Forthcoming in Computer Law & Security Review

Artificial Intelligence as a Service: Legal Responsibilities, Liabilities, and Policy Challenges

*Jennifer Cobbe and Jatinder Singh**

Abstract: Artificial Intelligence as a Service ('AIaaS') will play a growing role in society's technical infrastructure, enabling, facilitating, and underpinning functionality in many applications. AIaaS providers therefore hold significant power at this infrastructural level. We assess providers' position in EU law, focusing on assignment of controllership for AIaaS processing chains in data protection law and the availability to providers of protection from liability for customers' illegal use of AIaaS. We argue that in data protection law, according to current practice, providers are often joint controllers with customers for aspects of the AIaaS processing chain. We further argue that providers lack protection from liability for customers' illegal activity. More fundamentally, we conclude that the role of providers in customer's application functionality – as well as the significant power asymmetries between providers and customers – challenges traditional understandings of roles and responsibilities in these complex, networked, dynamic processing environments. Finally, we set out some relevant issues for future regulation of AIaaS. In all, AIaaS requires attention from academics, policymakers, and regulators alike.

Keywords: *cloud computing, artificial intelligence, data protection, intermediary liability, internet consolidation, internet regulation*

* Compliant and Accountable Systems Group, Department of Computer Science and Technology, University of Cambridge (firstname.lastname@cst.cam.ac.uk). We acknowledge the financial support of the University of Cambridge (through the Cambridge Trust & Technology Initiative), the UK Engineering and Physical Sciences Research Council (EPSRC) (through grants EP/P024394/1 and EP/R033501/1), and Microsoft, through the Microsoft Cloud Computing Research Centre. Thanks to Reuben Binns, Jon Crowcroft, and the anonymous reviewers for their helpful feedback on earlier drafts of this paper.

1. Introduction

Cloud computing now underpins many websites, mobile apps, and other internet-connected services (collectively referred to as ‘applications’, encapsulating a range of software, including websites, mobile applications, online services, and so on). Cloud providers make available, as a service, various assortments of technical infrastructure that support applications. Cloud services have seen significant uptake, as application developers seek to benefit from reduced barriers to entry and lower operating costs brought about by providers’ economies of scale. Many cloud services are now available – the common term *Anything-as-a-Service*[1] reflects that most any technical infrastructure component is available as a service.

In recent years, various cloud providers have begun to offer *Artificial Intelligence as a Service* (‘AIaaS’). ‘AI’ here refers to machine learning models trained on data that can be presented with new data to gain insights into that new data by making predictions and classifications[2]. Though the phrase ‘Artificial Intelligence’ is overused – sometimes describing even simple algorithmic systems – we adopt ‘Artificial Intelligence as a Service’ in accordance with dominant industry use of the term, referring to pre-trained models provided to customers on a commercial basis. Customers send inputs to the service and receive back the AI analyses’ result, giving on-demand access to various AI-backed capabilities such as object recognition, face detection, speech transcription, and so on. Results returned from an AI service will directly influence the capabilities of the application itself – that is to say, unlike traditional cloud services that support application deployment (such as hosting and storage), AI services are intrinsic to some of the application’s functionality.

The nature of many AI technologies – requiring large quantities of training data, specialised hardware for building and training models, data centres to provide real-time analysis, and

[1] Yucong Duan, Guohua Fu, Nianjun Zhou, Xiaobing Sun, Nanjangud C. Narendra, and Bo Hu, ‘Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends’ [2015] *2015 IEEE 8th International Conference on Cloud Computing*, June, 621–628.

