**1. The specific impacts on the enjoyment of the right to privacy caused by the use of artificial intelligence including profiling, automated decision-making and machine-learning technologies (hereinafter referred to in short as “AI”) by governments, business enterprises, international organisation and others. Of particular interest is information concerning:**

1. **Relevant technological developments, the driving economic, politicial and social factors promoting the use of AI and the main actors in and beneficiaries of deploying and operation AI (developers, marketers, users);**

1.1 **Artificial Intelligence (AI)** can be described conceptually as the ability of a machine to perceive and respond to its environment independently and perform tasks that would typically require human intelligence and decision-making processes, but without direct human intervention.

1.2 AI applications can be found in many aspects of our lives, from agriculture to industry, communications, education, finance, government, service, manufacturing, medicine, and transportation.

1.3 Intelligence agencies in the State of Mauritius are bound by Section 9 of the Constitution, namely the “Right to privacy of home and other property” when it comes to the use of Artificial Intelligence (AI) for intelligence gathering purpose. Provisions of Section 9 can be found at ***Annex I***.

1.4 The State of Mauritius has deployed AI in its operations and policing for public safety, namely in the following four primary areas;

1. **public safety video and image analysi**s;
2. traffic safety systems (Fixed Speed Cameras/ Photographic Enforcement Device) are installed at strategic location to identify violations and enforce the rules of the road;
3. CCTV Cameras integrated with audio recording system have been installed in Police Stations/Police Posts and CCID:
4. to promote security and safety;
5. to enhance service delivery;
6. to promote more accountability and transparency;
7. to use as a management tool to uphold discipline and promote best policing practices;
8. to use CCTV footages as evidence in cases where the attitude and demeanour of parties concerned are being questioned in the course of an investigation; and,
9. to assess the quality of service delivery and review it, as and when required, for the betterment of the service;
10. **DNA analysi**s;
11. DNA analysis where AI can also benefit the law enforcement community from a scientific and evidence processing standpoint. This is particularly true in forensic DNA testing, which has had an unprecedented impact on the criminal justice system over the past several decades. Forensics uses biological material, such as blood, saliva, semen, and skin cells, which can be transferred through contact with people and objects during the commission of a crime. As DNA technology has advanced, so has the sensitivity of DNA analysis, allowing forensic scientists to detect and process low-level, degraded, or otherwise unviable DNA evidence that could not have been used previously. For example, decades-old DNA evidence from violent crimes such as sexual assaults and homicide cold cases is now being submitted to laboratories for analysis. As a result of increased sensitivity, smaller amounts of DNA can be detected, which leads to the possibility of detecting DNA from multiple contributors, even at very low levels.
12. **forensic;**
13. Photo Sketches using Facial Identification Techniques (FITS) in relation to reported Police Cases advanced considerably in the past few years, as a result of the advancements in the field of AI;
14. AI algorithms are being used in medicine to interpret radiological images, which could have important implications for the criminal justice and Police medical examiners when establishing cause and manner of death;
15. **crime forecasting;**
16. crime forecasts allow for more efficient allocation of policing resources. The Safe City Project comprises installation of 4000 Intelligent Video Surveillance (IVS) and 300 Intelligent Traffic Surveillance cameras at different sites where traffic and illegal activity/offences can be monitored. The IVS often rely on facial images to help establish an individual’s identity and whereabouts;
17. AI is also helping to identify the potential for an individual under criminal justice supervision to reoffend. The Criminal Attribute Database (CADB) uses structured data, fingerprint and defines relationship between an individual, offence, trial and conviction;
18. Supreme Court Website where with AI, volumes of information on law and legal precedence, social information, and media can be used to suggest rulings, identify criminal enterprises, and predict and reveal people at risk from criminal enterprises;
19. assistance to victims in the investigations of Gender Based Violence (GBV) using the Mobile App ‘Lespwar’. Additional information on the App can be found at **Part 2 of *Annex I.***

1.5 AI is also used in the education sector, whereby the Ministry of Education, Tertiary Education, Science and Technology along with the educational institutions falling under its aegis, are repositories that host, collect, manage and use student data. These are meant to personalize learning and improve overall student outcomes and achievement. Moreover, the advent of digital technology and the current COVID-context is accelerating the shift to blended learning and AI-based Learning Management Systems- a powerful and cost-effective tool to achieve learning goals.

