Protecting privacy in practice

The current use, development and limits of Privacy Enhancing Technologies in data analysis

THE ROYAL SOCIETY

Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis
Issued: March 2019 DES5759
ISBN: 978-1-78252-390-1

This report can be viewed online at:
royalsociety.org/topics-policy/projects/privacy-enhancing-technologies

---

Contents

Foreword

Image
Professor Alison Noble FREng FRS, Chair, Privacy Enhancing Technologies Working Group.

This report comes in the midst of a period of rapid developments in the collection, analysis and use of data. We are becoming ever more aware of the social, research and business benefits of accessing and using the data generated through everyday activities. We need to ensure that when such data is collected and used it is done so for good reasons, in a well-governed way and so that sensitive personal data or valuable commercial data is adequately protected.

Privacy Enhancing Technologies (PETs) offer an avenue for enabling that well-governed access. The evolving role of PETs is in ensuring that, when we have good reasons and the legal and ethical grounds to access and use data, we can do so while protecting that data and the individuals and organisations it relates to. We aim in this report to explore that role and bring it to the attention of those who hold, analyse and use data.

The field of PETs development is likewise moving quickly, and this 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 here 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, our aim here is to help raise awareness of the potential of these technologies so that we can inspire further research into their development, spurred by identifying the opportunities where they can be put into practice. We also aim to highlight their practical and technical limitations and to note that there is no technology that replaces the need for good governance and proper business practice relating to the use of data.

We hope that this report adds to the lively debate on the topic of data use and data governance, and complements other work assessing the technological readiness levels of PETs. Our aim is that it will be an important part of conversations between researchers, government and industry on the future use cases for PETs that can both drive research forward and enable everyone to access social benefits from data.

Professor Alison Noble FREng FRS
Chair, Privacy Enhancing Technologies Working Group

Executive summary

The scale and rate at which data is collected, used and analysed is rapidly increasing, offering significant new and developing benefits to society and the economy. However, realising the full potential of large-scale data analysis may be constrained by important legal, reputational, political, business and competition concerns. These concerns arise because the use of data creates a set of social and ethical tensions and risks: in particular there is a balancing act between realising the benefits of data analysis versus protecting sensitive data and the interests of the individuals and organisations it relates to. The failure to adequately address privacy risks may damage trust and limit the realisation of the benefits that can be delivered by data-enabled technologies.

Certain risks can potentially be mitigated and managed with a set of emerging technologies and approaches often collectively referred to as 'Privacy Enhancing Technologies' (PETs). Whilst cybersecurity is focussed on protecting data so that other people cannot access it, PETs, in data analysis, are focussing on enabling the derivation of useful results from data without giving other people access to all of the data. This nascent but potentially disruptive set of technologies, combined with changes in wider policy and business frameworks, could enable significantly greater sharing and use of data in a privacy-preserving, trustworthy manner. It could create new opportunities to use datasets without creating unacceptable risks. It also offers great potential to reshape the data economy, and to change, in particular, the trust relationships between citizens, governments and companies.

The field of PETs is rapidly evolving. However, currently, many of the most promising tools, whilst having a rich research heritage, are relatively new to real-world applications. As such there remain a number of important unanswered questions: What are concrete trade-offs in real-world applications? How mature are different PETs? What opportunities do they present and what are their limitations? How can government and industry accelerate their uptake and make the most of their potential?

This report provides a high-level overview of current PETs, and the roles that they can play, in order to inform applied data science research and government departments' digital strategies as well as those of business. It also considers how PETs sit within wider governance frameworks that are intended to enable the beneficial use of data in an ethical and well-governed way.

This report also aims to prompt reflection about the use of technology in governance and to encourage regulators to consider new ways to approach privacy risks, including the use of PETs. To this end, this document provides an evidence base – including a set of case studies that capture concrete example uses for each of the five PETs considered in this report – and signposts to further resources.

Finally, this report includes recommendations on how the UK could fully realise the potential of PETs and to allow their use on a greater scale.

The field of PETs development is moving quickly. This report looks at five interrelated and heterogeneous approaches within a broad field and there is no intention to suggest that these particular technologies will develop earlier or get more uptake than others. However, this report is intended to raise awareness of the potential of this diverse field of technologies and approaches and ways that they could be applied, in order to encourage further research into their development and to inform future policy conversations about the development and use of PETs.

Recommendations

RECOMMENDATION 1

Accelerate the research and development of PETs.

Funders, government, industry and the third sector can work together to articulate and support the development of cross-sector research challenges, alongside providing continued support for fundamental research on PETs.

RECOMMENDATION 2

Promote the development of an innovation ecosystem.

UK Research and Innovation (UKRI) have a role in encouraging data-handling companies to engage with the start-ups and scale-ups developing PETs, to support research and early trials. This will help UK investors and businesses realise the extent of the market opportunity for PETs.

RECOMMENDATION 5

Give public sector organisations the level of expertise and assurance they need to implement new technological applications, enable a centralised approach to due diligence, and assure quality across the board.

The National Cyber Security Centre should act as a source of advice and guidance on the use of suitably mature PETs, as part of a network of expert organisations. 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 organisations interested in learning about PETs could access information on existing case studies.

RECOMMENDATION 6

Create the skilled workforce needed to develop and implement PETs.

Funding should be made available so that the capacity to train UK PhD and Master students in cryptography, statistics, systems engineering and software development increases with the level of demand for well-trained, high-calibre candidates. This could be an outcome of the National Cyber Security Programme and the cybersecurity centres of excellence scheme by the Engineering and Physical Sciences Research Council. Universities should consider adding privacy engineering to the curriculum of software engineering and data science courses, treating the need to protect data as core knowledge in data analysis.

RECOMMENDATION 3

Drive the development and adoption of PETs.

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 whilst fully addressing privacy and confidentiality concerns.

RECOMMENDATION 4

Support organisations to become intelligent users of PETs.

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) should provide guidance about the use of suitably mature PETs to help UK organisations minimise 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 organisation's overall data governance infrastructure, since the use of PETs in isolation is unlikely to be sufficient.

RECOMMENDATION 7

Promote human flourishing by exploring innovative ways of governing data and its use that are enabled by PETs.

The Department for Digital, Culture, Media and Sport (DCMS), the Centre for Data Ethics and Innovation (CDEI), Office for AI, regulators and civil society should 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.

Summary table[(a)]

	Trusted Execution Environments	Homomorphic Encryption		
Type of privacy	• Securely outsourcing to a server, or cloud, computations on sensitive data	• Securely outsourcing specific operations on sensitive data • Safely providing access to sensitive data		
Privacy risk addressed	• Revealing sensitive attributes present in a dataset	• Revealing sensitive attributes present in a dataset		
Data protected	• In storage • During computing	• In storage • During computing		
Benefits	• Commercial solutions widely available • Zero loss of information	• Can allow zero loss of information • FHE* can support the computation of any operation		
Current limitations	• Many side-channel attacks possible	• FHE currently inefficient, but SHE* and PHE* are usable • Highly computationally intensive; bandwidth and latency issue • Running time • PHE and SHE support the computation of limited functions • Standardisation in progress		
Readiness level	Product	PHE: Product	SHE: Pilot	FHE: Research – proof of concept
Qualification criteria		• Specialist skills • Custom protocols • Computing resources		

KEY

FHE: Fully Homomorphic Encryption **SHE:** Somewhat Homomorphic Encryption **PHE:** Partial Homomorphic Encryption
PIR: Private Information Retrieval **PSI:** Private Set Intersection

Secure Multi-Party Computation	Differential Privacy	Personal Data Stores (b)
• Enabling joint analysis on sensitive data held by several organisations	• Organisation releasing statistics or derived information – generally an organisation that holds a large amount of data	• Individual managing with whom and how they share data • De-centralising services that rely on user data
• Revealing sensitive attributes present in a dataset	• Dataset or output disclosing sensitive information about an entity included in the dataset	• Undesired sharing of sensitive information
• During computing	• At point of dataset or result disclosure	• At point of collection • During computing (locally)
• No need for a trusted third party - sensitive information is not revealed to anyone • The parties obtain only the resulting analysis or model	• Formal mathematical proof / privacy guarantee • The user can set the level of protection desired, in particular by reasoning about the number of times the data might be queried	• Gives full control to individuals • Removes the risk of attacks on 'honeypots' of centralised data • Analysis can be run locally
• Highly compute and communication intensive	• Noise and loss of information, unless datasets are large enough • Setting the level of protection requires expertise	• Impracticality of individual controlling data sharing with many parties
PSI*, PIR*: Product / Proof of concept – pilot	Pilot	Product
• Specialist skills • Custom protocols • Computing resources	• Specialist skills • Custom protocols • Very large datasets	

(a) This table is intended as a guide to the reader of this report, to help understand the five PETs covered in the report in their current state of development as of March 2019. It is not an exhaustive taxonomy of PETs.

(b) Unlike the other four PETs covered in the report, which are tools for privacy-preserving computation, Personal Data Stores are consumer-facing apps and services 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.

Introduction

PETs allow the derivation of useful insights from data, without requiring full data access.

Background – previous Royal Society reports

The amount of data we generate, collect and use and the power of analysis to draw insights from it are increasing rapidly. This significant change in data-enabled technologies has been the basis for three major Royal Society reports in recent years. *Progress and research in cybersecurity*[1] made the case that trust is essential for growing and maintaining participation in the digital society. Organisations earn trust by acting in a trustworthy manner: building systems that are reliable and secure, and treating people, their privacy and their data with respect. It argued that, as part of this, organisations need to provide credible and comprehensible information to help people understand and assess how secure these systems are.

That report was followed by the Royal Society and British Academy's joint report *Data management and use: governance in the 21st century*[2] which identified a number of social and ethical tensions that arise out of the changing ways that we use data. Several of these relate to the use of (personal or otherwise) sensitive data:

- Making use of the data gathered through daily interaction to provide more efficient services and security, whilst respecting the presence of spheres of privacy.
- Providing ways to exercise reasonable control over data relating to individuals whilst encouraging data sharing for private and public benefit.
- Incentivising innovative uses of data whilst ensuring that such data can be traded and transferred in mutually beneficial ways.

That report recommended a principled approach to resolving these tensions and the need for stewardship of data use. It highlighted that governance challenges go beyond the remit of data protection laws. In line with the report's recommendation that a new stewardship body be created to oversee the whole landscape of data use, several initiatives have been established in the UK. In particular, the UK Government has created a Centre for Data Ethics and Innovation and the Nuffield Foundation has established the Ada Lovelace Institute. Both will have a role in exploring the social, ethical and regulatory issues that arise from new uses of data and the practical means of addressing them. However, the extent to which the tensions identified in the 2017 Royal Society and British Academy report can also be resolved through technological means is a key question for this current project.

The Royal Society *Machine learning: the power and promise of computers that learn by example*[3] report called for a new wave of machine learning research, including technical solutions that can maintain the privacy of datasets, whilst allowing them to be used in new ways by different users. That report referenced differential privacy and homomorphic encryption as promising lines of research. Here we explore these technological approaches, along with others, in more detail. Such technologies and approaches are often collectively referred to as Privacy Enhancing Technologies (PETs).

1. The Royal Society 2016 Progress and Research in Cybersecurity: supporting a resilient and trustworthy system for the UK (see https://royalsociety.org/topics-policy/projects/cybersecurity-research/, accessed 12 February 2019)
2. The British Academy and The Royal Society 2017 Data management and use: Governance in the 21st century. (see https://royalsociety.org/topics-policy/projects/data-governance/, accessed 12 February 2019)
3. The Royal Society 2017 Machine learning: the power and promise of computers that learn by example (see https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf, accessed 12 February 2019)

Purpose

Previous reports all show that data is an important resource and new technologies enable us to use it to significant benefit. However, collecting and using such data creates risks for the data user – including legal, reputational, political, business and competition risks – and can generate privacy concerns for individuals, communities and organisations. This report considers the extent to which PETs provide satisfactory routes through these dilemmas, and offer an optimal outcome, where we can release the value in data whilst protecting its sensitivities. How close are we to achieving this through the use of specific technologies, and which of these tensions cannot be robustly resolved through technological means?

Whilst cybersecurity is focussed on protecting data so that other people cannot access it, PETs are focussing on enabling the derivation of useful results from data without giving other people access to all of the data. Different PETs achieve this in different ways, which are described in section 2.2.

The field of PETs is rapidly evolving; however, many of the most promising tools, whilst having a rich research heritage, are relatively new to real-world applications. As such there remain a number of important unanswered questions: What are concrete trade-offs in real-world applications? How mature are different PETs? What opportunities do they present and what are their current limitations? How can government and industry accelerate their uptake and make the most of their potential? Where is there potential for better take up, and where is there need for caution?

Answering these questions, and in fact understanding PETs themselves, requires bringing together knowledge from multiple fields. This is reflected in the multidisciplinary nature of this Royal Society project on PETs.

Target audience

This report is aimed at an audience that might not have deep technical knowledge of statistics, cryptography, systems security, hardware or other disciplines relevant to the detailed understanding of PETs. This report might, in particular, be of use to those in charge of digital strategies and data protection in the public, private and third sector (eg chief data officers and data protection officers). It is also intended to inform those working in government and third sector bodies concerned with the ethics and governance of data use, in order to consider the extent to which the use of PETs can play a role in data governance frameworks.

Scope

This project has examined the role of PETs in enabling data analysis and extracting value whilst preserving sensitive information, and drawing out the implications for policy and practice. The aims of the project were to explore the interplay between the following questions:

- What are the ethical and social issues at stake?
- What is mathematically possible and what is technically feasible? In particular, the project considered how privacy can be defined mathematically, and what is theoretically possible, alongside practical questions of implementation.
- What business models and incentive systems can deliver these technologies?

Chapter one looks at some of the drivers for the use of PETs, in particular the types of risks associated with the analysis of personal data, and the way current regulation in this domain may encourage the uptake of PETs. Chapter two explores opportunities for PETs-enabled data analysis and considerations for the use of PETs as a whole, before taking a deeper dive into a selection of five PETs. Chapter three brings together the rationale for the recommendations made in this report.