[2] The terms AIaaS and also Machine Learning as a Service (MLaaS) are sometimes also used to refer to services that allow customers to build and train their own bespoke models (see §2.2.1).

technical expertise in machine learning – raises costs of entry higher than many organisations can meet. By offering AI 'as a service', large cloud providers with substantial resources can derive revenue, while smaller companies – who may lack the skills, data, and resources to develop their own systems – can take advantage of state-of-the-art technologies that may otherwise be beyond their reach. Indeed, Amazon markets their AIaaS with the line "Build an AI-driven application – No machine learning experience required"[3]. As a result, AIaaS allows customers to embed AI capabilities in a much wider range of applications than might otherwise be possible. Indeed, AIaaS potentially enables functionality in a range of applications in both physical and virtual spaces; in websites, mobile apps, and so on, and in homes, vehicles, offices, shops, factories, commercial premises, public areas, and anywhere else with internet-connected services, systems, and devices.

The AIaaS market is set for rapid growth[4]. As AIaaS greatly lowers the barriers to entry to state-of-the-art capabilities, much public and private use of AI will likely come to rely on providers' services, rather than on bespoke systems developed in-house. As such, AIaaS raises several legal, regulatory, and policy questions. Some relate to the difficulties of assigning legal responsibilities and liabilities in these complex processing environments. Others relate to the general implications of these powerful technologies working to both determine and drive the functionality of customer applications. Consolidation of AIaaS around a small number of companies that already dominate other digital and internet-connected services further entrenches those companies at an infrastructural level and confers greater power upon them. That providers also use customer data to improve their models raises concerns about privacy and the ability of providers to leverage their dominant position in this sector to develop systems that give them in advantage in others. The cross-border supply chains relied upon for developing systems can allow providers to evade responsibilities in data protection law. The potential for AIaaS to underpin widespread AI-augmented surveillance and analytics also risks transforming public and private spaces and

[3] Amazon Web Services, 'Explore AWS AI services' <https://aws.amazon.com/machine-learning/ai-services> accessed 13 November 2020.

[4] Markets and Markets, 'Artificial Intelligence as a Service: Market Research Report' (2018) <https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-ai-as-a-service-market-121842268.html> accessed 13 November 2020.

altering power dynamics and balances of rights and interests. Moreover, the potential for misuse and abuse of AI services, readily and cheaply available for deployment at scale, is a serious problem that requires attention. As a result of these concerns, AI services should receive close scrutiny from regulators and policymakers.

In this paper, we explore some of the legal responsibilities of AIaaS providers and highlight some of these legal, regulatory, and policy challenges that AI services present. We first describe AIaaS in more detail – distinguishing it from traditional cloud offerings, identifying common AI services offered by the major providers, and setting out key actors and stages in the AIaaS data processing chain. Next, we assess the current legal position of AIaaS providers in terms of their data protection responsibilities and potential liability for unlawful use of AI services, focusing our analysis in particular on key provisions of two relevant EU frameworks: the General Data Protection Regulation[5] ('GDPR') and the E-Commerce Directive[6]. In doing so, we assess the assignment of responsibilities in the AIaaS processing chain and highlight several potential legally difficult issues for providers, including around data controllership and their protection from liability for illegal activity undertaken by customers using their services. We discuss whether existing legal frameworks can contend with the emergence of complex, networked, and dynamic processing arrangements and relationships such as in AIaaS, with significant asymmetries in power and technical capacity between customers and providers. We then turn to broader issues relating to AIaaS, identifying directions for future law and regulation in four key areas: the amplification of problems that could develop with AI systems through the scale that can be reached with AIaaS; the training of these AI systems; the potential for an expansion of AI-augmented surveillance in virtual and physical spaces; and the risks of misuse and abuse of AI systems offered as a service.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 ('GDPR').

[6] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178/1) ('E-Commerce Directive').

2. Artificial Intelligence as a Service

AIaaS is a subset of cloud computing, whereby AI capabilities are offered commercially alongside other cloud services. To ground our discussion in the real-world practices of providers, we now provide a brief overview of the general nature of cloud and AIaaS, and the chain of data flow and processing in AI services.