1.6 The State of Mauritius is also envisaging to enact the Mauritius Emerging Technologies Council Bill which has as aim to promote high quality research in emerging technologies including the AI technology and provide for the establishment of the Mauritius Emerging Technologies Council. The objects of the Council shall be to:

1. advise the Government on the formulation of national policies and strategies in emerging technologies;
2. promote the application of emerging technologies in line with national, economic and social objectives;
3. advise the Government on matters related to emerging technologies with respect to their adoption, use, development, harnessing, value and wealth creation, research and innovation and capacity building;
4. advise on the establishment and sustainability of an appropriate ecosystem in the field of emerging technologies and other emerging technologies; and
5. facilitate and coordinate the implementation of ready-made emerging technologies solutions in Mauritius to boost the national economy.

1.7 Moreover, the State of Mauritius, through the Ministry of Information Technology, Communication and Innovation is initiating steps to implement a chatbot which will assist service providers including Ministries in delivering customer services.

1. **Ways, in which AI can help promote and protect the right to privacy;**

1.8 The right to privacy is mostly governed by the Mauritian **Data Protection Act (DPA) 2017**. The object of the DPA is to provide for the protection of the privacy rights of individuals in view of the developments in the techniques used to capture, transmit, manipulate, record, or store data relating to individuals.

1.9 Under the DPA, the general principle is that the consent of an individual is required before the sharing of personal data can be done and that individual must under Section 23, be informed of same at the time of collection of the personal data.

1.10 The DPA requires a lawful basis for processing personal data under Section 28. Besides, Section 21 provides for the principles to the processing of personal data. In addition to the principles of fairness, accountability and transparency, the core principles of purpose limitation and data minimisation which have implications for the development, use and application of AI systems have been included in the DPA.

1.11 The DPA also provides the rights of the data subjects in Part VII such as the right of access, right not to be subject to automated decision-making including profiling, right to rectification, restriction and erasure and right to objection. Section 38 of the Act limits the use of automated decision-making in certain circumstances and requires individuals to be provided with information as to the existence of automated decision-making, the logic involved and the significance and envisaged consequences of the processing for the individual. ***Annex 1*** provides the relevant detailed sections applicable.

1.12 The DPA was also amended to comply with the new EU Data Protection Regulations, which came in force in May 2018 to strengthen privacy rights, while establishing a secure legal environment for the safe transaction of personnel data locally and abroad.

1.13 The DPA is technology-neutral and provides no constraint for the successful adoption of new technologies, in particular AI. On the contrary, it is meant to foster the application of any technology to the processing of personal data whilst in full respect of human values and fundamental rights. It is worth noting that the DPA already addresses the various concerns raised by the Human Rights Council Resolution.

1.14 The DPA also creates conditions that are conducive to the respect for human rights by AI actors and do not create barriers to effective accountability and remedy for AI related human rights violations comprising *inter alia:*

1. key definitions such as personal consent and personal data are introduced;
2. new concepts such as data protection impact assessments, data breaches notifications, voluntary certification mechanism, data protection seals and right to object;
3. simplify the complaints mechanism and the procedures related to hearings conducted by the Data Protection Office;
4. Section 3 of the Act shall not apply to:
5. the exchange of information between Ministries, Government departments and public sector agencies where such exchange is required on a need-to-know basis; and
6. the processing of personal data by an individual in the course of a purely personal or household activity.
7. Section 30 of the DPA provides for the protection of the personal data of a child.

1.15 An organisation developing or utilizing AI is bound by the same legal constraints as any other organisation that is processing personal data. To promote and protect the right to privacy, controllers/processors developing AI must:

1. incorporate privacy by design - The controller shall build privacy protection into the systems and ensure that data is properly safeguarded. This is a requirement as per Section 31 of the DPA and applies when developing software. Data protection must therefore be given due consideration in all stages of system development;
2. conduct a Data Protection Impact Assessment to manage privacy risks as per Section 34 of the DPA;
3. apply data protection principles as per Section 21 of the DPA. E.g. only the data types necessary to create the AI must be collected for the purpose specified;
4. identify lawful basing for processing the data under Section 28;
5. use Privacy Enhancing Technologies (PETs); and
6. use good data sets- AI system must be build using accurate, fair and representative data sets.