'PETs' is an umbrella term covering a broad range of technologies and approaches – from a piece of tape masking a webcam to advanced cryptographic techniques[4,5]. This project did not consider the role of PETs in private communications. We focus on 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: homomorphic encryption, trusted execution environments, secure multi-party computation, differential privacy, and personal data stores.

They represent a quite diverse set of approaches highlighting the different ways that distinct communities – such as systems security/hardware, statistics and cryptography – are tackling similar problems.

We recognise that some of these are not technologies *per se*, but rather concepts or definitions which can be fulfilled by technological means; however, it is common practice to use 'PETs' as shorthand for the broader field. Where possible, we draw out how these five PETs may be combined with one another or with other technologies. For example, blockchain[6], which is not a PET in itself, can actually be made more privacy-preserving using PETs (see Case study 2 section 2.2.2). Additionally, section 2.3 summarises how these and other PETs can support privacy-preserving machine learning – enabling the use of a powerful form of data analysis.

Case studies have been used to help illustrate these technologies in practice, suggesting the potential and relevance of different PETs to a range of sectors and application areas (see section 2.2). Sharemind is a commercially available distributed database system, developed by Cybernetica, using secure multi-party computation to enable the safe sharing of sensitive information between companies. Microsoft has developed CoCo, a confidential blockchain framework where trusted processors add confidentiality, performance and governance to blockchain. NHS Digital is using Privitar's de-identification product, Privitar Publisher, which uses homomorphic encryption to enable the safer sharing and linkage of data between authorised parties. The US Census Bureau has used differential privacy and is planning on using it on a large scale for the release of statistics from the upcoming 2020 census. Finally, CitizenMe is a phone app, and an example of a personal data store, that enables users to choose what data to share and with whom.

4. ENISA 2014 Privacy and data protection by design – from policy to engineering (see https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design, accessed 8 February 2019)
5. Office of the Privacy Commissioner of Canada 2017 Privacy Enhancing Technologies – A Review of Tools and Techniques (see https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/, accessed 12 February 2019)
6. Blockchain is an open, distributed ledger that can record transactions between several parties efficiently and in a verifiable and permanent way. See Introduction, Key terms and definitions.

Methodology

This report was informed by a series of conversations with a broad range of stakeholders from academia, industry, government and civil society, two interdisciplinary workshops on 16 May 2018 and 18 July 2018 (on the business and societal needs for PETs, and trends affecting their uptake; and on the state of play of research and implementation, respectively), and consideration by an expert Working Group. The report was reviewed by expert readers and peer reviewers. Full details of the workshop speakers, Working Group members, expert readers and peer reviewers are provided in the Appendix.

Key terms and definitions

This report draws on some concepts and models from business, technology and data analytics. Here is a concise glossary of 23 key terms used:

B2B: Business-to-business; application or service provided by a business to another business.

B2C: Business-to-consumer; application or service provided by a business to an individual.

Blockchain: an open, distributed ledger that can record transactions between several parties efficiently and in verifiable and permanent way. Blockchain is not a PET.

Derivation: part of a de-identification process where the granularity of a data item is reduced (eg date of birth to year of birth). This is an irreversible activity. It is also known as sub-sampling.

Differential privacy: security definition which means that, when a statistic is released, it should not give much more information about a particular individual than if that individual had not been included in the dataset. The differential privacy definition allows one to reason about how much privacy is lost over multiple queries (see privacy budget).

Epsilon: see privacy budget.

FHE: Fully homomorphic encryption (FHE) refers to encryption schemes where it is possible to compute any polynomial function on the data, which means both additions and multiplications.

Homomorphic encryption (HE): a property that some encryption schemes have, so that it is possible to compute on encrypted data without deciphering it.

Integrity: confidence that data is not tampered with.

MPC: see secure multi-party computation.

Noise: noise refers to a random alteration of data/values in a dataset so that the true data points (eg personal identifiers) are not as easy to identify.

Personal Data Store (PDS): systems that provide the individual with access and control over data about them, so that they can decide what information they want to share and with whom.

Partial Homomorphic Encryption (PHE): encryption supporting only additions or only multiplications (also referred to as additive homomorphic encryption and multiplicative homomorphic encryption).

Privacy budget, or differential privacy budget, or epsilon: quantitative measure of by how much the risk to an individual's privacy may increase by, due to that individual's data inclusion in the inputs to the algorithm.

Privacy Enhancing Technologies (PETs): an umbrella term covering a broad range of technologies and approaches that can help mitigate security and privacy risks.

Private Information Retrieval (PIR): an MPC protocol allowing a user to query a database whilst hiding the identity of the data retrieved.

Private Set Intersection (PSI): secure multi-party computation protocol where two parties compare datasets without revealing them in an unencrypted form. At the end, each party knows which items they have in common with the other. There are some scalable open-source implementations of PSI available.

Redaction: part of a de-identification process where an identifier (such as name) is deleted;

Secure Multi-Party Computation (SMPC or MPC): 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.

Somewhat Homomorphic Encryption (SHE): encryption supporting a limited number of both additions and multiplications on encrypted data.

Tokenisation: consistently obscuring a data item (eg an NHS number) by replacement with a token, such as a regular expression, as part of a de-identification process. This is a reversible activity.

Trusted Execution Environment (TEE): isolated part of secure processors that allow the isolation of secret code from the rest of the software that is running on a system in order to achieve confidentiality of the data. Trusted execution environments are also known as secure enclaves.

Zero-knowledge proof: method by which one party can prove to another party that they know a value *x*, without conveying any information apart from the fact that the statement is true.

Image © scanrail.

Chapter one
Data sensitivity and protections: what are the issues at stake?

Left
© filadendron.

Data sensitivity and protections: what are the issues at stake?

Data might be considered sensitive for a range of reasons, including personal privacy, commercial sensitivity or national security.

This section looks at some of the drivers for the use of PETs, in particular the types of risks associated with the analysis of personal data, and the way current regulation in this domain may encourage the uptake of PETs.

1.1 Data sensitivity

Growing computing power, the volume of information generated every day, and their wider availability is making both benevolent applications and attacks rapidly more powerful. What seemed inconceivable in the past may now become possible. For example, using a smartphone comes with the risk of a profile containing sensitive attributes being created about you without your full knowledge[7]; and information about you can be inferred from your contacts[8]. Also, in the case of machine learning models, which are usually trained using a large dataset, there is an expectation that the training dataset cannot be recovered from the trained model, but this is not true in all cases[9]. As data collection and use is expanding, the analysis of available datasets can make it possible to identify individuals and information about them, therefore data privacy management is also about identity management.

Personal privacy is not the only concern, data might be commercially sensitive or related to national security, for example. Individuals or organisation might be keen to share data but want to restrict whom they are sharing information with and what information they want to share. PETs can help achieve such restrictions in different ways.

An additional need for new PETs is being driven by cloud computing, with the need for the data controller to give the data processor specific and limited capabilities.

People and organisations are becoming more aware of the individual and group harms caused by misuse of data and data breaches – for example the Facebook and Cambridge Analytica scandal or the Equifax breach[10,11].

7. New York Times 2017 Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret (see https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html, accessed 12 February 2019)
8. Such JM and Criado R. 2018 Multiparty Privacy in Social Media. Communications of the ACM 61, 74–81. (see https://cacm.acm.org/magazines/2018/8/229766-multiparty-privacy-in-social-media/fulltext, accessed 12 February 2019)
9. Veale M *et al* 2018 Algorithms that remember: model inversion attacks and data protection law. Phil. Trans. R. Soc. A 376. (see http://rsta.royalsocietypublishing.org/content/376/2133/20180083, accessed 12 February 2019)
10. Information Commissioner's Office 2018 ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information (see https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/, accessed 12 February 2019)
11. Information Commissioner's Office 2018 ICO Credit reference agency Equifax fined for security breach (see https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/credit-reference-agency-equifax-fined-for-security-breach/, accessed 12 February 2019)

It should be emphasized that the use of PETs does not in itself automatically make an analysis legal, ethical or trustworthy. Many ethical questions arise through the data analysis pipeline, eg 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 does not tell us anything about these broader ethical concerns.

1.2 Privacy risks and the data analysis pipeline

To understand how PETs protect against privacy risks it is important to acknowledge that 'privacy' is a term which has many different meanings[12,13]. Privacy has been referred to in legal concepts such as the right to be left alone, data protection rights, rights to control or 'own' personal data, secrecy, anonymity, and the right to respect for private and family life[14]. To consider the way PETs can mitigate privacy risks that stem from data analysis, it is necessary to establish at the outset different kinds of privacy risk. First of all, for any given data analysis, one might ask generally how much sensitive information it risks revealing. This question has several possible angles and interpretations:

- How much does the analysis reveal about the whole population or group from which the data used for the analysis originated? (Note that there is a definitional issue here: some might argue that this question relates rather to fairness and discrimination, and others might point out that it also affects the privacy of individuals in the population)
- Does the analysis reveal whether someone or a specific entity is included in the dataset that was used to conduct the analysis?
- How much does an analysis reveal about sensitive attributes about specific individuals or entities in the dataset?
- To whom is information revealed and what might they do with it?
- How sensitive are the input, intermediate values and output of an analysis?

Secondly, it is also important to consider and test whether or not a system presents vulnerabilities. Cryptographers and other experts have set goals for security and privacy which can then be assessed. The security engineering community specified a set of testable goals which systems can be assessed against, in particular: confidentiality, integrity and availability (CIA). Echoing this triad of security requirements, the European Network and Information Security Agency (ENISA), alongside others, have proposed the following testable goals to be considered in privacy engineering: ENISA proposed the goals of unlinkability[15], transparency, and intervenability[16];

12. *Op. Cit.* 2
13. The Israel Academy of Sciences and Humanities and The Royal Society 2019 Israel-UK Privacy and Technology workshop – note of discussions (see https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/, accessed March 2019)
14. Article 8, European Convention on Human Rights (see https://www.echr.coe.int/Documents/Convention_ENG.pdf, accessed 12 February 2019)
15. 'Unlinkability of two or more items of interest means that within the system (comprising these and possibly other items) from the attacker's perspective, these items of interest are no more and no less related after his observation than they are related concerning his a-priori knowledge' - Pfitzmann A and Hansen M. 2005 Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology (see https://www.freehaven.net/anonbib/cache/terminology.pdf, accessed 8 February 2019)
16. *Op. Cit.* 4

in the US, the National Institute of Standards and Technology (NIST) proposed predictability, manageability and disassociability[17].

Thirdly, an interesting proposition from academia is the development of formal mathematical approaches to privacy to support a robust connection between regulation and practical enforcement[18]. Formalism potentially allows a shift from informal requirements and goals ('obey law', 'be ethical') towards quantifiable measurement of privacy enforcement (such as the 'privacy budget' parameter in differential privacy (section 2.2.4)). However, this would require matching legal and mathematical definitions, as demonstrated by Kobbi Nissim and colleagues (2018)[19]. It is also important to recognise that technology is not value-neutral and also to scrutinise how governance-sensitive choices are made – see in particular the subsequent discussion around setting the value of the 'privacy budget' parameters when using differential privacy (section 2.2.4). In any case, technical solutions need to be grounded in the legal framework.

Finally, it is useful to consider the risks and harms associated with each stages of a typical data analysis pipeline – collection, processing and dissemination – and where PETs may be applied. Different types of potentially problematic actions in the data analysis pipeline can result in privacy harms (see Box 1 and Figure 1, focusing on harms to individuals). Note that harms and actions are distinct. For instance, different actions (eg 'identification' or 'exposure') can result in the same harm (eg distress)[20]. Certain tools, such as PETs, can reduce the chance of specific problematic data actions resulting in a harm, but they do not necessarily stop other actions which could result in the same or different types of harm.

17. National Institute of Standards and Technology 2017 An Introduction to Privacy Engineering and Risk Management in Federal Systems (see: https://doi.org/10.6028/NIST.IR.8062, accessed 12 February 2019)

18. Nissim K and Wood A. 2018 Is Privacy Privacy? *Phil. Trans. R. Soc. A* 376. (see https://doi.org/10.1098/rsta.2017.0358, accessed 12 February 2019)

19. Nissim K *et al*. 2018 Bridging the gap between computer science and legal approaches to privacy. *Harvard Journal of Law & Technology 31*. (see https://privacytools.seas.harvard.edu/publications/bridging-gap-between-computer-science-and-legal-approaches-privacy, accessed 12 February 2019)

20. *Op. Cit.* 17

BOX 1

Daniel Solove's taxonomy of privacy

Different types of actions in a data analysis pipeline can result in privacy harms. One way of understanding these different harms is through Daniel Solove's taxonomy of privacy[21]. Focusing on the analysis of personal data, problematic data actions include:

