alexandra**, **Bun Mark**, **MarcoGaboardi**, **O'Brien David R. and Vadhan Salil** (2018) Differential Privacy: A Primer for a Non-technical Audience. Available at https://privacytools.seas.harvard.edu/files/privacytools/files/pedagogical-document-dp_new.pdf (accessed 5 March 2020).

Player Rachel (2018) Homomorphic Encryption: State of the art and applications. Invited talk at Workshop on Privacy Enhancing Technologies, Royal Society, London, UK. Available at https://rachelplayer.files.wordpress.com/2018/07/homomorphic-encryption-pets-workshop.pdf (accessed 5 March 2020).

The British Academy and the Royal Society (2017) Data Management and Use: Governance in the 21st Century. Available at https://royalsociety.org/topics-policy/projects/data-governance/ (accessed 3 May 2019).

The Royal Society (2019) Protecting Privacy in Practice – The Current Use, Development and Limits of Privacy Enhancing Technologies in Data Analysis. Available at https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/ (accessed 3 May 2019).

Von Maltitz Marcel and Carle Georg (2018) A Performance and Resource Consumption Assessment of Secure Multiparty Computation. Available at https://arxiv. org/pdf/1804.03548.pdf (accessed 19 February 2019).

World Economic Forum (2013) Unlocking the Value of Personal Data: From Collection to Usage. Available at http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf (accessed 5 March 2020).

Cite this article: McCarthy, N. and Fourniol, F. 2020. The role of technology in governance: The example of Privacy Enhancing Technologies. *Data & Policy*, 2: e8. doi:10.1017/dap.2020.8

https://doi.org/10.1017/dap.2020.8 Published online by Cambridge University Press