1.16 Moreover, under Part III of the **Computer Misuse and Cybercrime Act 2003,** any investigatory authority may apply to the Judge in Chambers for

1. Preservation order (Section 11),
2. Disclosure of Preserved Data (Section 12),
3. Production Data (Section 13),
4. Powers of access, search and seizure for the purposes of investigation (Section 14)
5. Real time collection of traffic data (Section 15) and
6. Deletion order (Section 16)

with respect to access to data and to prevent abuses.

1. **Challenges posed by the use of AI for the effective exercise of the right to privacy and other human rights, including features and capabilities of AI that present existing or emerging problems.**

1.17 AI is increasingly infiltrating many aspects of our lives. The distinct benefits that AI can bring is understandable, but it can also pose risks to the rights and freedoms of individuals. A list of the unique challenges that AI poses to privacy is as follows:

1. AI technology is not confined to one state or jurisdiction, making it difficult to create and maintain good privacy practices and governance across borders.
2. The diversity of AI applications, systems and uses: *Different types of AI and different domains of application raise distinct ethical and regulatory privacy concerns.[[1]](#footnote-1)*
3. Lack of algorithmic transparency and accountability – *Many companies developing critical AI systems do so in inscrutable ways due to the complexity of methods used.* *Individuals are granted little control and oversight over how their personal data is used to draw inferences about them.*
4. Challenges come when it comes to effectively regulating AI technology. Determining who owns the data, where it is stored and who has responsibility for it is a complex task for regulators.
5. Cyber Security Vulnerabilities - *A RAND perspectives report Osoba and Welser (2017)[[2]](#footnote-2) highlights various security issues related to AI, for example, fully automated decision-making leading to costly errors and fatalities; the use of AI weapons without human mediation; issues related to AI vulnerabilities in cyber security.*
6. Unfairness, bias and discrimination - *Because algorithms are trained on existing data, they can end up replicating unwanted patterns of unfairness due to the data they have ingested.*
7. **Discriminatory impacts of the use of AI.**

1.18 Section 16 of the Constitution, inter alia, provides that *“no law shall make any provision that is discriminatory either of itself or in its effect”.* The term “discriminatory” is defined as *“affording different treatment to different persons attributable wholly or mainly to their respective descriptions by race, caste, place of origin, political opinions, colour, creed or sex whereby persons of one such description are not made subject or are accorded privileges or advantages that are not accorded to persons of another such description*”.

1.19 From the ICT regulatory perspective, artificial intelligence is a new technology which is being used for different purposes. The usual approach of the ICT regulator is to be technology neutral, meaning that, it is how this technology is being used which is of interest to the regulator and not the technology in itself. This, in turn, implies a thorough understanding of how AI works in order to be able to identify the necessary safeguards to be put in place to prevent privacy breaches.

1.20 The mode of operation of AI is undertaken through the use of algorithms. An algorithm is a step-by-step procedure or a set of instructions whose application makes it possible to solve a stated problem. Algorithms are used for calculation, data processing, and automated reasoning.

1.21 AI on the other hand, is a group of algorithms that can modify its own algorithms and create new algorithms in response to learned inputs and data as opposed to relying solely on the inputs it was designed to recognise as triggers. This ability to change, adapt and grow based on new data, is described as “intelligence.”

1.22 The underlying issue to be looked into by the ICT regulator is, therefore, in terms of the algorithms used for AI.

1.23 The issue of how artificial intelligence (AI), including profiling, automated decision-making and machine-learning technologies may, without proper safeguards, affect the enjoyment of the right to privacy is indeed a multifaceted topic which requires the attention of different stakeholders.

1.24 Moreover, the use of AI solutions should not be countenanced for final decisions, but only as part of decision-support in certain areas, for example, judicial or medical decision-making. Possible bias and discriminatory effects must be checked and corrected before the roll-out of an AI solution and at regular intervals throughout its lifetime.

1. **The interlinkages between the promotion and protection of the right to privacy in the context of the use of AI and the exercise of other human rights (including the rights to health, social security, an adequate standard of living, work, freedom or expression and freedom of movement);**

1.25 The demands of public security, efficient administration, economic development and the ever rapid growth of new communications devices which integrate information and communications technologies must not jeopardize our privacy rights. Data protection, which strikes the right balance between the concerns of Government and businesses, whilst respecting the fundamental rights of people, is the guiding principle of the Data Protection Office.