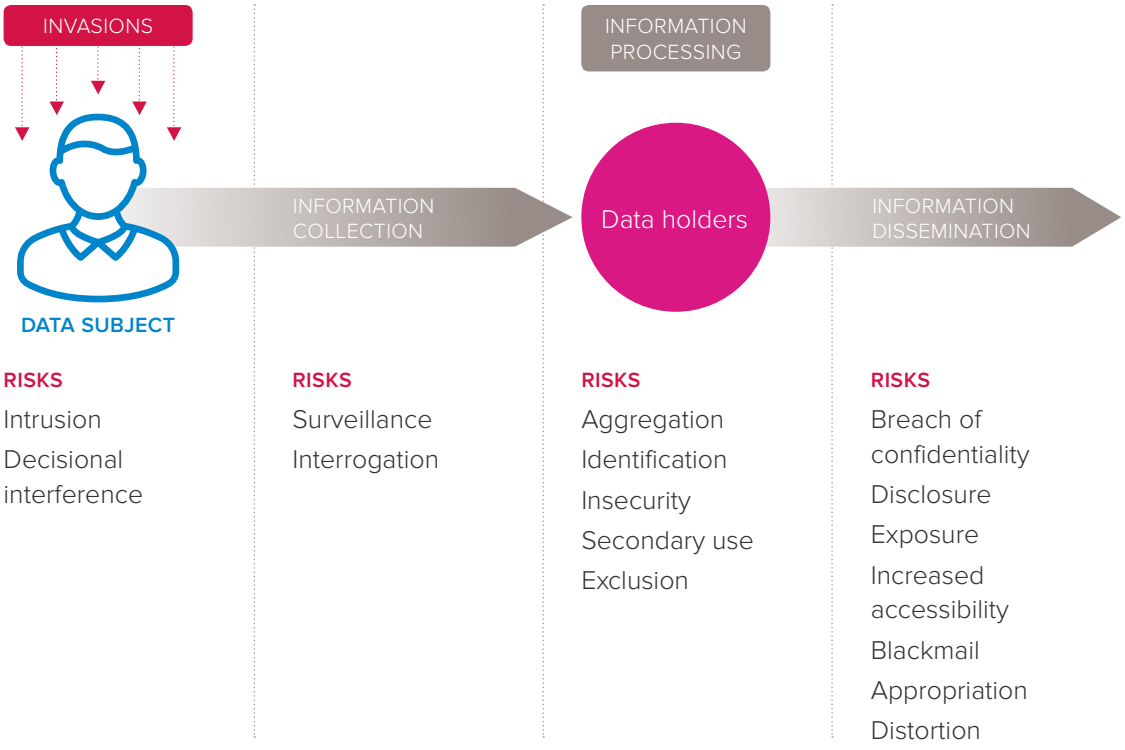
- 'Aggregation', the gathering together of information about a person. A piece of information here or there is not very telling. But when combined together, bits and pieces of data begin to form a portrait of a person. The accumulation of data and increasing power of analytics mean that aggregation is easier and more insightful than ever before. This presents both potential benefits (eg personalised recommendations by online retailers) and potential harms (eg potential distress or other harms resulting from a profile containing sensitive attributes being created about an individual without their full knowledge)[22].
- 'Identification' is connecting data to a specific individual. An obvious benefit is identity verification. Identification can result in harm if an individual would rather stay anonymous. Of note, aggregation can lead to the identification of an individual, by linking 'de-identified' data (where personal identifiers have been removed) and other data.
- 'Insecurity' is a problem caused by the way our information is handled and protected. It might involve glitches, a lack of cybersecurity, abuses and illicit uses of information. One major harm that can result from insecurity is identity theft.
- 'Exclusion' refers to the failure to provide individuals with notice and input about their records. Insecurity and exclusion can create a sense of vulnerability, uncertainty and powerlessness amongst individuals from whom the data comes.
- 'Disclosure' occurs when certain information about a person is revealed to others. Disclosure can threaten people's security and might limit their freedom of association and expression.
- 'Exposure' involves the exposing to others of certain physical and emotional attributes about a person. Such exposure risks creating embarrassment and humiliation.
- 'Intrusion' involves invasions or incursions into one's life, whether in the physical or digital space. For example, spam and junk mail are intrusions that sap people's time.

21. Solove DJ. 2006 A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154, 477–560. (see https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf, accessed 12 February 2019)

22. *Op. Cit.* 7

FIGURE 1

Mapping of data lifecycle stages and problematic actions presenting a risk to privacy.



Source: Solove DJ. 2006 A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154, 477–560. (see https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf, accessed 12 February 2019)

1.3 The legal context for data processing: personal data and the GDPR

Considering how technologies can be used as a means of governance is the essence of the 'data protection by design and default' approach required by the General Data Protection Regulation (GDPR), which came into force in May 2018 and introduced new protections across the European Union. Following many of the principles at the heart of the GDPR, new data protection regimes are being adopted across the world. Such regulatory change builds a fresh case for the development and uptake of PETs, which could overcome their apparent 'failure' to go mainstream[23]. This report is not intended to provide a comprehensive analysis of all relevant legal frameworks with regards to the processing of personal or otherwise sensitive data (such as those mentioned in section 1.2) – rather we take a closer look at the GDPR in the context of the protection of personal data.

The 'data protection by design and default' approach introduced by the GDPR includes a number of data protection principles, including data 'minimisation' – to collect and store only the minimum required amount of data for the

23. *Op. Cit.* 5

purpose of a given application. An increased emphasis on data minimisation could lead to a cultural shift within the organisations that handle data. In particular, the GDPR challenges business models that involve data hoarding and constitutes a push for business models that involve privacy protection. At the moment there is a general culture of accumulating data and working out purpose and use later. However, there might be a counter-trend towards more focused data collection[24] based on specific variables of interest and specific hypotheses to be tested. This move could potentially encourage the development of data-enabled technologies that utilise small, high quality data, rather than relying on very large datasets. This in turn could open up new opportunities.

The regulation also recommends that data users employ 'safeguards' to ensure their processing of personal data is compliant with the regulation. Personal data is information that relates to an identified or identifiable individual[25]. Organisations wanting to adopt a privacy-preserving approach may often ask for a solution that transforms a dataset containing personal data into an anonymised one, so that they can perform computation on it. A key approach to do so is pseudonymisation, a data management procedure by which personally identifiable information fields are replaced by artificial identifiers. However, there have been several studies showing that pseudonymised datasets could in certain cases be re-identified, by linking them with other data[26]. *k*-anonymisation is an alternative approach where certain variables in a dataset are suppressed or generalised in a manner that ensures the information from any single individual cannot be distinguished from at least *k-1* other individuals in the dataset. But this approach can still lead to sensitive attribute disclosure in some cases.

This has prompted the Information Commissioner's Office to consider ways it could address data that is not *per se* 'personal data' but might still contain sensitive information[27]. New approaches, such as the PETs described in this report, need to be considered as alternative safeguards.

The GDPR places an increased emphasis on accountability and, regarding consent for data processing in particular, it requires more specificity about the purposes that data is used for. Personal data stores, one of the PETs considered in more detail in chapter two, have been proposed as one solution to help the 'data subject' manage granular consent and provide individuals with control over their data.

Finally, GDPR also introduces mandated data 'portability' – a data subject has the right to receive data about them from the controller, in a structured, commonly used, and machine readable format. This could, for instance, help consumers switch services and this might create markets, such as a service-switching market. Could PETs be part of the solution and help share consumer data in a secure way?

Considering how technologies can be used as a means of governance is the essence of the 'data protection by design and default' approach required by the GDPR.

24. The Economist 2018 Can the EU become another AI superpower? (see https://www.economist.com/business/2018/09/22/can-the-eu-become-another-ai-superpower, accessed 12 February 2019)

25. See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ (accessed 12 February 2019)

26. Narayanan A and Shmatikov V. 2008 Robust De-anonymization of Large Sparse Datasets (see https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf, accessed 12 February 2019)

27. The British Academy and The Royal Society 2017 Data management and use: Governance in the 21st century – Priorities for data governance: discussions at a British Academy and Royal Society seminar on 16 October 2017. (see https://royalsociety.org/topics-policy/projects/data-governance/, accessed 12 February 2019)

Chapter two
PETs today: capabilities and limitations

Left

PETs today: capabilities and limitations

PETs can reduce the privacy risk of existing processing, reduce the friction of processing currently deemed too high risk, and create entirely new opportunities to access and use data.

This section explores the opportunities for PETs-enabled data analysis and considerations for the use of PETs as a whole, before taking a deeper dive into a selection of five PETs. Finally, section 2.3 shows how different PETs might be used to achieve one type of analysis, focusing on the example of machine learning.

The overviews given here provide a snapshot of this emerging area with the understanding that a number of new methods are being proposed and are developing at different rates, with the five selected PETs presented as examples of some of the main classes of methods at the current time. Some of these technologies are emerging into the basis of real-world applications, and the case studies included demonstrate their potential for use; whilst others remain some distance away from practical use and uptake, being at the point of fundamental research. This section shows what is possible, whilst giving a sense of the technical and practical limitations of the technologies at their current stage of development.

2.1 PETs and privacy-preserving data analysis

2.1.1 What are the potential opportunities?

At a high level, PETs can reduce the privacy risk associated with existing processing, reduce the friction of processing which otherwise would not be able to take place for being deemed too high risk, and create entirely new opportunities to access and use data which had not previously been thought of. Once developed to the appropriate level of technical maturity, PETs could enable secure and controlled data access, and a range of new data-enabled products or services, in circumstances that would otherwise raise legal, reputational, political, business or competition concerns due to the potential for privacy risks. In this respect, PETs may be an enabler of data use, rather than an additional layer of cybersecurity defence. Here we discuss some of the potential benefits offered by the use of PETs.

A system of certification for PETs could enable organisations using them to provide assurance that they are sharing and processing data in a secure, privacy-preserving way, assuming the appropriate standard for the certifications could be agreed by relevant stakeholders. In so doing, these technologies could help open up datasets to more external parties, and thus encourage innovation. PETs could, for example, enable government departments to share data with one another to allow analysis that would provide benefits to citizens through improved services – for example they could support the sharing of data between the National Health Service (NHS) and the Department for Work and Pensions (DWP) for administering health-related benefits.

In addition, PETs may help remove the need for government departments and agencies to hold large datasets in places of restricted access and only perform analysis *in situ*, which is currently the case, for instance, for Department for Education data[28]. Instead, PETs might allow secure cloud-based computation. They could also enable wider use of distributed processing on data stored on citizens' smartphones and other connected objects, thus saving the need for servers that could be subject to security breaches[29].

Within organisations, PETs could support cross-team working, by enabling different internal teams to work on data that they otherwise would not be able to match or view because of data protection rules. In academia, the safe sharing of data with the research community could also lead to innovations benefiting citizens. However, this would not detract from the need to assess whether it is legal or ethical to carry out an analysis or give access to the data in the first place[30].

PETs could also help commercial organisations introduce new business models and use consumer data in new ways. Personal data stores are an interesting example of such an application (see section 2.2.5).

2.1.2 What sort of protections do PETs provide?

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 (see Summary table), such as:

- securely providing access to private datasets;
- enabling joint analysis on private data held by several organisations;
- securely out-sourcing to the cloud computations on private data;
- de-centralising services that rely on user data.

It is worth noting that some PETs might be better suited for use by organisations (business-to-business; B2B), and others for use by individuals (business-to-consumer; B2C). For example, cloud providers may want to employ secure hardware or techniques based on encryption to protect code and data on their platform, whereas individuals may benefit from using personal data stores and other PETs designed for individuals[31].

The use of PETs would not detract from the need to assess whether it is legal or ethical to carry out an analysis or give access to the data in the first place.

28. See https://www.gov.uk/guidance/how-to-access-department-for-education-dfe-data-extracts (accessed 12 February 2019)

29. The Royal Academy of Engineering 2018 Internet of Things: realising the potential of a trusted smart world (see https://www.raeng.org.uk/publications/reports/internet-of-things-realising-the-potential-of-a-tr, accessed 12 February 2019)

30. For example, in 2017 the Digital Economy Act provided the Office for National Statistics (ONS) with permissive and mandatory gateways to receive data from all public authorities and Crown bodies, and new powers to mandate data from some UK businesses. In limited circumstances data held by ONS may also be shared with the devolved administrations solely for statistical purposes. (see https://www.ons.gov.uk/aboutus/transparencyandgovernance/lookingafterandusingdataforpublicbenefit/policies, accessed 12 February 2019)

31. *Op. Cit.* 5

The choice of a PET requires considering forms of control or oversight in any given system, and what attacks that system might be vulnerable to.

The choice of a PET also requires considering forms of control or oversight, or trust models. In any given system, whether centralised, decentralised or distributed[32], trust depends on the context and who 'sees' unencrypted data. Most of the PETs discussed in this report have their origins in the field of cryptography, which often frames challenges in terms of 'attacker' models (or threat models), ie what attacks a certain system might be vulnerable to. This has implications for the ways in which these PETs manage data access, for example:

- secure multi-party computation specifically removes the need for a central trusted authority, with which parties would otherwise need to share information (section 2.2.3, Figure 5);
- centralised and distributed differential privacy (section 2.2.4) come with different trust models: in centralised (aka 'global') differential privacy, noise[33] is added upon release of the output which means trust lies in a central organisation, whilst in distributed (aka 'local') differential privacy noise is added at the time of data collection. In other words, the risk of sensitive information being disclosed in the case of an attack on the central authority is lower if that organisation uses distributed differential privacy;
- personal data stores provide individuals with the means to choose and control who they want to trust with the data they generate. Also, they might offer the possibility to process data locally rather than sending the raw data to a central authority, whose concentration of data makes it an attractive target for hackers (also known as a 'honeypot').

Finally, it should be noted that there is a difference between ways of specifying privacy definitions and mechanisms for achieving them. Because of the complexity of the context in which PETs operate, guaranteeing privacy in computing requires a solid mathematical definition, often referred to as a 'security definition' or a 'privacy definition'. Differential privacy (section 2.2.4) is an example of a privacy definition – it is a way of measuring privacy. Each privacy definition might have different mechanisms for being achieved.

For example, there might be several different ways of injecting random noise into a computation that would result in different 'differentially private' algorithm. These algorithms would all satisfy the definition of differential privacy, and thus offer the same protection, but some might be more accurate than others, resulting in different scalability trade-offs.

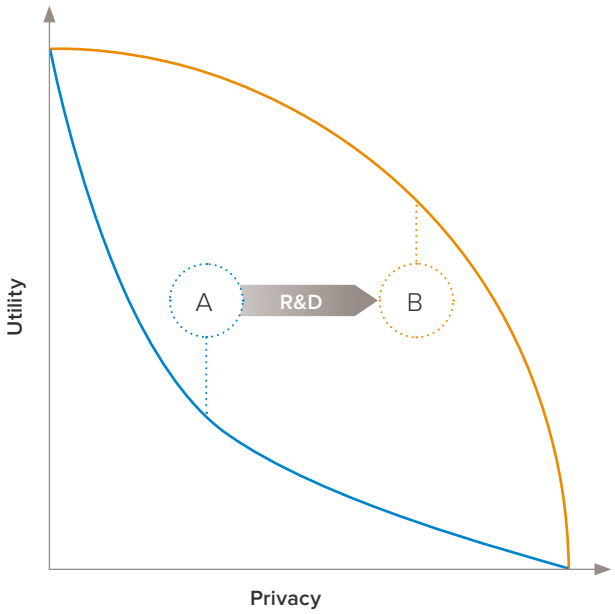
2.1.3 The cost of using PETs – accuracy, utility and financial costs

How else do PETs alter data applications?
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. 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. In the case of PETs where computation happens on encrypted data, such as homomorphic encryption and secure multi-party computation, the main cost to utility is in terms of *computation resources* (time, computing power).