2.1. Cloud services

Cloud computing involves the delivery of computing resources and capabilities over a network, usually the internet[7]. Cloud offerings are generally provided as *services*, in that they are typically 'rented' or otherwise provisioned on demand and billed based on usage. Cloud services ('cloud') work to underpin *applications*, which include websites, mobile apps, and other software and services. As Fig 1 illustrates, *tenants* – the customers of *cloud service providers* – leverage cloud to support their applications.

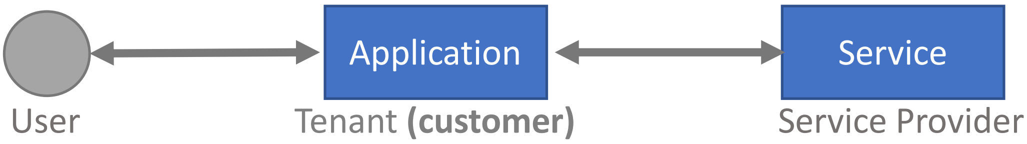

Figure 1. Simple representation of a common cloud service scenario. A ***tenant*** *operates an* ***application****, which provides functionality for their users.*[8] *The tenant, the cloud* ***service provider****'s customer, uses the provider's services to support their application.*

Traditionally, cloud was described in terms of the following service models: *Infrastructure as a Service* ('IaaS'), which involved 'lower-level' computing resources[9] (for example, virtual servers); *Software as a Service* ('SaaS'), which involved complete managed applications (for example, a pre-built webmail service that customers can brand as their own), and *Platform*

[7] Christopher Millard, *Cloud Computing Law* (2nd edn, Oxford University Press 2021).
[8] Note that depending on the particular application, the users of the tenant's services could be external to the organisation (i.e. third parties), or part of the tenant organisation itself. We expand on this later.
[9] Note that the *internet's* infrastructure level is different, and includes the technical architecture and protocols for the internetworking of and transmission across multiple networks operating around the world.

as a Service ('PaaS'), which provides various components that support application development and deployment (for example, database systems). However, there are many cloud offerings and these distinctions may blur. As such, the term *Anything as a Service* ('XaaS')[10] is increasingly used, reflecting the fact that most any computing and software infrastructure can be accessible as a service. The specifics of a tenant's cloud usage depend on the application, the tenant's requirements, and the services the provider offers. In practice, multiple cloud services, potentially from different providers, may support a particular application. Access is often 'turn-key' – tenants can leverage cloud services on demand, as required, at a few clicks, with services provided 'as-is', typically without negotiating or interacting with the provider[11].

Cloud services are ubiquitous, underpinning most applications[12], because they provide low-cost alternatives to running and managing supporting infrastructure, systems, and services in-house. For application developers, costs and barriers to entry are reduced by the on-demand, typically pay-per-use nature of cloud services, avoiding the overheads and expertise required for procuring and managing hardware and software. Cloud providers leverage economies of scale by sharing their infrastructure and expertise and reusing technical components between tenants. As technical systems become ever more pervasive, with sensors and actuators embedded in physical surroundings, cloud increasingly supports applications in both virtual *and* physical spaces – not only in websites and apps, but in homes, offices, shops, commercial premises, public areas, and, ultimately, anywhere else where internet-connected services, systems, and devices operate.

2.2. AI as a Service

'AI' is an overloaded term. In this context, AI is used in relation to *machine learning*[13] ('ML'). ML works to uncover patterns in data to build and refine representative models of that

[10] Duan et al (n 1).

[11] Services may have options for customers to configure some aspects of the service. However, the mechanism and scope for any configuration are pre-defined by the provider for the particular service.

[12] Jennifer Cobbe, Chris Norval, and Jatinder Singh, 'What lies beneath: transparency in online service supply chains' (2020) 5 *Journal of Cyber Policy* 1.

[13] Despite the focus on ML, we use 'AI' and 'AIaaS' to be consistent with the terminology used by providers in this space.

data[14]. These models can be used to make classifications, predictions, decisions, and so on with new data. To illustrate[15], a model might be developed to recognise certain objects from images. This model will be trained on a dataset containing many different images to 'learn' (statistically recognise) aspects that characterise particular objects. Once trained, the model can be presented with new images, and work to classify objects in those images.