1.26 The key principle underpinning data protection is to ensure that people know to control how personal information about them is used or, at the very least, to know how others use that information. Data controllers are people or organisations holding information about individuals and they must comply with the data protection principles in handling personal data, and “data subjects” are individuals who have corresponding rights.

1.27 All AI solutions must respect the rule of law, human rights, democratic values and diversity. Therefore, every planned AI solution, including algorithms, should undergo a timely human rights assessment, including ethical and equality assessments. The right to equal treatment must not be unlawfully violated by the planned AI solution.

1.28 Both the right to privacy and human rights emphasizes on transparency in AI system/solutions. The use of an AI system in any decision-making process that has a meaningful impact on a person’s privacy and human rights needs to be identifiable. AI system must not only be made public in clear and accessible terms but individuals must also be able to understand how decisions are reached and how those decisions have been verified.

1.29 Privacy by design and by default necessitates a data protection assessment in the planning phase of how any human rights, including the right to privacy, might be affected by the implementation of the AI solution.

**2. Legislative and regulatory framework, including**

**(a) Information on relevant existing or proposed national and regional legislative and regulatory frameworks and oversight mechanisms;**

2.1 The State of Mauritius has a panoply of laws governing Information and Communications Technology such as the:

1. the **Code Civil Mauricien** under Article 22;
2. the **Data Protection Act 2017**;
3. the **Information and Communication Technologies Act 2001**;
4. the **Computer Misuse and Cybercrime Act 2003**;
5. the **Prevention of Terrorism Act 2002**;
6. the **DNA Identification Act 2009**;
7. the **Electronic** **Transactions Act 2000**; and
8. the **Civil Aviation Regulations 2007**.

2.2 The relevant sections of the above mentioned legislations can be found at ***Annex I***.

2.3 Moreover, as mentioned above in paragraph 1.5, the State of Mauritius, through the Ministry of Information Technology, Communication and Innovation has initiated steps for the enactment of the Mauritius Emerging Technologies Council Bill as well as the Cybersecurity and Cybercrime Bill. They aim at promoting emerging technologies including AI technology and better safeguarding individual’s rights against cybercrime, respectively.

**(b) Analysis of related human rights protection gaps, ways to bridge those gaps and barriers to advancing effective, human-rights based regulation of AI;**

2.4 There are risk factors associated with algorithms, which are tools subject to misuse. The importance they have gained and the abuses they may cause warrant proper monitoring for the eventual deployment of proper safeguards. This involves transparency, i.e. the means to make the underlying logic understandable. Transparency cannot simply be declared. It is a particularly complex task to check the integrity of the algorithms used by companies. Transparency will be effective only if it results from regular dialogue with operators. The key principles for action by the public authorities, therefore, clearly need to be defined by legislation in order to impose transparency on the algorithms.

2.5 Subsequently, the regulator will need to have the resources to do so by using statistical measures through the use testing tools and third-party certification or compliance mechanisms. In practice, it will particularly be necessary to establish a proper equilibrium between the principle of transparency and the protection of business secrecy.

2.6 Beyond the technical and legal issues surrounding algorithms and their transparency, the aim of regulation will be to bring the ethical issues such as privacy concerns raised by algorithms used in AI into the public debate, to clearly reveal the “algorithmic policy”.

2.7 Examples of questions on the range of issues which need to be factored into the algorithmic transparency framework include;

1. What data is used to train the algorithms? How is it collected? Is it personal data?
2. What data is used in the algorithm’s input parameters?
3. Does this data present biases?
4. What is the processing flow followed?
5. What supervisory/monitoring mechanisms are used in algorithmic learning?
6. Does the algorithm reproduce biases? Can it be misused? What are potential abuses to avoid?
7. What are the false positive/false negative rates?
8. Which metrics can be used to report on the algorithm’s performance?
9. What procedures are used to correct errors?