32. Goyal S. 2015 Centralized vs Decentralized vs Distributed (see https://medium.com/delta-exchange/centralized-vs-decentralized-vs-distributed-41d92d463868, accessed 12 February 2019)
33. Noise here refers to a random alteration of data values in a dataset so that the true data points (eg personal identifiers) are not as easy to identify. See Introduction, Key terms and definitions.

FIGURE 2

Privacy and utility function. Whilst utility is a multi-dimensional and nuanced concept, this diagram is a simplification to illustrate how research and development (R&D) on a PET may change the way it affects both privacy and utility.



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 optimised 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.

It is worth noting that legal requirements might mean that organisations will have to observe a 'minimum' privacy aim, and guidance from regulators might help improve understanding of this.

Figure 2 illustrates how general developments in PETs can help achieve better utility-privacy trade-offs, moving from A to B in the plot. Here, developments could be of a theoretical or engineering nature. For example, better provable bounds for sufficient noise to achieve differential privacy would improve accuracy at no cost to privacy, while further implementations of existing homomorphic encryption shemes would improve utility in terms of running time.

2.1.4 Readiness levels and efficacy assessment

How close are PETs to going mainstream?
PETs have different levels of maturity or 'readiness', which has been described as an expression of "whether a PET can be deployed in practice on a large scale, or whether it can only be used within a research project to build upon and advance the state of the art in privacy protection"[34.35], (for the readiness levels of the PETs this report focuses on, see Summary table). These readiness levels provide an indication, based on current knowledge and status of development, of how much investment is likely to be required to create a PET from initial idea, through to it being deployed to it finally becoming an outdated technology (see Box 2).

The efficacy of a PET can be assessed based on whether sensitive information is effectively protected. In order to make this assessment, before a solution is deployed, it is important to consider who the 'attacker' might be and what prior information they might have.

BOX 2

PETs readiness levels, as defined by the European Network and Information Security Agency (ENISA):

Idea: Lowest level of readiness. The PET has been proposed as an idea in an informal fashion, eg written as a blog post, discussed at a conference, described in a white paper or technical report.

Research: The PET is a serious object of rigorous scientific study. At least one, preferably more, academic paper(s) have been published in the scientific literature, discussing the PET in detail and at least arguing its correctness and security and privacy properties.

Proof-of-concept: The PET has been implemented, and can be tested for certain properties, such as computational complexity, protection properties, etc, ie 'Running code' is available, but no actual application of the PET in practice, involving real users, exists, nor is the implementation feature complete.

Pilot: The PET is or has recently been used in practice in at least a small scale pilot application with real users. The scope of application, and the user base may have been restricted, eg to power users, students, etc.

Product: The highest readiness level. The PET has been incorporated in one or more generally available products that have been or are being used in practice by a significant number of users. The user group is not *a priori* restricted by the developers.

Outdated: The PET is not used anymore, eg, because the need for the PET has elapsed, because it is dependent on another technology that is not maintained anymore, or because there are better PETs that have superseded that PET.

34. ENISA 2016 Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies. (see https://www.enisa.europa.eu/publications/pets, accessed 12 February 2019)

35. *Op. Cit.* 4

2.2 Example PETs, capabilities and limitations

This section focuses on a selection of five technology areas of a different nature and collectively known as PETs. These five PETs were identified during the scoping of the project as being particularly promising to enable privacy-preserving computation. They represent a quite diverse set of approaches highlighting the different ways that distinct communities – in particular systems security/hardware, statistics and cryptography – are tackling similar problems. For each, this section provides a brief overview of:

- definition and use case – examples of the types of problems they might be used to solve, including which privacy risk is being addressed;
- variations;
- history;
- current challenges and limitations;
- overall readiness assessment and considerations for use;
- case study.

Summary table on pages 8 – 9.

It is worth noting that the five PETs discussed in detail will be used in conjunction with other existing, effective and mature technologies, for example: encryption (both public key and symmetric), digital signatures, and more generally techniques that provide authentication, confidentiality and integrity. Whilst these classical cryptographic techniques will typically do the heavy lifting with regard to security, they do not provide all the security capability that is needed. In addition to the five techniques focused on in this report, there are other available techniques, examples being group signatures, attribute based encryption, commitment schemes and direct anonymous attestation – techniques with varying degrees of maturity but which may also have various parts to play in the toolkit needed for the protection of data.

3.2.1 Homomorphic Encryption

Definition and use case

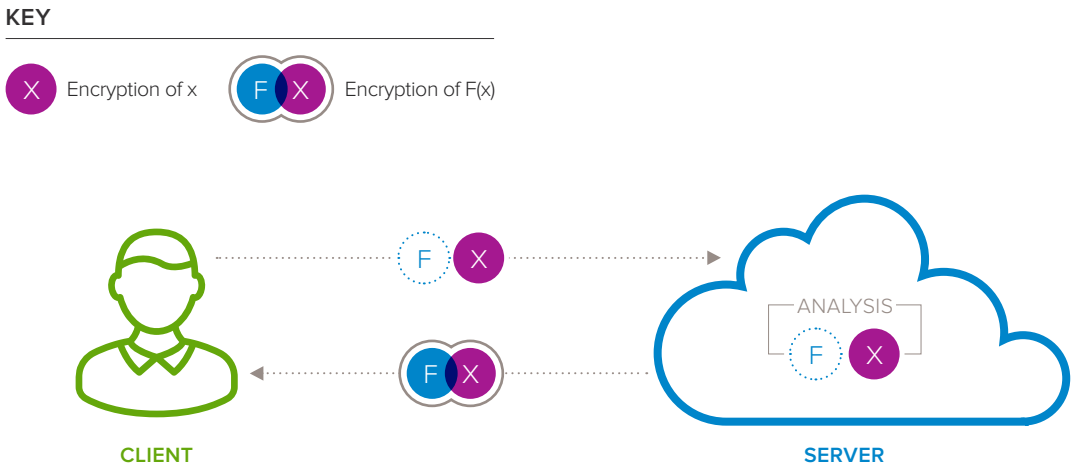
Homomorphic encryption is a form of encryption that allows certain computations on encrypted data, generating an encrypted result which, when decrypted, matches the result of the same operations performed on the data before encryption. It might be used in particular to securely outsource certain specific operations on sensitive data to the cloud, or to another third party organisation. It can also be used in combination with other PETs to safely share data (see for instance Case Study 1).

Homomorphic encryption can be used to analyse data in circumstances where all or part of the computational environment is not trusted, and sensitive data should not be accessible. It is applicable where the computation required is known and relatively simple. Homomorphic encryption provides confidentiality and can be used to address the problems of ‘insecurity’ and ‘exposure’ (see Box 1), and the risk of revealing sensitive attributes related to individuals or organisations, in a dataset or output.

Figure 3 illustrates how homomorphic encryption can be used by a client (data owner) to carry out an analysis (function F) on data (x) using cloud-based computation. In this example, the client wishes to make use of the cloud to save resources, but does not want to share their data with a server or environment that they do not trust. Instead, they wish to share the data in encrypted form. Homomorphic encryption can be used in these circumstances to encrypt the data so that the server does not need access to the secret key to perform the analysis, and the client, owning the secret key, can decrypt the output sent by the server to obtain the result they wanted.

FIGURE 3

Homomorphic encryption, depicted in the context of a client-server model. The client sends encrypted data to a server, where a specific analysis is performed on the encrypted data, without decrypting that data. The encrypted result is then sent to the client, who can decrypt it to obtain the result of the analysis they wished to outsource.



Variations

There are a number of variations of homomorphic encryption methods, which can be used in different ways. Fully homomorphic encryption (FHE) refers to encryption schemes where it is possible to compute any polynomial function on the data, which means an unbounded number of additions and multiplications. However, FHE, which is still at the point of research, is inefficient in practice and this is why schemes that can achieve a limited number or type of operations are more commonly used – so-called Somewhat Homomorphic Encryption (SHE) or Partially Homomorphic Encryption (PHE). SHE is encryption supporting a limited number of both additions and multiplications on encrypted data, fixed in advance; PHE is encryption supporting only additions or only multiplications (also referred to as additive homomorphic encryption and multiplicative homomorphic encryption). Homomorphic encryption can enable other PETs such as secure multi-party computation (section 2.2.3).

History

Homomorphic encryption was first posed as an open problem in 1978[36]. It was realised early on that classical group theory based public key encryption naturally has homomorphic properties. On this basis PHE schemes were proposed over the following 30 years. The first FHE scheme was only proposed in 2009 by Craig Gentry[37], resolving positively a long-standing open question in cryptography. All the early schemes were extremely impractical, in particular because of the cost incurred in terms of computation time. From 2017, SHE has started to become commercially viable, following efforts to standardise the technology. In particular, a North American industry, government and academia open consortium has produced three white papers (2017)[38], on security, Application Programming Interfaces (APIs) and applications; and a draft standard for parameter selection[39].

Current challenges and limitations

Homomorphic encryption is not currently appropriate in circumstances where analysts wish to carry out arbitrary computations. Whilst PHE is commonly used – for example for secure database querying or to delegate computation, SHE and FHE are the subject of current ongoing research. The most practical SHE and FHE schemes are based on so-called lattice-based constructions, where active areas of research are effective encodings and noise management techniques. This type of encryption schemes rely on noisy encryptions. Such noise grows with every encrypted operation, and if noise grows past a certain threshold decryption will fail.

Compared with computing on unencrypted data, homomorphic encryption is extremely computationally expensive and has lower throughput. Encryption can entail a substantial increase in data size, which can cause a major bandwidth problem. Also, computations need to be represented as polynomials, which can be a limitation in practice. In the case of FHE, the running time increases dramatically with the number of operations (additions or multiplications). These concerns are the subject of ongoing research[40].

In terms of managing trust, with homomorphic encryption it may be hard, considering current developments, for the client to verify that the server performed the function it said it would – this is the subject of ongoing research.

36. Rivest R *et al*. 1978 On data banks and privacy homomorphisms. (see http://luca-giuzzi.unibs.it/corsi/Support/papers-cryptography/RAD78.pdf, accessed 12 February 2019)
37. Gentry C. 2009 Fully homomorphic encryption using ideal lattices. STOC 2009, 169–178. (see https://www.cs.cmu.edu/~odonnell/hits09/gentry-homomorphic-encryption.pdf, accessed 12 February 2019)
38. See homomorphicencryption.org (accessed 12 February 2019)
39. Albrecht MR *et al*. 2015 On the concrete hardness of Learning with Errors. J. Mathematical Cryptology 9. (see https://eprint.iacr.org/2015/046.pdf, accessed 12 February 2019)
40. Brakerski Z *et al*. 2011 Fully Homomorphic Encryption without Bootstrapping (see https://eprint.iacr.org/2011/277.pdf, accessed 12 February 2019)

CASE STUDY 1

Homomorphic encryption – Privitar-NHS De-identification project

The NHS holds a wealth of patient level data which it makes available to recipients with legitimate permissions, in de-identified form. Currently the NHS has a number of tools which are used to de-identify the data. The De-identification project was set up to replace these disparate tools with a single NHS-wide solution. This means that when the right legal basis, controls and safeguards are in place, data can be linked across different care settings and geographic boundaries. The aim is to help to improve health and care services through research and planning, and ultimately lead to better individual care.

The De-identification methodology applies a variety of actions to deliver de-identification:

- **Redaction:** Where an identifier (such as name) is deleted;
- **Derivation:** Where the granularity of a data item is reduced (eg date of birth to year of birth). This is an irreversible activity;
- **Tokenisation:** Consistently obscuring the data item (eg NHS number), by replacement with a token, such as a regular expression. This is a reversible activity.

De-identification of data is a balance between risk and utility. As the granularity of the information in a dataset is reduced, the risk of unauthorised re-identification is reduced, but so is the utility of that dataset. This risk is managed through both technical and procedural measures to reduce it to an acceptable level while maintaining utility of the data for the specified purpose.

One of the major benefits of using a single de-identification tool across the NHS is the ability to link data. Any records which have been de-identified using the same base record identifier (in this case the NHS number) and the same tool are potentially linkable. However, for security reasons, data is de-identified in different 'pseudonymisation domains' for each different part of an organisation. Within one domain, all data with the same base value will be replaced with the same token. Across domains, the same base value will receive different tokens.

Making data available and linkable for specific recipients may require transforming data between domains. When doing this using standard encryption or tokenisation techniques there is a requirement to remove the encryption for the first domain and replace it with the second domain encryption. This reveals the base value – in this case the NHS number, an identifiable attribute – an action which cannot be allowed. Using consistent tokenisation and Partially Homomorphic Encryption (PHE) by Privitar Publisher, it 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 to make 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. This gives the greatest potential utility to the data held by the NHS.

Source: Stuart Gunson, De-Identification Project Manager, Data Processing Services Programme, NHS Digital.

Readiness assessment and considerations for use

Based on the ENISA taxonomy of readiness levels, there are 'products' relying on PHE, SHE is 'piloted' and FHE can be considered to be at the 'research' level (see section 2.1.4). For example, several start-ups and scale-ups offer solutions using PHE schemes and pilot SHE schemes, and it is on the agenda of some large tech companies.

HE today requires a bespoke approach, tailored to a specific application: users need to pick a specific scheme and optimise the function they want to implement with that scheme. There are a number of libraries for HE schemes[41], which are academic prototypes, and choosing the best one for a given application is a challenge. This means that organisations need to access expertise in HE in order to implement these techniques.