Models and their outputs are *probabilistic*: as ML involves deriving a statistical model representing the training data provided, there will be some degree of error or uncertainty regarding their representation and outputs. The performance and operation of an ML model is determined by how it is engineered – relevant factors include the specifics of the data used for training, testing, and analysis; how the data is selected, cleaned, and processed; the machine learning methods, configurations, and parameters used to build the statistical model representing the data; any post-processing (corrections and adjustments of model outputs); and so on. ML is therefore often described as differing from traditional software engineering, where the functionality and outcomes are explicitly programmed for.

2.2.1. AIaaS in practice

AIaaS is a subset of cloud services that can encompass: *(i)* providing technical environments and resources to facilitate customers in undertaking their own ML (sometimes called 'Machine Learning as a Service'); or *(ii)* providing access to pre-built models that customers can essentially 'plug' into their applications. There are a range of possible AIaaS arrangements; for instance, some services may represent a hybrid of the above, such as those involving prebuilt or partially trained models that can be customised by the customer through additional ML operations. This paper focuses specifically on *(ii)*, the most prominent form of AIaaS*,* though aspects of our discussion may also be relevant for other AIaaS variations. As such, we use "AIaaS" to refer to *commercial offerings that allow access to*

[14] Junfei Qiu, Qihui Wu, Guoru Ding, Yuhua Xu, and Shuo Feng, 'A Survey of Machine Learning for Big Data Processing' [2016] *Eurasip Journal on Advances in Signal Processing* 1.

[15] This illustration details a *supervised* machine learning system. That is, where the system learns from input data that is labelled with the desired output. Most AI services involve supervised systems. Some services – such as anomaly detection – involve *unsupervised* machine learning. That is, where data is not labelled, but the system itself is tasked with finding patterns and correlations in the data.

generalised pre-built ML models as a service. As Fig 2 illustrates, this process entails customers[16] sending input data to providers; the ML model is then applied to those inputs; and the provider returns the results (analyses, classifications, predictions, decisions, and so on) to the customer.

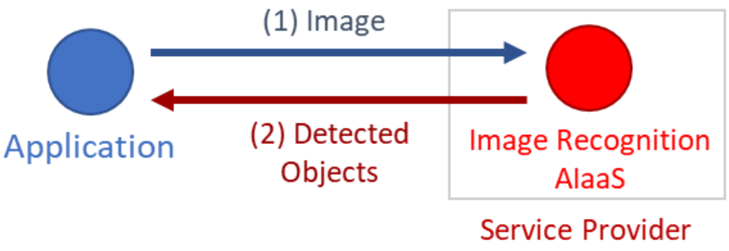

Figure 2. A simplified AIaaS scenario. An image is sent via the customer's application to the provider's image recognition service. The service analyses the image (applying the model) and returns the detected objects.

The most prominent AIaaS providers tend to be bigger technology companies with the financial and technical resources required to develop and offer complex machine learning systems. These include Amazon (through Amazon Web Services[17], or 'AWS'), Microsoft (through Microsoft Azure[18]), Google (through Google Cloud[19]), IBM (Watson)[20], though some smaller providers also exist (for example, BigML[21]). We focus on the three largest and most prominent providers – Amazon, Microsoft, and Google – as they dominate the market and collectively offer a range of services indicative of those of other providers. AI services exist in a wider ecosystem which includes, for instance, data brokers supplying both customers and providers, and training data labelling services (such as Mechanical Turk[22]).

[16] In this paper, we use the term **customer** rather than tenant as is traditionally used for cloud, as customer more naturally fits the API-based (request/response) access to models of such services. In practice, the customer is likely to use other cloud services that are more 'tenant'-like, hence the terminology persisting.

[17] https://aws.amazon.com.

[18] https://azure.microsoft.com.