2.8 Moreover, regarding the education sector, while there are several benefits that can be derived from the use of new technology, it becomes important at the same time to address student data privacy and security to ensure safety and welfare of all students, in particular minors. This would require:

1. new legislation and regulations to protect student data on platforms such as Learning Management Systems, Educational Management Information Systems and Educational Portals;
2. all educational institutions to have a transparent set of policies for student privacy
3. good governance processes about usage, storage and disclosure, to minimise collection of personal student data and keeping it only for as long as necessary for the provision of educational services;
4. regular review of security practices and safeguards
5. employees who handle or have access to personal information must have undergone the required training. Students, too need to taught to be safe and responsible in sharing personal data online, on social media, via apps on tablets and smartphones; and
6. responding to parents' rights and concerns about the privacy and safety of their children

**(c) Assessments of the need to prohibit certain AI applications or use cases (“red lines”).**

2.9 Use cases for AI are increasingly based on sensitive personal information, which has raised much public concern about how unfair societal bias, developer bias, and model bias could impact decisions and ultimately lead to discrimination against data subjects.

2.10 The European Data Protection Supervisor (EDPS) remarks that the protection of fundamental rights might warrant, in certain scenarios, not only specific safeguards but also a clear limitation on the use of AI where certain uses of the technology are evidently incompatible with fundamental rights. Some high-risk AI scenarios should also be forbidden from the outset. Following the European precautionary principle approach, and in particular, when the impact on individuals and society as a whole is not yet fully understood, a temporary ban should also be considered. These potential situations should be explicitly addressed in any possible future regulatory framework. The ‘cautious’ and ‘risk-adapted’ approach as proposed by the German Data Ethics Commission, by completely or partially banning algorithmic systems ‘with an untenable potential for harm.’

**3. Other safeguards and measures to prevent violations of privacy when using AI, and address and remedy them, where they occur, including**

**(a) Self-governance approaches by business enterprises to regulate AI applications, which meet the companies’ responsibilities to respect the right to privacy.**

3.1 Organizations should be proactive and prepared to consider the unique governance and risk implications as they are embarking on their AI journey, and help shape those frameworks and principles.

3.2 In order to govern AI, businesses can make use of various mechanisms consisting of formal structures connecting business, IT, data, model, system management functions, formal processes and procedures for decision-making and monitoring as well as practices supporting the active participation of and collaboration among stakeholders.

3.3 Risk mitigation can be based on international standards such as those published jointly by the International Organization for Standardization and the International Electrotechnical Commission in the ISO/IEC 27000 series (information security management systems). In particular, ISO/IEC 27701 contains data privacy extensions establishing at the minimum measures for:

1. Protection: controls to protect against the effects of assessed risks;
2. Detection: controls to detect abnormalities as soon as possible; and
3. Responding: controls to contain and defeat the risk of abnormal events and to ensure that core business processes can still function until such time as the overall solution is found and the situation returns to normal1.

3.4 Mauritian organisations implementing AI applications will need to abide by the overall provisions of the DPA and other applicable laws for the proper use and governance of AI applications.

**(b) Human rights due diligence in the context of the use of AI by governments, business enterprises and international organisations;**

3.5 Human rights due diligence is critical to any legislative, policy, measures or programmes undertaken by any State. There is a need to ensure that the fundamental rights and freedoms are duly protected throughout. The impacts of the new initiative should be considered and necessary actions be taken to limit or mitigate restrictions and violations of human rights.

3.6 Moreover, appropriate sensitization/guidelines and self-regulation should be adopted to ensure adequate responsibility by all stakeholders. Another important aspect remains the enforcement of agreed laws, agreed methodologies and approach. Adequate resources should be provided thereto. Furthermore, an appropriate independent body should be set up or under operation allowing any aggrieved individual whose fundamental rights have been violated to claim violations and obtain effective remedy. AI is no exception to this human rights due diligence.

3.7 In the State of Mauritius, the Data Protection Office is the enforcing body responsible for protecting privacy rights of individuals. Each and every controller and processor must, before collecting and processing personal data, register himself with the Data Protection Commissioner. This registration will be valid for a period of 3 years.

3.8 The Data Protection Office has also issued a Code of Practice which came into operation on 30 October 2020. The Code of Practice sets out the basic conditions for the use of Safe City systems operated by the Mauritius Police Force (MPF) in accordance with the provisions of the Data Protection Act 2017 (DPA). It is the responsibility of the MPF to monitor the compliance of this Code of Practice and to register as a controller with the Data Protection Office. All officers involved in the Safe City system(s) must read, understand and adhere to this Code of Practice.