Case study

The NHS is using Privitar's de-identification product, Privitar Publisher, which uses partially homomorphic encryption (see Case Study 1). This is an example of how homomorphic encryption – specifically PHE – is employed in a complex scenario.

2.2.2 Trusted Execution Environments

Definition and use case

A Trusted Execution Environment (TEE) is a secure area inside a main processor[42]. Figure 4 shows TEEs are isolated from the rest of the system, so that the operating system or hypervisor[43] 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 analysed, 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. TEEs are a good place to store master cryptographic keys, for example.

In addition, TEEs can support any type of analysis. They have a low cost to utility: the actual computation is performed on the unencrypted data, and no noise needs to be added to the data.

TEEs can be used to address the problems of 'insecurity' and 'exposure' (see Box 1), and the risk of revealing sensitive attributes related to individuals or organisations, in a dataset or output.

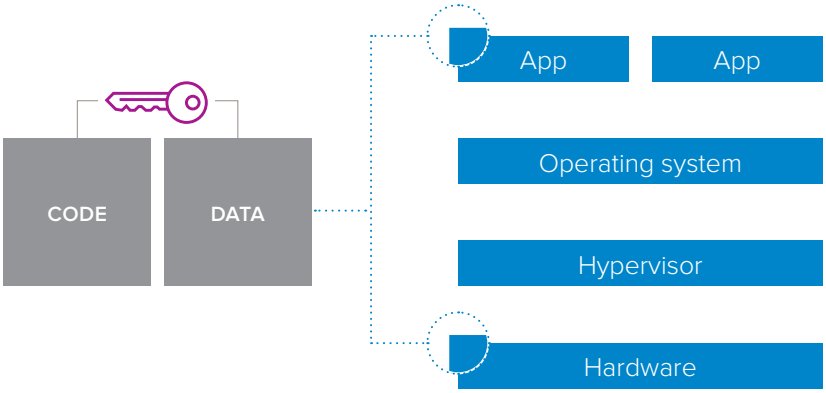
41. See for example: github.com/vernamlab/cuHE; github.com/shaih/HElib; github.com/CryptoExperts/FV-NFLlib; https://git.njit.edu/palisade/PALISADE; sealcrypto.org; tfhe.github.io/tfhe (accessed 12 February 2019)

42. TEEs are sometimes referred to as secure enclaves.

43. A hypervisor is a process that separates a computer's operating system and applications from the underlying physical hardware.

FIGURE 4

Trusted Execution Environment (TEE). TEEs are a secure area inside a processor.



History

Research on TEEs has its roots in the development of programmable secure coprocessors – a computer processor used to supplement the functions of the primary processor – at IBM in the 1990s[44]. These coprocessors allowed secure applications in hostile environments whilst maintaining high performance. In the early 2000s, ARM issued TrustZone[45], a collection of hardware modules that can conceptually partition a system's resources between a secure world, which hosts an authenticated and encrypted area, and a normal world, which runs untrusted software. In the early 2010s, Intel introduced its own secure processor known as Software Guard Extensions (SGX)[46].

Current challenges and limitations

As with other existing cryptographic technology, protecting secure keys in TEEs remains a challenge. It is necessary in particular to protect the system that generates secure crypto functions.

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 (see for example Spectre attacks)[47].

44. Smith SW *et al*. 1999 Validating a high-performance, programmable secure coprocessor. 22nd National Information Systems Security Conference. IBM Thomas J. Watson Research Division. (see https://csrc.nist.gov/csrc/media/publications/conference-paper/1999/10/21/proceedings-of-the-22nd-nissc-1999/documents/papers/p16.pdf, accessed 12 February 2019)

45. Alves T and Felton D. 2004 Trustzone: Integrated hardware and software security. Information Quarterly 3, 18–24.

46. Anati I *et al*. 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. (see https://software.intel.com/sites/default/files/article/413939/hasp-2013-innovative-technology-for-attestation-and-sealing.pdf, accessed 12 February 2019)

47. Kocher P *et al*. 2018 Spectre Attacks: Exploiting Speculative Execution (see https://spectreattack.com/spectre.pdf, accessed 12 February 2019)

CASE STUDY 2

Trusted execution environments – Confidential Consortium Blockchain Framework

The Confidential Consortium Blockchain Framework (CCBF) is a system using trusted execution environments that enables high-scale, confidential blockchain networks that meet enterprise requirements for speed and scalability[48]. By enabling confidentiality within the blockchain, it has the potential to accelerate adoption of blockchain technology.

CCBF originates from enterprises' concern when it comes to control, confidentiality, and performance. To prevent malicious behaviours, blockchains were designed so that all transactions are recorded and open for all to see and replicated across hundreds of decentralised nodes for integrity. There are other approaches to hiding transaction details, for example using zero-knowledge proofs[49] and other advanced cryptographic techniques, however these techniques are currently complex, resource intensive and are not applicable to all use cases.

Within CCBF, confidentiality is provided by TEEs that can process transactions encrypted using keys accessible only to a CCBF node of a specific CCBF service. Besides confidentiality, TEEs also provide publicly verifiable artefacts, called quotes, that certify that the TEE is running a specific code. Hence, integrity of transaction evaluation in CCBF can be verified via quotes and not be replicated across mutually untrusted nodes as it is done in public blockchains. It is worth pointing out that transaction data is replicated in CCBF across a small network of nodes, each executing in a TEE, but for the purpose of fault-tolerance rather than integrity. In addition, Microsoft's test showed that the CCBF could process 50,000+ transactions per second, demonstrating the scalability of the technology. As a comparison, the public blockchain Ethereum network has an average processing rate of 20 transactions per second, whilst the Visa credit card processing system averages 2,000 transactions per second.

The above framework is not a standalone blockchain protocol. Rather it provides trusted foundations that can support any existing blockchain protocol.

Microsoft announced it intended to make the source code of the framework open source in 2019.

Source: Olya Ohrimenko and Sylvan Clebsch, Microsoft Research Cambridge.

48. See https://github.com/Azure/coco-framework/blob/master/docs/Coco%20Framework%20whitepaper.pdf (accessed 18 March 2019)

49. Zero-knowledge proof is a method by which one party can prove to another party that they know a value x, without conveying any information apart from the fact that the statement is true. See Introduction, Key terms and definitions.

TEEs are the subject of ongoing research, for instance on:

- new hardware design. The lack of memory in TEEs is currently a challenge, so that only limited data can be processed at any one time;
- combining TEEs with homomorphic encryption or other cryptographic techniques;
- verifiable computation in zero-knowledge;
- secure multi-party machine learning using TEEs.

Readiness assessment and considerations for use

There are a number of products available on the market, and a number of secure cloud providers. Microsoft's cloud, Azure, was the first cloud to offer this technology which has been in place since September 2017, using secure processors Intel SGX or Virtual Secure Mode (VSM). Secure processors are widely used on smartphones, and are used, for instance, to store and process information related to touch identification[50].

Case study

TEEs enable new scenarios, such as adding confidentiality, performance and governance to blockchain (see Case Study 2).

2.2.3 Secure Multi-Party Computation

Definition and use case

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.

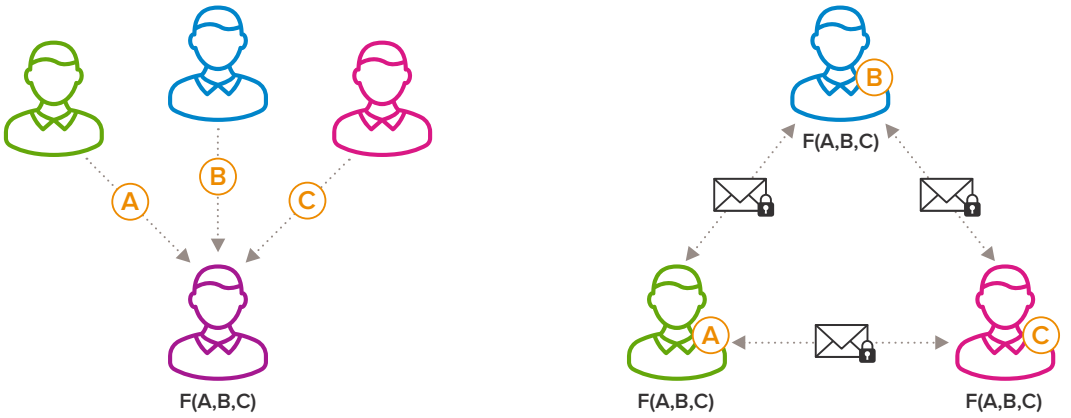
For example, MPC can allow bidders to identify who has won an auction without revealing anything about the actual bids. MPC can also be used to allow private multi-party machine learning: in this case, different parties send encrypted data to each other and they can train a machine learning model on their combined data, without seeing each other's unencrypted data (see Figure 5). This removes the need for a trusted central authority that would perform the computation by pooling together all the data and decrypting it. This also presents the advantage that computation is distributed.

The use of MPC can address the problems of 'insecurity' and 'exposure' (see Box 1), and the risk of revealing sensitive attributes related to individuals or organisations, in a dataset or output.

50. Hoffman C. 2018 Your Smartphone Has a Special Security Chip. Here's How It Works (see https://www.howtogeek.com/387934/your-smartphone-has-a-special-security-chip.-heres-how-it-works/, accessed 12 February 2019)

FIGURE 5

Private multi-party machine learning with MPC. Using MPC, different parties send encrypted messages to each other, and obtain the model F(A,B,C) they wanted to compute without revealing their own private input, and without the need for a trusted central authority.



Central trusted authority

Secure multi-party machine learning

Variations

Private Set Intersection (PSI) where two or more parties compare datasets without revealing them in an unencrypted form, can be implemented using MPC techniques. At the end, each party knows which items they have in common with the other. There are some scalable open-source implementations of PSI available. Private Information Retrieval (PIR) can also be implemented using MPC techniques and allows a user to query a database whilst hiding the identity of the data retrieved. Google employs PIR to warn a user that their password might be unsafe[51].

History

The first prototypes of MPC date back to 2004[52]. Real-world development and commercial products for multi-party computation started to appear in 2010. The initial commercial application was in auctions[53]. For example, MPC was used to redistribute Denmark's EU-fixed production quota among sugar beet producers in the country, in a privacy-preserving way – without revealing commercially sensitive information. Recent theoretical developments have further enabled data analysis using MPC.

51. Pullman *et al.* 2019 Protect your accounts from data breaches with Password Checkup (see https://security.googleblog.com/2019/02/protect-your-accounts-from-data.html, accessed 19 February 2019)
52. Malkhi D *et al.* 2004 Fairplay – a secure two-party computation system. SSYM'04: Proceedings of the 13th conference on USENIX Security Symposium, 20–20. (see https://www.usenix.org/legacy/event/sec04/tech/malkhi/malkhi.pdf, accessed 12 February 2019)
53. Bogetoft P *et al.* 2009 Secure multiparty computation goes live. Financial Cryptography and Data Security, 13th International Conference, FC 2009. (see https://eprint.iacr.org/2008/068.pdf, accessed 12 February 2019)

CASE STUDY 3

Secure multi-party computation – Sharemind[54]

Sharemind, a secure, distributed database system developed by Cybernetica, uses MPC to enable organisations to perform analysis on shared data. The data from input parties is securely encrypted and distributed, remains private during computation by computing parties and results are revealed to authorised result parties only.

Sharemind applications seek to achieve the following four security goals:

1. **Cryptographic privacy:** No computing party shall learn a private value held by an input party.
2. **Source privacy:** No computing party shall be able to relate the results of a computation to the inputs of a certain input party.
3. **Query restrictions:** No result party or any unauthorised set of computing parties shall be able to successfully initiate and complete a query that has not been authorised by the computing parties.
4. **Output privacy:** No result party shall learn a private value held by an input party from the results of queries.

The first real-world application of Sharemind was the analysis of Key Performance Indicators (KPIs) for the Estonian Association of Information Technology and Telecommunications (ITL). The ITL proposed collecting certain financial metrics and analysing 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. 17 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. Data collection and queries were implemented as web applications integrated into the ITL intranet. In this specific example, the amount of data (17 companies) and lines of code (1,000) was limited, and the actual processing time was 2 minutes. In other examples, with hundreds of thousands of data records or more, the processing can take a number of hours.

Sharemind has been applied to a range of cases, including to allow social studies on tax and education records, for tax-fraud detection, to predict satellite collisions in Low Earth Orbits, and to demonstrate the feasibility of genome-wide association studies with multiple data providers.

54. Based on Archer DW *et al.* 2018 From Keys to Databases – Real-World Applications of Secure Multi-Party Computation (see https://eprint.iacr.org/2018/450, accessed 12 February 2019)

Current challenges and limitations

MPC currently significantly increases the time it takes to compute a given function, due in part to delays incurred in communicating encrypted data across the network (latency). The computing time has been cut down since the first implementations came out and still needs further improvement to make MPC more practical[55].

Another challenge, common to all cryptographic methods, is the protection of the cryptographic keys.

Readiness assessment and considerations for use

Whilst secure multi-party computation has been applied in a limited number of 'products', research and development is ongoing and other applications are at a 'proof of concept' stage[56]. For real-world data analysis, organisations need to produce custom protocols. For this, they need to access expertise in MPC and to invest time in developing and testing bespoke solutions.

It should also be noted that different MPC protocols come with different threat models. For example, these vary depending on whether there are two or more parties. In implementing MPC, different approaches will be needed depending on whether there might be a majority of honest parties or dishonest parties.

Case study

Sharemind is a secure, distributed database system using MPC and deployed towards multiple applications (see Case Study 3).