[19] https://cloud.google.com.

[20] https://www.ibm.com/cloud/machine-learning.

[21] https://bigml.com.

[22] Amazon Mechanical Turk 'AWS introduces a new way to label data for Machine Learning with MTurk' (13 December 2018) <https://blog.mturk.com/aws-introduces-a-new-way-to-label-data-for-machine-learning-with-mturk-2f9c19866a98> accessed 13 November 2020.

Various AI services are available; these typically offer generic capabilities useful in many application contexts. Broadly speaking, commercial AIaaS providers offer four categories of service,[23] though others also exist:

- *Language* – for example, text sentiment analysis; translation; and knowledge base creation.
- *Speech* – for example, speech transcription; speech synthesis; and voice recognition.
- *Vision* – for example (for both still images and video), image analysis and classification; object recognition; and facial detection, analysis, or recognition[24].
- *Analytics* – for example, web usage; behavioural analysis; recommendations and personalisation; content moderation; and anomaly detection.

AI services are usually closely integrated into a provider's other cloud services, thereby offering a wide range of services that customers may employ to support their application. If a customer uses AWS hosting for their application, for example, they can readily leverage Amazon's AI services as part of that hosting package, thereby extending application functionality (though customers could also use services from other providers to support that application). This ease of integrating AIaaS with other cloud services allows customers to take advantage of cloud infrastructure to deploy AI-augmented applications at a scale that might otherwise be unreachable.

As with many cloud services, AIaaS is available 'turn-key' – on demand, with standard form contracts specified by the provider, at relatively low cost, often with only a few steps required by the customer to configure and use the service. Some providers offer AI services on a consultancy basis, working closely with the customer to tailor services to their needs

[23] See Amazon: https://aws.amazon.com/machine-learning/ai-services; Microsoft: https://azure.microsoft.com/en-gb/services/cognitive-services; and Google: https://cloud.google.com/products/ai.

[24] While all three of Amazon, Microsoft, and Google offer other vision services, only Amazon and Microsoft offer facial recognition; this is not currently part of Google's portfolio, although they do offer face detection and analysis.

(sometimes involving pre-built models that are heavily or entirely customised for the customer), though this is usually for certain higher-value customers.

2.2.2. Motivations for considering AIaaS

AIaaS warrants particular attention for several reasons. First, AI services are intrinsically tied to realising particular *functionality* in customer's applications. Traditional cloud services generally support application *deployment* – relating to operational aspects such as availability, storage, connectivity, scalability, and security. Even services more closely integrated with applications, as in PaaS, such as database services or around identity (sign-on) management, still orient towards supporting application delivery. Indeed, even for SaaS, where providers define the application itself, they still ultimately support delivery and deployment. AI services, however, play a more direct role in enabling, facilitating, and underpinning core functionality of *customer-defined* applications – that is to say, an AI service provides classifications, analyses, detections, predictions, and other capabilities on which particular functionality of the customer's application is predicated and relies[25]. As the performance of the AI service's model is determined by the specifics of the provider's engineering processes, so too is the particular functionality in the customer's application that uses the model.

Second, AI systems can exhibit errors, biases, inequalities, and other problems, which, through AIaaS, could be reproduced at scale. Further, by making state-of-the-art AI capabilities widely accessible at scale, often with little provider oversight, AIaaS risks enabling a range of undesirable, problematic, or possibly illegal applications. This raises

[25] Note that AIaaS contrasts with *Software as a Service* (SaaS), whereby the service provider defines, offers, and manages the complete application on behalf of the customer (though typically provides some possibility for customisation). AIaaS to some extent resembles a form of *Platform as a Service* (PaaS), more traditional forms of which provide general infrastructure that enables some supporting function (for example, for managing deployment and operation specifics, storage and data management, sign-on services, and so on). AIaaS, however, provides generic AI capabilities that enable, facilitate, underpin, and directly determine particular application functionality.

questions around the roles, responsibilities, and potential liabilities of both AIaaS providers and their customers.