3.9 As per Section 5 of the DPA 2017, the Data Protection Commissioner can investigate any complaint or information which gives rise to a suspicion that an offence may have been, is being or is about to be, committed under this Act.

3.10 When personal data is collected, the data controller must be able to provide some general information such as:

1. the identity of the data controller (User login and password). New requirements such as pseudo-ny-misation and encryption are introduced in DPA 2017;
2. when and where the data was accessed;
3. how the data controller can be contacted;
4. the purpose of processing;
5. the legal basis for processing;
6. the categories of personal data that are processed; and
7. the data subjects’ right to inspect the data; and, where possible, the envisaged time limits for the erasure of the different categories of data (for ex. Stored data relating to CCTV camera footages are automatically wiped off after 30 days).

3.11 Moreover, with regards to human rights and businesses, the United Nations Guiding Principles on Business and Human Rights (UNGPs) which is a fairly new concept in the Mauritian business landscape, addresses issues such as the state duty to protect human rights and the corporate responsibility to respect human rights. Appropriate sensitisation about the guidelines are being effected with relevant stakeholders including the private sector for consideration and its incorporation in the various processes by the business enterprises and the relevant public bodies.

 **(c) Data governance models, such as data trusts, that provide effective protection to the right to privacy in data-intensive environments**

3.12 Data Institute’s definition of data trusts as a starting point, namely, that a data trust must have a clear purpose; a legal structure, constitution and trustees; (some) rights and duties over stewarded data.[[3]](#footnote-3) Data trusts reflect a move away from existing individual consent-based models of data governance towards a framework based on common law trust principles. As proposed, a data trust would direct and manage access, consent and use rights to data sets through a trustee empowered with certain authority and fiduciary obligations to persons whose data resides in the data trust. A data trust would direct and manage access, consent and use rights to data sets through a trustee empowered with certain authority and fiduciary obligations to persons whose data resides in the data trust.[[4]](#footnote-4)

3.13 This approach, as documented in an [Element AI whitepaper](https://hello.elementai.com/data-trusts.html)4, is intended to provide individuals greater control over their personal information, enhance privacy, and give the public the opportunity to “share in the value of data and artificial intelligence.” Element’s whitepaper builds on a recent workshop in which representatives from numerous fields, including data governance, machine learning, privacy, public policy, and property law, provided perspectives on the utility of data trusts to enable the development of ethical AI.

3.14 However, the journey to becoming a data-driven organization fit for the emerging AI economy is long and arduous. Data trusts are an opportunity for collaboration between organizations to make that journey faster, less costly, and less risky.

3.15 Data trust is critical to consider if the use of AI will emerge and grow significantly.

**(d) Technological applications that could help adequately protect the right to privacy when applying AI and their limits.**

3.16 AI solutions must be clear from the outset to the final switch-off and decommissioning stages with respect to what data are processed in the AI solution, what parameters and data quality metrics provide the basis for the decision-making and how they will be balanced and weighted against each other. The results must be monitored continuously and corrected if necessary. In the area of automated decision-making solutions, no decisions are to be made based on conscious or unconscious bias.

3.17 Some of the technological applications are:

1. Cryptographic algorithms (Homomorphic Encryption, Secure multi-party computation (SMPC), Differential privacy)– E.g. differential privacy protects from sharing any information about individuals. This cryptographic algorithm adds a “statistical noise” layer to the dataset which enables to describe patterns of groups within the dataset while maintaining the privacy of individuals[[5]](#footnote-5); and
2. Data masking techniques.

3.18 AI systems must always remain under human control, even in circumstances where machine learning or similar techniques allow for the AI system to make decisions independently of specific human intervention.

1. https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf [↑](#footnote-ref-1)
2. OA Osoba, W Welser IV - The risks of artificial intelligence to security and the future of work

RAND Corporation Santa Monica (2017)-https://www.rand.org/pubs/perspectives/PE237.html [↑](#footnote-ref-2)
3. Data Trusts A New Tool for Data Governance - <https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf> [↑](#footnote-ref-3)
4. Data Trusts: A Pathway to “Ethical” AI or a Solution in Search of a Problem? - <https://www.lexology.com/library/detail.aspx?g=fdaf4ff6-2007-42df-859d-b348604152c0> [↑](#footnote-ref-4)
5. <https://research.aimultiple.com/privacy-enhancing-technologies/> [↑](#footnote-ref-5)