2.2.4 Differential Privacy

Definition and use case

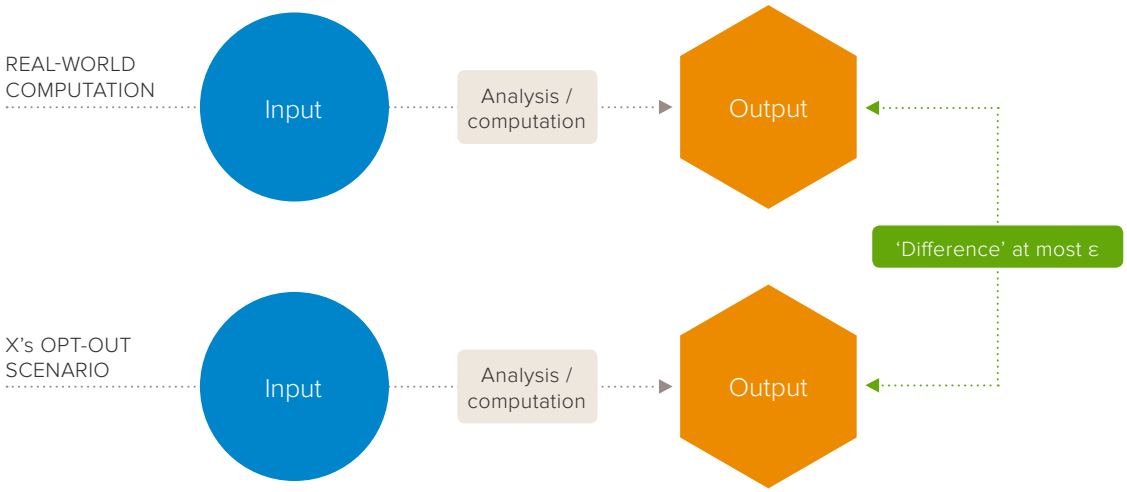
The differential privacy security definition means that, when a dataset or result is released, it should not give much more information about a particular individual than if that individual had not been included in the dataset (see Figure 6)[57,58]. Unlike, the previous three PETs which address privacy during computation, differential privacy addresses privacy in disclosure.

The differential privacy definition allows reasoning about how much privacy is lost upon multiple queries. The parameter ε (epsilon), information leaked about a specific entity, increases linearly with the number of queries. ε can be set as the limit after which a user is not allowed to perform any more queries – it is also called 'privacy budget' in the literature.

55. Von Maltitz and Carle 2018 A Performance and Resource Consumption Assessment of Secure Multiparty Computation (see https://arxiv.org/pdf/1804.03548.pdf, accessed 19 February 2019)
56. Archer DW *et al*. 2018 From Keys to Databases – Real-World Applications of Secure Multi-Party Computation (see https://eprint.iacr.org/2018/450, accessed 12 February 2019)
57. Dwork C *et al*. 2006 Calibrating Noise to Sensitivity in Private Data Analysis (see http://people.csail.mit.edu/asmith/PS/sensitivity-tcc-final.pdf, accessed 12 February 2019)
58. Page H *et al*. 2018 Differential privacy: an introduction for statistical agencies (see https://gss.civilservice.gov.uk/wp-content/uploads/2018/12/12-12-18_FINAL_Privitar_Kobbi_Nissim_article.pdf, accessed 12 February 2019)

FIGURE 6

The differential privacy security definition. The output of an analysis is ε-differentially private if the difference between the real-world output and the output in an 'opt-out' scenario, where X's data would be excluded from the input, is at most ε (epsilon).



Source: Nissim *et al*. 2018 Differential Privacy: A Primer for a Non-technical Audience (see https://privacytools.seas.harvard.edu/files/privacytools/files/pedagogical-document-dp_new.pdf, accessed 12 February 2019)

Differential privacy has some similarities but also important differences to the definition of 'anonymisation' in data protection law. For instance, in differential privacy, the concern is about privacy as the relative difference in the result whether a specific individual or entity is included in the input or excluded (see Figure 6). In contrast, 'anonymisation' in data protection law is concerned about removing any attributes associated with an individual that could make them identifiable in a dataset. The two concepts can be brought together by setting the value of ε so that the relative difference in the result is so small that it is unlikely anyone could infer, with confidence, anything about a specific individual or entity in the input.

Differential privacy comes with a mathematical proof (or guarantee) that bounds what can be learnt about any individual from a release[59]. The parameter ε allows one to reason about the level of privacy protection desired. The amount of noise (or other alteration) that needs to be added to data to achieve ε-differential privacy is calibrated to each application and context.

Differentially private mechanisms can, in particular, provide secure public access to private datasets and protect data whilst disclosing derived information. They can be used to address the problems of 'identification' and 'disclosure' (see Box 1), and the risk of revealing whether a specific individual or organisation is present in a dataset or output.

59. Nissim *et al*. 2018 Differential Privacy: A Primer for a Non-technical Audience (see https://privacytools.seas.harvard.edu/files/privacytools/files/pedagogical-document-dp_new.pdf, accessed 12 February 2019)

Variations

Differential privacy can be applied at different stages of the data analysis pipeline:

- At the data collection stage – adding noise so that users get a 'plausible deniability' type of of guarantee with respect to data being collected about them. This is known as distributed (or local) differential privacy. For example, Apple adds noise to data before gathering certain user statistics from smartphones. As noise is added at an early stage of the data lifecycle, it is not possible to optimise noise to a specific analysis – in practice this means that distributed differential privacy may require adding more noise than the centralised approach.
- When disclosing results – adding noise to the output so that it is not possible to tell whether a given data record was in the dataset that was used to produce the output. This is known as centralised (or global) differential privacy.

Differential privacy can be achieved or amplified through a range of mechanisms[60], such as removing or randomising data points, 'subsampling' (also known as derivation or generalisation) and injection of carefully calibrated noise.

The most common differential privacy mechanism is known as Laplace mechanism, which adds noise drawn from a Laplace distribution. This technique relies on calculating the 'sensitivity' of the computation at hand, ie how sensitive a given analysis is to whether an individual is included in a dataset or not.

History

When released summary statistics contain enough information about the underlying dataset, an adversary may be able to reconstruct the dataset – this is known as a reconstruction attack[61]. Dinur and Nissim showed in 2003 that releasing too many randomly selected statistics with high accuracy will allow reconstruction with extremely high probability[62]. The introduction of differential privacy has provided a new approach to releasing statistical information on datasets in a privacy-preserving manner, together with a mathematical proof. The concept of differential privacy was introduced in a 2006 publication by Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith[63].

Current challenges and limitations

A key issue in differential privacy is that adding noise can harm utility. Intuitively, for population-level statistics, the more individuals included in a dataset, the harder it might be to identify that a specific individual was included – and therefore less noise needs to be added in order to protect privacy.

60. *Op. Cit.* 58
61. *Op. Cit.* 60
62. Dinur I and Nissim K 2003 Revealing Information While Preserving Privacy. Proceedings of the twenty-second ACM SIGNOD-SIGNET-SIGART symposium on Principles of Database systems, 202–210.
63. *Op. Cit.* 57

In other words, with differential privacy there is a better trade-off of utility and privacy with larger datasets, where noise will have less of an impact on the output. In fact, there is a parallel to be made with statistics where the larger the dataset the more robust the result. In machine learning, achieving differential privacy also goes hand in hand with preventing overfitting to particular examples.

It should be noted that the use of differential privacy is not in itself a guarantee of privacy-preservation as it depends on how the 'privacy budget' was set.

The selection of the 'privacy budget' is a governance question rather than a technological one. In practice, setting the privacy budget requires expertise and careful consideration from those who seek to implement differential privacy; and it requires the attention of those who set standards, whether inside an organisation or at a higher level. However, the literature about how ε should be set is sparse.

Differential privacy comes from a tradition of cryptography, which involves an adversarial mindset and thinking about how data or a system could potentially be exploited by an adversary. Setting the overall 'privacy budget' requires careful consideration of the statistical inferences that might happen after the release of results and how, for example, outsiders might be able to link data with side information. Differential privacy allows one to see how the release of information is impacting the privacy of the individuals on whom the data is based, and quantifies this per query. The limitation is true of all data releases.

Of note, the National Statistician's Quality Review[64] has investigated the governance of the 'privacy budget' as part of a broader effort to implement differential privacy for national statistics in the UK[65].

Readiness assessment and considerations for use

Differential privacy has been piloted by tech companies and governmental organisations that hold large datasets, where differentially private mechanisms are most likely to yield both a useful and privacy-preserving result. For example, Apple and Google implemented their own versions of distributed differential privacy for collecting statistics from end-users[66,67].

Differential privacy involves sophisticated mathematics and reasoning about uncertainty. Also, most statisticians in industry and government rely on existing software, and such legacy systems mean that they cannot implement a sophisticated approach such as differential privacy in a straightforward manner.

Case study

The US Census Bureau has implemented solutions using differential privacy. It is planning on using it more widely for the release of statistics from the upcoming 2020 census (see Case Study 4).

64. See gss.civilservice.gov.uk/guidances/quality/nsgr/privacy-and-data-confidentiality-methods-a-national-statisticians-quality-review (accessed 8 March 2019)

65. *Op. Cit.* 58

66. Erlingsson U *et al*. 2014 RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response (see https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/42852.pdf, accessed 12 February 2019)

67. See https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf (accessed 12 February 2019)

CASE STUDY 4

Differential privacy – US Census[68]

In 2017, the US Census Bureau announced that it would be using differential privacy as the privacy protection mechanism for the 2020 decennial census – this is after having implemented differential privacy for other services (OnTheMap, 2008; an online application developed in partnership with 50 US 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 contrast, the Census Bureau says that such a risk is much less controlled in the case of traditional approaches to statistical disclosure control.

In the light of these benefits, and despite encountering a number of hurdles, the Census Bureau is continuing to pursue its decision to implement differential privacy. The institution is not only implementing differential privacy in its statistical analyses, but integrating it into its organisational structure.

Challenges for the Census Bureau have included obtaining qualified personnel and a suitable computing environment. There is no off-the-shelf mechanism for applying differential privacy to a national census. Applying the Laplace Mechanism or Google's RAPPOR mechanism would result in far too much noise for any output statistics to be of much value. Instead the Census Bureau has been developing, implementing, testing and deploying a new differential privacy mechanism.

Setting the value of the privacy budget ε has not been trivial. In practice the value of ε chosen by the Census Bureau's Data Stewardship Executive Policy committee was far higher than those envisioned by the creators of differential privacy.

More efficient mechanisms and proofs are needed to achieve lower amounts of noise for the same level of privacy loss, and to make efficient use of the privacy-loss budget for iterative releases of edited and corrected statistics.

Transitioning existing data products to differential privacy has also demonstrated the difficulty of retrofitting legacy statistical products to conform with modern privacy practice. This is despite the Census Bureau having prior experience of differential privacy for another service in 2008 (OnTheMap).

The Census Bureau has found it helpful to establish a common language to facilitate both internal and external communication between stakeholders representing multiple disciplines. The institution has also created an informed team of senior leaders in charge of communicating with data users and the public.

68. Based on Garfinkel SL *et al.* 2018 Issues Encountered Deploying Differential Privacy (see https://arxiv.org/pdf/1809.02201.pdf, accessed 12 February 2019)

2.2.5 Personal Data Stores

Definition and use case

Personal Data Stores (PDS) are systems that provide individuals with access and control over data about them, so that they can decide what information they want to share and with whom (see Figure 7). PDS provide transparency and agency to individuals over the data they generate. They could empower citizens with the managing and processing of data about them.

Unlike the other four PETs covered in the report, which are tools for privacy-preserving computation, Personal Data Stores are consumer-facing apps and services 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.

PDS enable a distributed system, where the data is stored and processed at the 'edge' of the system, rather than centralised. 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 solves a number of issues such as the 'honeypot' issue – whereby an organisation holding millions of records constitutes a 'honeypot' that is economically attractive to hack.

A distributed architecture would also relieve the power asymmetry brought about by large tech companies that are concentrating a large portion of the world's data.

PDS address the problems of 'aggregation', 'exclusion' and 'disclosure' (see Box 1), as well as the risk of undesirably sharing information.

Variations

PDS can be physical box-sets or apps on for instance phones or tablets. Their design can incorporate a number of other PETs.

History

Personal data stores have been proposed by community-led initiatives since the 2000s[69]. The UK Government launched its own version in 2011, midata[70], providing citizens with access and control over data about them (see Figure 7).