Third, AIaaS is likely to grow in prominence. In-house machine learning can be prohibitive, given the need for data, expertise, and computational power. By enabling developers to 'plug-in' state-of-the-art ML capabilities to their applications, at low cost and without requiring great expense, AIaaS increases the likelihood that ML will underpin a larger range of applications. In future, many organisations wishing to use AI may rely on AI services for their desired functionality.

Finally, and again due in part to the data, expertise, and computational power needed to develop sophisticated systems, it will likely be companies already dominant elsewhere in the digital economy who can practically offer a range of AI services. Indeed, as noted previously, AIaaS has already coalesced around Amazon, Microsoft, and Google, each of which is also market-leading in multiple other online services sectors. In other work, we have explored consolidation at this sub-application infrastructure level[26]. While this did not study AIaaS, specifically, we found consolidation in infrastructure services more generally (particularly around Amazon and Google). This echoes the consolidation of user-facing web applications around much the same companies[27] (affording them significant societal and market power[28]). Dominance in those sectors allows these companies to take leading positions as AIaaS providers, particularly where they repurpose systems developed to support their activities elsewhere and offer access commercially. As with existing cloud services, other organisations are likely to in time become dependent on AI services offered by these providers.

[26] Cobbe et al (n 12).

[27] Internet Society, 'Consolidation in the Internet Economy' (2019) Technical Report.

[28] Zeynep Tufekci, 'As the Pirates Become CEOs: The Closing of the Open Internet' (2016) 145 *Dædalus, the Journal of the American Academy of Arts & Sciences* 1, 74; Martin Moore and Damian Tambini (eds), *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018); Lina M Khan 'Sources of Tech Platform Power' (2018) 2 *Georgetown Law Technology Review* 2; Jennifer Cobbe and Jatinder Singh 'Regulating recommending: Motivations, Considerations, and Principles' (2019) 10 *European Journal of Law and Technology* 3.

Moreover, not only does AIaaS consolidation offer providers a potentially fruitful and monopolistic revenue source, but providers will also be at the heart of any societal transformation brought about by the wide and affordable availability of AI technologies. This has significant implications for the power of providers and their role in future society. The leading AIaaS providers are three of the five 'Big Tech' companies[29], and represent three of the four most valuable publicly traded companies in the world by market capitalisation[30]. In recent years, the five Big Tech companies have emerged as an oligopoly that concentrates power through their financial resources and their dominance of online services[31]. They have aggressively pursued strategies intended to dominate markets and centre themselves in online services, and their dominance of AIaaS allows them to further entrench themselves at an infrastructural level in both virtual and physical spaces.

2.3. The AIaaS processing chain

We now describe the 'chain of processing' in AIaaS. As with cloud more generally (Fig 1), the AIaaS processing chain typically involves at least two entities – those offering the service ('**providers**'), and application vendors availing of the service ('**customers**', or 'tenants' in common cloud parlance). This may also involve **third-parties**[32], typically where customers use AIaaS to either *(i)* add functionality (by providing a particular capability) to applications that are in turn used by these third-parties, or *(ii)* analyse or process activities and behaviours of third parties (as they use the customer's application or in some other form of surveillance or behavioural analysis). Third-parties in AIaaS are broadly either 'active' users of services (where third-party end-users directly interact with aspects of a customer's application that rely on AIaaS for functionality) or 'passive' subjects of data processing (where the customer collects data from or about third-parties for processing that involves AIaaS, but where those third parties are not themselves doing or directly interacting with something that relies on the AI service). Though third-parties will be discussed where

[29] Sometimes abbreviated as 'GAFAM', for Google (Generally understood in this context as synonymous with its parent holding company, Alphabet), Amazon, Facebook, Apple, and Microsoft.

[30] As of mid-2020.

[31] Nick Smyrnaios 'The GAFAM effect: Strategies and logics of the internet oligopoly' (2016) 188 *Communication & Languages* 2.