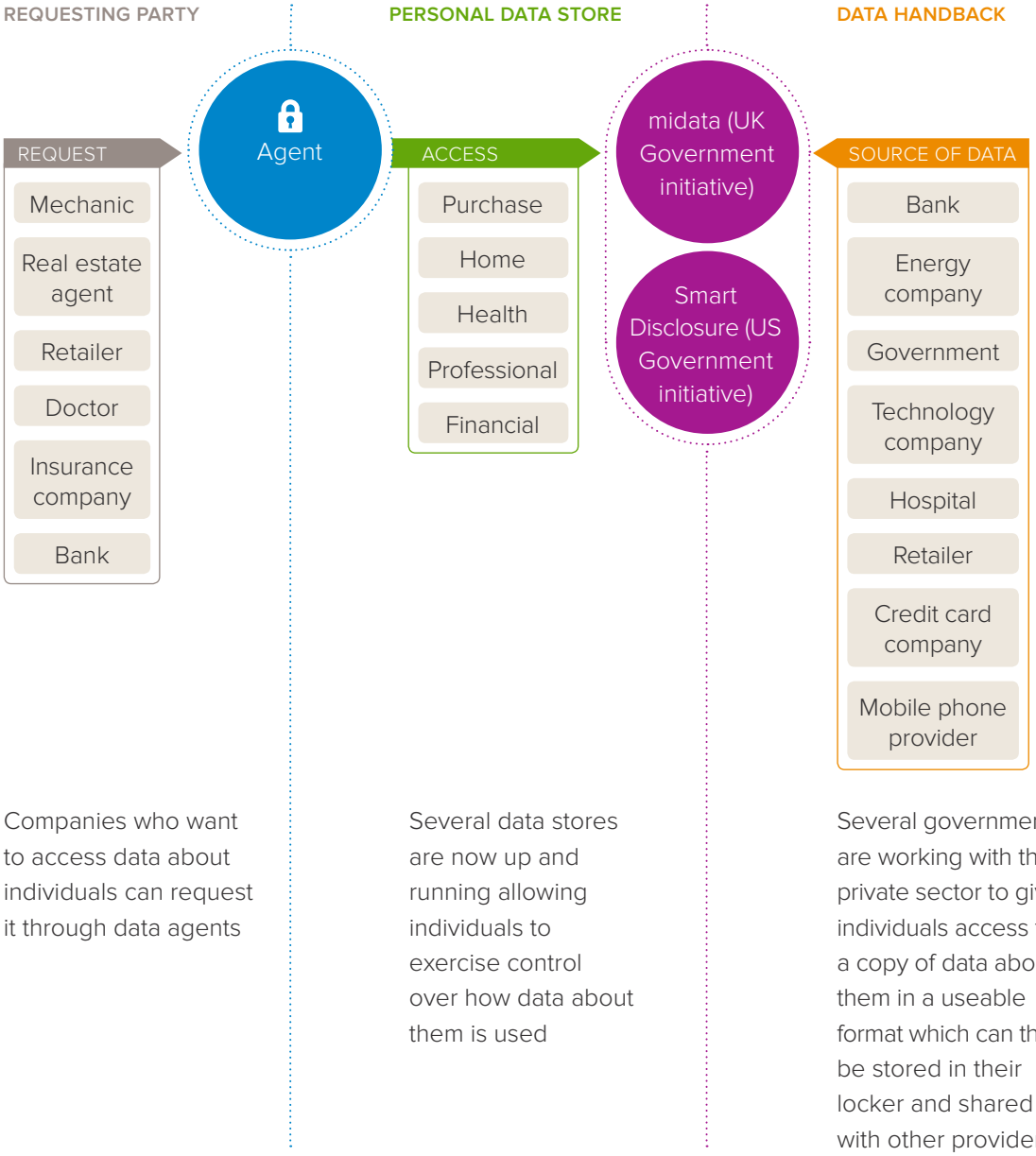
Current challenges and limitations

Existing business models and the current monetisation of data, based on centralised architectures, do not encourage the development of PDS. Currently an individual's data on its own does not have a high monetary value, whilst aggregated data is much more profitable[71]. Further research is needed, in particular, from the economics and social sciences fields, to investigate alternative models. There are already examples of such alternative models emerging, for example: Tim Berners-Lee, inventor of the World Wide Web, has been working on a decentralised web platform, whereby individual users could store data about them in different personal online datastores (PODs) and give permission of access to services of their choice[72].

69. World Economic Forum 2013 Unlocking the Value of Personal Data: From Collection to Usage (see http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf, accessed 12 February 2019)
70. See https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment (accessed 12 February 2019)
71. The British Academy, The Royal Society and techUK 2018 Data ownership, rights and controls: Reaching a common understanding. (see https://royalsociety.org/topics-policy/projects/data-governance/, accessed 12 February 2019)
72. See https://solid.inrupt.com/how-it-works (accessed 12 February 2019)

FIGURE 7

Personal data stores allow individuals to exercise control over how data about them is used.



Source: World Economic Forum and The Boston Consulting Group building on original graphic by Forrester Research.

In order for PDS to be effective, individuals with variable levels of technical experience need to be able to access and interact with them. User engagement is central to their success. Interface design is an important component of this, and user interfaces need to be accessible and engaging. This adds an additional dimension to the process of research and development in PDS.

Readiness assessment and considerations for use

There are a few products on the market, in the UK and internationally. They include midata, DigiMe, Databox[73], HATDeX and CitizenMe.

The adoption of such technologies is currently limited. A challenge for the technology is reaching a critical mass of uptake that would provide confidence to other consumers and businesses that PDS are worth using[74].

The terms and conditions attached with the use of a number of PDS imply that the individual is negotiating a contract with service providers[75]. However, it is unclear how easy or feasible it might be for an individual to use a PDS to try and impose their terms on a large organisation. There is a need for a framework to help individuals increase their negotiation power. Whether people are content or not with providing large organisations with their data in exchange for 'free' services, currently people have little choice as they do need services provided by such large organisations, as part of their lives.

Case study

CitizenMe is one example of a PDS enabling users to choose how they want to share and trade the data they generate (see Case Study 5).

2.3 Privacy in practice – Privacy-preserving machine learning

Machine learning is a powerful set of techniques, allowing computers to learn from data. The Royal Society's report on *Machine learning: the power and promise of computers that learn by example*[76] called for further research into privacy-preserving machine learning. There are a number of promising areas of research and practice, some of which have been discussed in section 2.2 and elsewhere[77].

In brief, privacy-preserving machine learning may refer to different approaches, such as:

- **Machine learning with synthetic data** Synthetic data is data generated by an algorithm, rather than from real-world events. The Royal Society's Machine learning report and the National Statistician's Quality Review, among

73. The Royal Academy of Engineering 2018 Towards trusted data sharing: guidance and case studies (see http://reports.raeng.org.uk/datasharing/case-study-1-databox/, accessed 12 February 2019)

74. European Commission 2015 Study on Personal Data Stores conducted at the Cambridge University Judge Business School (see https://ec.europa.eu/digital-single-market/en/news/study-personal-data-stores-conducted-cambridge-university-judge-business-school, accessed 12 February 2019)

75. Oswald M. 2017 Jordan's dilemma: Can large parties still be intimate? Redefining public, private and the misuse of the digital person. *Information & Communications Technology Law*, 26, 6–31. (see https://doi.org/10.1080/13600834.2017.1269870, accessed 12 February 2019)

76. *Op. Cit.* 3

77. Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for the New American Security, Electronic Frontier Foundation, and OpenAI 2018 The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation (see https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/1c6q2kc4v_50335.pdf, accessed 12 February 2019)

CASE STUDY 5

Personal Data Store – CitizenMe

CitizenMe enables people to derive value from their data: they can for instance donate data to charity or share data anonymously for cash. Storage and control is distributed out to devices. The platform uses a mixture of artificial intelligence (AI), MPC, differential privacy and deep encryption to train models across different devices. As data is stored on smartphones, CitizenMe does not hold any data itself.

Users generate a lot of data: social media; apps on phones and wearables; banking information. The linking of several data sources, such as sentiment information combined with step counts, could create valuable insight. CitizenMe have carried out a lot of research on consumers and how they want their data to be used. CitizenMe has over 160,000 users in 120 countries, growing at 10% a month. CitizenMe reports very high retention and engagement.

Getting money for their data is one of the motivations of CitizenMe's users. However, currently the value of individual data records is much less than the value of the same data once aggregated. Changes in the way data is monetised could accelerate the take up of CitizenMe and other PDS.

In fact, most users are initially attracted to the CitizenMe app for cash but typically after a month's use, they instead value the AI derived insights and ability to donate data to good causes, with cash incentive becoming a secondary activity driver.

Source: StJohn Deakins, Founder and CEO at CitizenMe.

others, looked into opportunities and considerations for the use of synthetic data[78,79]. Such data can serve to train a machine learning model or as a test set to validate a model. Training a model on synthetic data and then applying it to real, encrypted data has several advantages: it allows a better understanding of the relationship between the training data and the model, and a minimisation of the use of sensitive data.

- **Differentially-private machine learning**
  By definition, a differentially-private machine learning model should not give much more information about a particular individual than if that individual had not been included in the training dataset. This can be achieved for example with distributed differential privacy, where noise is added during the collection of training data, or with centralised differential privacy, where noise is added to the output. Also, differentially private synthetic data might be used to create data that retains properties of real example data whilst protecting against model inversion attacks[80].

78. *Op. Cit.* 3

79. *Op. Cit.* 64

80. *Op. Cit.* 58

- **Privacy-preserving machine learning using homomorphic encryption**
  Homomorphic encryption can support certain forms of machine learning[81]. It can in particular underpin 'privacy-preserving prediction' (see below).
- **Private multi-party machine learning using MPC**[82]
  With private multi-party machine learning, different parties send encrypted messages to each other, and obtain the model they wanted to compute without seeing each other's data, and without the need for a trusted central authority.
- **Secure multi-party machine learning using TEEs**[83]
  In this case, multiple users compute a machine learning model on pooled encrypted data without revealing their unencrypted data to each other or to the cloud.
- **Federated learning**
  Federated learning is an emerging approach allowing the training of machine learning models on decentralised data[84,85], for privacy or practical reasons. A central server coordinates a network of nodes, each of which has training data. The nodes each train a local model, and it is that model which is shared with the central server. In other words, data is protected at the device level. Google published such a federated learning algorithm in 2016.

Additionally, applying different PETs, which come with different privacy guarantees, at different stages of a data analytics or machine learning pipeline (see Figure 8) might help address particular needs or concerns, alongside other approaches for protecting privacy. These PETs may be applied individually or in combination to help reduce specific risks (as outlined in section 1.2), as follows:

- **Data collection**
  One option to protect the data that is pooled together is to collect 'noisy' data, as in distributed differential privacy. Another option is to collect data in an encrypted form. The first option may be more efficient and scalable, as there is no need to compute on encrypted data. However, it is worse for accuracy as noise alters the data. Alternatively, in some settings data collection might have been done by several organisations independently and the privacy challenge is to combine their data without compromising privacy, ie without the organisations sharing their data with each other. This calls for a solution based on multi-party computation.
- **Training**
  Protecting sensitive information during the training of a machine learning model might be done by computing on encrypted data using cryptographic techniques such as MPC or homomorphic encryption. These offer different trade-offs between

81. Aslett LJM *et al*. 2015 A review of homomorphic encryption and software tools for encrypted statistical machine learning. (see arXiv: 1508.06574, accessed 8 March 2015)
82. Gascón A *et al*. 2017 Privacy-Preserving Distributed Linear Regression on High-Dimensional Data. *Proceedings on Privacy Enhancing Technologies* 4, 345–364. (see https://eprint.iacr.org/2016/892.pdf, accessed 19 February 2019)
83. Ohrimenko O *et al*. 2016 Oblivious Multi-party Machine Learning on Trusted Processors (see https://www.microsoft.com/en-us/research/wp-content/uploads/2016/07/paper.pdf, accessed 12 February 2019)
84. McMahan HB *et al*. 2017 Communication-Efficient Learning of Deep Networks from Decentralized Data. *Proceedings of the 20 the International Conference on Artificial Intelligence and Statistics (AISTATS)* 2017. (see https://arxiv.org/abs/1602.05629, accessed 12 February 2019)
85. Bonawitz *et al*. 2019 Towards Federated Learning at Scale: System Design (see https://arxiv.org/abs/1902.01046, accessed 19 February 2019)

FIGURE 8

Links between stages in a data analytics pipeline and privacy enhancing technologies (PETs): example of a machine learning system first trained on a training dataset, then deployed to a real-world application. Inference refers to executions of the model to make prediction on previously unseen, and possibly sensitive, data.

computation and communication, and the latter is significantly slower. Alternatively, one could rely on secure hardware.

- **Deployment**
  When a machine learning model is deployed to a real-world application, sensitive information could in certain cases be deducted about the model by repeatedly querying it[86]. To address this risk, an organisation may want to choose a PET that enables them to deploy their algorithm in a way that prevents model inversion attacks.
- **Inference**
  Machine learning models can be used for example to predict the risk of somebody having a certain disease. The user of such a service may wish for this prediction, or inference, to be only revealed to them. Such a 'privacy-preserving prediction' might be achieved by sending the algorithm to an individual's data, for computation to be performed locally. However, this might not be possible for models that involve some kind of intellectual property. An alternative is to use a PET to protect the sensitive user data whilst computing on it[87].
- **Disclosure of results**
  Even if a data analysis model is computed in a way that does not reveal anything about the data, the result itself must contain information about the input, as that is the goal of the analysis. Privacy during computation and upon disclosure are complementary concerns, and both need to be addressed. Differential privacy provides strong guarantees to limit the amount of information about each user in the training dataset that is disclosed by a computation.

86. Veale M *et al* 2018 Algorithms that remember: model inversion attacks and data protection law. Phil. Trans. R. Soc. A 376. (see http://rsta.royalsocietypublishing.org/content/376/2133/20180083, accessed 12 February 2019)

87. Dowlin N *et al*. 2016 CryptoNets: Applying Neural Networks to Encrypted Data with High Throughput and Accuracy. Proceedings of the 33rd International Conference on Machine Learning (see http://proceedings.mlr.press/v48/gilad-bachrach16.pdf, accessed 19 February 2019)

Chapter three
The road to adoption

Left
© shapecharge.

The road to adoption

3.1 Further research and development

As shown in chapter two, PETs present the possibility of multiple applications and open up new opportunities for data analysis. They are a nascent but potentially disruptive set of technologies that have the potential to reshape the data economy, and to change, in particular, the trust relationships between citizens, governments and companies. However, in their current state a number of these technologies have substantial limitations such as the computing resources that they require, and some are still very much in the research phase. In order to start realising the potential of PETs, and to work towards their use on a greater scale, further research and development is needed.

Going forward, developing solutions that are fit for purpose will require an interdisciplinary research and development effort; it will also need constant updating to adapt to new challenges arising with increasing data and compute power. For instance, implementing MPC for a given large organisation, such as the NHS, could not be done by the PETs research community alone; rather it will need to involve additional expertise such as security engineers as well as domain experts. It is necessary to consider how to build a whole ecosystem that could deliver the development and use of PETs.

There is a key role for government to enable markets to develop. In fact, the UK government has taken a 'leaning forward' approach on this. The Office for National Statistics and the national security agencies, in particular, have experimented with and sought to increase their use of PETs.

The Alan Turing Institute, as the national institute for data science and artificial intelligence, plays a key role in enabling multi-disciplinary approaches to privacy-preserving data analysis. Privacy is an area of strategic focus for the institute across several of its research programmes, including Defence and Security, Artificial Intelligence, and Health.

The US has directed challenge-based funding for the strategic development of PETs. The Intelligence Advanced Research Projects Activity (IARPA), in particular, has a major programme instigated in 2017 called Homomorphic Encryption Computing Techniques with Overhead Reduction (HECTOR)[88]. Such a challenge-based funding approach seems particularly suited to bridge gaps between theory and practice.

RECOMMENDATION 1

Accelerate the research and development of PETs.

Funders, government, industry and the third sector can work together to articulate and support the development of cross-sector research challenges, alongside providing continued support for fundamental research on PETs.

RECOMMENDATION 2

Promote the development of an innovation ecosystem.

UK Research and Innovation (UKRI) have a role in encouraging data-handling companies to engage with the start-ups and scale-ups developing PETs, to support research and early trials. This will help UK investors and businesses realise the extent of the market opportunity for PETs.

88. IARPA 2017 Homomorphic Encryption Computing Techniques with Overhead Reduction (HECTOR) (see https://www.iarpa.gov/index.php/research-programs/hector/hector-baa, accessed 12 February 2019)

RECOMMENDATION 3

Drive the development and adoption of PETs.

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 whilst fully addressing privacy and confidentiality concerns.

3.2 Awareness raising and quality assurance

Standards and kitemarks are needed for quality assurance and to increase 'buyer confidence' in PETs[89]. 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.

At the time of writing this report, several standardisation efforts are on-going. NIST in the US has undertaken substantial work on privacy engineering and risk management[90]; in particular NIST has developed standards for cryptographic key management. The International Standardisation Organization (ISO) is developing standards on 'consumer protection: privacy by design for consumer goods and services' (ISO/PC 317)[91]. The Institute of Electrical and Electronics Engineers (IEEE) is also working on international standards.

However, because of the cultural and legal discrepancies in different systems around the world, global efforts are likely to lead to fairly high-level standards. This would require interpretation of such standards prior to deployment, so would only represent a partial step forward. In the UK, the reviewing of PETs and provision of kitemarks by a trusted authority such as the National Cyber Security Centre (NCSC) would give more confidence to companies and their customers. Trustworthy standards and appropriate guidance will further drive a culture change that goes beyond a 'sticking plasters' strategy and would build upon the 'privacy-by-design' approach embodied in GDPR.

RECOMMENDATION 4

Support organisations to become intelligent users of PETs.

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) should provide guidance about the use of suitably mature PETs to help UK organisations minimise 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 organisation's overall data governance infrastructure, since the use of PETs in isolation is unlikely to be sufficient.

89. *Op. Cit.* 1

90. *Op. Cit.* 17

91. See https://www.iso.org/committee/6935430.html (accessed 12 February 2019)

RECOMMENDATION 5

Give public sector organisations the level of expertise and assurance they need to implement new technological applications, enable a centralised approach to due diligence, and assure quality across the board.

The National Cyber Security Centre should act as a source of advice and guidance on the use of suitably mature PETs, as part of a network of expert organisations. 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 organisations interested in learning about PETs could access information on existing case studies.

3.3 Adoption within a wider business framework

PETs are only one aspect of effective privacy practice, and are not silver bullets that can ensure the protection of sensitive information[92]. Organisations handling data should not consider PETs as an add-on, but rather embed them as part of multiple layers of information privacy, including information security, information management, information principles, information use and information privacy culture[93]. As some controls in each layer are optimally implemented by humans, each organisation must decide, for their particular context, the most suitable mixture of technology, processes and people when designing effective privacy practice at each layer. This will ensure the best and most cost effective approach to privacy protection is taken.

Notably, whilst PETs will help put more data to use, they will not replace the need for data minimisation and curation, nor the need for considering whether a particular use is ethical. Therefore, PETs need to be considered in the context of appropriate business models and auditing processes for data-enabled businesses and organisations. For example, the National Statistician's Data Ethics Advisory Committee (NSDEC) has been established to advise the National Statistician that the access, use and sharing of public data, for research and statistical purposes, is ethical and for the public good[94]. This includes but is not limited to considerations of whether sufficient measures are in place to protect privacy.

92. The Royal Academy of Engineering (2018) Towards trusted data sharing (see http://reports.raeng.org.uk/datasharing/cover/, accessed 12 February 2019)

93. Morton M and Sasse MA. 2012 Privacy is a process, not a PET: a theory for effective privacy practice. Proceedings of the 2012 New Security Paradigms Workshop, 87–104.

94. See https://www.statisticsauthority.gov.uk/about-the-authority/committees/nsdec/ (accessed 12 February 2019)

RECOMMENDATION 6

Create the skilled workforce needed to develop and implement PETs.

Funding should be made available so that the capacity to train UK PhD and Master students in cryptography, statistics, systems engineering and software development increases with the level of demand for well-trained, high-calibre candidates. This could be an outcome of the National Cyber Security Programme and the cybersecurity centres of excellence scheme by the Engineering and Physical Sciences Research Council. Universities should consider adding privacy engineering to the curriculum of software engineering and data science courses, treating the need to protect data as core knowledge in data analysis.

3.4 Consider the wider markets

PETs may help the public and private sectors develop solutions that meet their needs and satisfy societal concerns. Based on a public dialogue exercise on consumer data, Which? recommended a "thoroughgoing review of governance of data in motion, with due attention given to creative ways to improve oversight and enforcement. [...] This is likely to mean understanding the forefront of potential technological solutions that could provide truly decentralised and scalable accountability for how data flows"[95].

Europe has led on implementing a stricter data protection regulation with the GDPR, thus promoting a consumer-centric approach to digital markets. Europe has a market for technology for public good, and the potential to lead on the development of technologies that serve social purposes in a way that is secure and well-governed[96]. Europe has in particular a flourishing start-up scene for GovTech – that is, technologies that underpin new ways of delivering public services.

Finally, the UK Government and the Open Data Institute have launched pilots for 'data trusts', which they define as a legal structure that provides independent third-party stewardship of data.

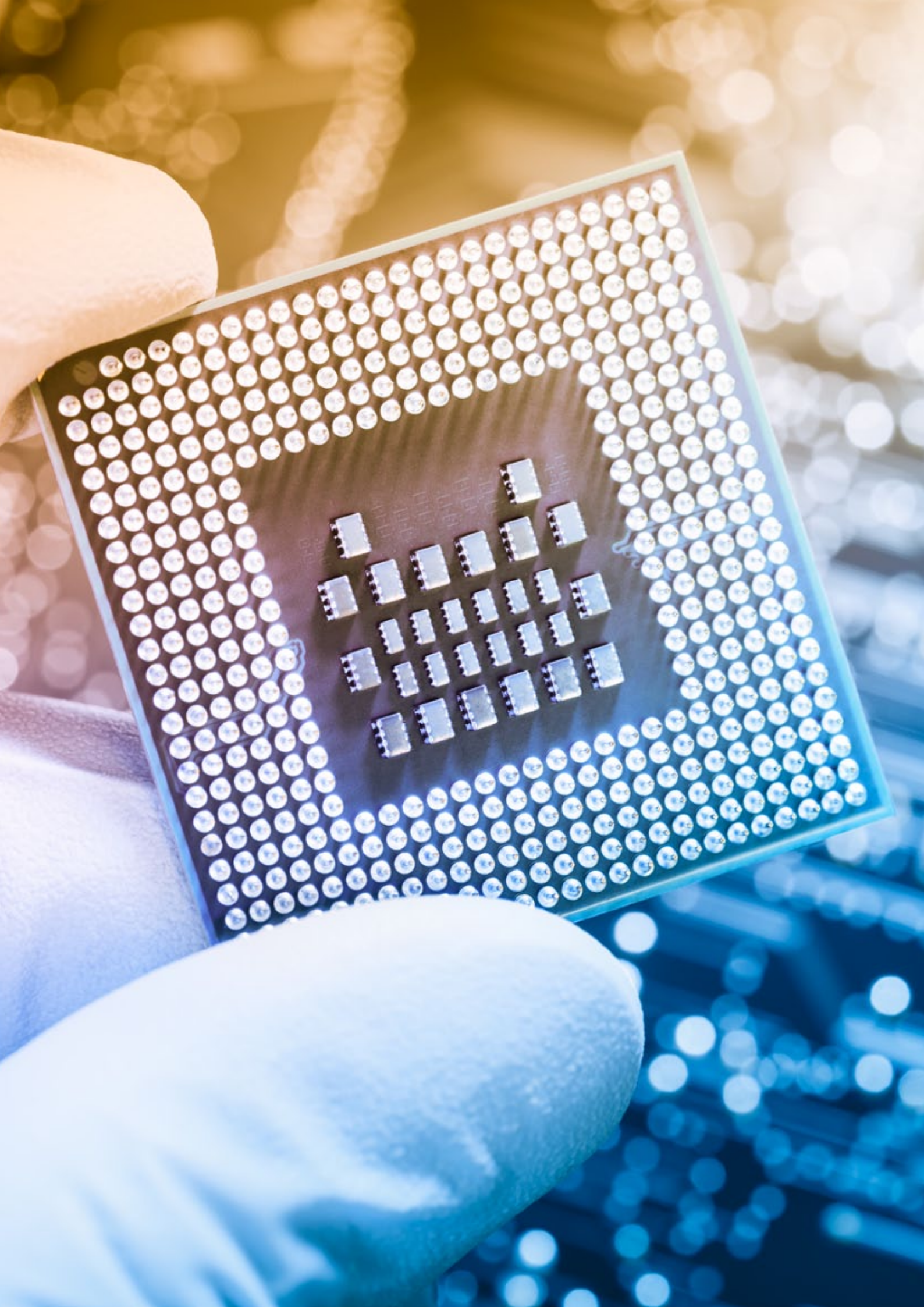
RECOMMENDATION 7

Promote human flourishing by exploring innovative ways of governing data and its use that are enabled by PETs.

The Department for Digital, Culture, Media and Sport (DCMS), the Centre for Data Ethics and Innovation (CDEI), Office for AI, regulators and civil society should 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.

95. Which? 2018 Control, Alt or Delete? The future of consumer data (see https://www.which.co.uk/policy/digitisation/2659/control-alt-or-delete-the-future-of-consumer-data-main-report, accessed 12 February 2019)

96. Thornhill J. 2018 There is a 'third way' for Europe to navigate the digital world. *Financial Times*.



Appendices

Left

Appendix

Index of case studies

Working Group members

The members of the Working Group involved in this report are listed below. Members acted in an individual and not a representative capacity, and declared any potential conflicts of interest. Members contributed to the project on the basis of their own expertise and good judgement.

Chair
Prof Alison Noble FRS FREng OBE, Technikos Professor of Biomedical Engineering and Department of Engineering Science, University of Oxford

Members
Guy Cohen, Strategy and Policy Lead, Privitar
Prof Jon Crowcroft FRS FREng, Marconi Professor of Communications Systems in the Computer Lab, University of Cambridge; Alan Turing Institute
Dr Adrià Gascón, Research Fellow, Alan Turing Institute
Marion Oswald, Senior Fellow, Department of Law, University of Winchester
Professor Angela Sasse FREng, Professor of Human-Centred Security, University College London

Royal Society staff

Royal Society secretariat
Dr Natasha McCarthy, Head of Policy, Data
Dr Franck Fourniol, Policy Adviser and Project Lead

Royal Society staff who contributed to the development of the project
Dr Claire Craig CBE, Chief Science Policy Officer
Jessica Montgomery, Senior Policy Adviser
Dr Mahlet Zimeta, Senior Policy Adviser (from January 2019)
Jennifer Panting, Policy Adviser
Connie Burdge, Project Coordinator
Louise Pakseresht, Senior Policy Adviser (until September 2018)
Lindsay Taylor, Policy Adviser (until September 2018)
Ellen Phillipson, Project Coordinator (until December 2018)
Mark Pickering, Oliver Watson, Verity Smith, Policy interns (various periods)

Reviewers

This report has been reviewed by expert readers and by an independent Panel of experts, before being approved by Officers of the Royal Society. The Review Panel members were not asked to endorse the conclusions or recommendations of the report, but to act as independent referees of its technical content and presentation. Panel members acted in a personal and not a representative capacity. The Royal Society gratefully acknowledges the contribution of the reviewers.

Reviewers
Dr Clifford Cocks FRS CB, Independent
Professor Alison Etheridge FRS OBE, Professor of Probability, University of Oxford; Fellow, Magdalen College, Oxford
Professor Jim Norton FREng, Chair, Royal Academy of Engineering Community of Practice in Digital Systems Engineering; Pro-Chancellor, Coventry University
Giles Pavey, Global Head, Data Science, Unilever
Alex van Someren, Managing Partner, Amadeus Capital Partners; Member, Science, Industry and Translation Committee, The Royal Society

Expert readers who provided comments on the draft report
Professor Anthony Finkelstein FREng CBE, Chief Scientific Adviser for National Security; Professor of Software Systems Engineering, UCL
Professor Carsten Maple, Professor of Cyber Systems Engineering, WMG's Cyber Security Centre
Dr Rachel Player, Postdoctoral Researcher, Information Security Group – Royal Holloway University of London
Dr Andrew Powell, Government Office for Science
Dr Philippa Westbury, Senior Policy Adviser, The Royal Academy of Engineering

Workshop participants

The Royal Society would like to thank all those who contributed to the development of this Project, in particular through attendance at events:

Workshop

The potential of PETs: how can privacy enhancing technologies deliver societal and business needs in the near term? (16 May 2018)

35 participants from academia (including computer science, ethics, law), industry, government and civil society.

Workshop

PETs: state of play of the technology and its implementation (18 July 2018)

38 participants from academia, industry, government and civil society.

Roundtable

The Royal Society PETs project and how to ensure the UK makes the best use of PETs (4 September 2018)

15 participants including representatives from different government departments.

The Royal Society is a self-governing Fellowship of many of the world's most distinguished scientists drawn from all areas of science, engineering, and medicine. The Society's fundamental purpose, as it has been since its foundation in 1660, is to recognise, promote, and support excellence in science and to encourage the development and use of science for the benefit of humanity.

The Society's strategic priorities emphasise its commitment to the highest quality science, to curiosity-driven research, and to the development and use of science for the benefit of society. These priorities are:

- Promoting excellence in science
- Supporting international collaboration
- Demonstrating the importance of science to everyone

For further information
The Royal Society
6 – 9 Carlton House Terrace
London SW1Y 5AG

T +44 20 7451 2500
E science.policy@royalsociety.org
W royalsociety.org

Registered Charity No 207043

ISBN: 978-1-78252-390-1
Issued: March 2019 DES5759