[32] Note that in this paper we do not use 'third-party' as defined in GDPR art 4(10) to mean sub-processors.

relevant, they are largely outside our analysis, as they are usually not directly commissioning or provisioning the AI service from the provider. They may, for example, use a customer's application that includes speech transcription which utilises an AI service obtained by the customer, but that third-party is not involved in commissioning the specific transcription services of a particular provider.

Customers access AI services remotely by initiating a request to the provider accompanied by the input data, which is then analysed by the provider and the results of that analysis returned to the customer (Fig 2). Models are accessed through an Application Programming Interface ('API'). APIs are commonly used in software to obtain functionality through 'calls' or *requests* (with specified input parameters) to the service, software, database, or library in question and receiving responses (tailored to the input parameters). In AIaaS, API calls are typically executed over a network between customers' applications and the provider's AIaaS servers. Requests may pass from or through the customer's equipment in this process (as customers often use other cloud services to support deployment, they may not necessarily *own* that equipment), or the customer's (application) executing on an active third-party's equipment (device or cloud) may transfer requests *directly* from the application to the provider's server and then receive responses. In all cases, the customer's application determines that interaction. Depending on the nature of the service, often this process takes milliseconds to complete.

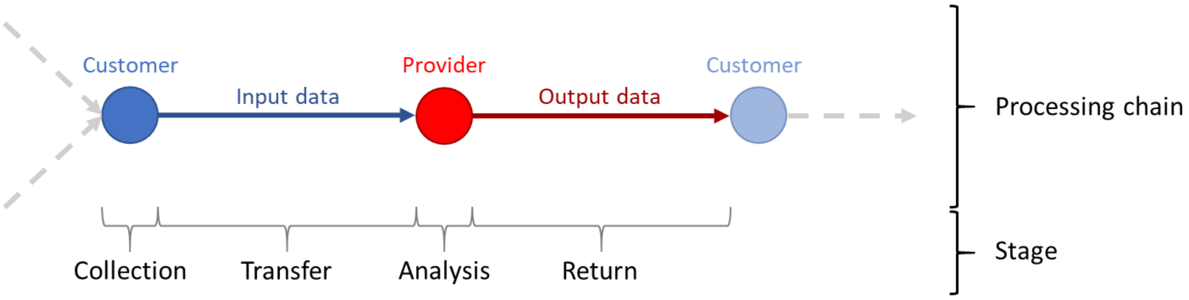

*Figure 3. Representation of the stages of the AIaaS **processing chain**. First, the customer **collects** input data from one or more sources (such as third-parties or data brokers). This stage may involve some processing – data collation, pre-processing, analysis, etc. – by the customer. The customer then **transfers** input data to the provider (request), who **analyses** that data. The provider **returns** outputs of that analysis to the customer (response). The return stage may be followed by further processing by the customer or the transmission of data onwards to others, but that activity before the collection stage and after the return stage is not part of the AIaaS chain itself.*

AIaaS therefore involves a *chain* of data flow between customers and providers (Fig 3). This **AIaaS processing chain** consists of several stages, detailed below. Our depiction is *an abstract representation of the stages of processing* rather than representing specific actions or operations performed on data; there may be several activities, organisational or technical, at each stage. We identify four stages of the AIaaS processing chain:

(1) **Collection** of input data and any processing of that data by customers. This could involve, for example, data input by third-parties to the customer's application; collecting usage or behavioural data; surveilling physical spaces using cameras, microphones, or sensors; acquisitions from data brokers, and so on. Collection does not necessarily involve storage, aggregation, or temporal delay; it could include, for instance, live sensor readings or video feeds. Again, collection does not necessarily mean that the data touches any equipment owned or managed by the customer.

(2) **Transfer** of input data by customers to providers through a networked API request. This may in practice involve transferring input data directly from a customer application's third-party end-users to the provider at the customer's instigation and direction but without the data passing through any customer managed server, or it may come from the customer themselves.

(3) **Analysis** of that data by the provider using a machine learning system, applying a model (or models). These models are trained using datasets collated by the AIaaS provider and are usually routinely and iteratively updated by the provider (to, for instance, improve accuracy, address identified problems, and so on). Again, our focus is on model(s) generally available to customers, not those tailored to specific customer concerns.

(4) **Return** of the results of analyses by providers to customers over a network as API responses. As results are generally returned to the requesting entity, it is possible for output data to be transferred directly from the provider to the third-party end-users of the customer's application for display or further processing without passing through the customer's managed equipment.

The processing chain effectively forms a loop in which data flows from customers, to providers, and back to customers. Subsequent to the return stage, and therefore after the end of the chain itself, customers may perform their own analyses or other processing of the service's outputs. Output data (or results of its subsequent processing) is used by customers applications to determine subsequent functionality; outputs may be displayed on-screen on a website or app, may trigger other application functionality including subsequent AIaaS calls, may be stored in a database, may inform device functioning, may help the customer better understand usage of their application, may be transferred onwards to another entity, and so on.

Providers may also process input data for their own purposes in a manner removed from and additional to the AIaaS processing chain itself. This may be to monitor and improve their service's performance, to update their models, or to monitor customers' use for billing purposes or to enforce the platform's terms of service. We divide this additional processing by providers broadly into two categories[33]. The first is '**ancillary**' processing necessary for and directly connected to providing a commercial AI service (for instance, for billing, security, technical maintenance, or legal and regulatory compliance). The second is '**supplementary**' processing for purposes other than those *necessary* for the commercial supply of the AI service itself. This includes things like improving models or systems[34], undertaking market research, or enforcing aspects of the provider's terms of service unconnected to the ancillary processing described above[35]. Access to customers' data for model building and development helps improve models by giving a broader range of 'example' deployments, allowing models to better account for a wider range of (changing) circumstances and use cases. Importantly, there is a key distinction here between AIaaS and other cloud services: while cloud providers use information that they gather about customers' *usage* of their other services (i.e. metadata) to inform product improvement and development, in AIaaS it is often the *customer input data itself*, obtained directly through

[33] A similar (though not identical) distinction can be found in Microsoft Azure's service agreement between "Processing for Microsoft's Legitimate Business Operations" (largely falling under 'ancillary processing') and "Processing to Provide Customer the Online Services" (including what we call 'supplementary processing') (Microsoft, 'Online Services Data Protection Addendum' (July 2020), 6 <https://www.microsoft.com/en-us/licensing/product-licensing/products> accessed 19 March 2021).

[34] Note that there are 'hybrid' services whereby a pre-built model is offered to customers which they can then customise and further refine by training the model on input data that they supply. As we focus on pre-trained models, which represent the bulk of AI services, these hybrid services are outside the scope of our discussion.

[35] Unlike monitoring for legal and regulatory compliance, enforcing other aspects of providers' terms of service is not strictly speaking necessary for providing the service itself. Providers have significant discretion to decide what they permit or prohibit and could, if they so wished and in line with their policies, allow anyone to use their services for any legal purpose or impose requirements or restrictions as a condition of using the service.

the AIaaS processing chain, that providers use for supplementary processing to improve the models that drive their core product. That is to say, supplementary processing of customer data for model improvement, a key feature of AIaaS, does not have an analogy in most other cloud services. This supplementary processing drives improvements both in the provider's models used across their customer base and, consequently, in the functionality of individual customers' applications.

Precise details about AIaaS providers' use of customer data are limited, but publicly available information suggests that all the major AIaaS providers engage in supplementary processing using customer data in some form. For example, Google asks customers to permit Google to use customers' speech recognition inputs to refine its models[36]. Amazon uses customer data from their Rekognition vision service to improve its models on an opt-out basis[37]. At present, Microsoft states explicitly that they do not use customer data from certain Azure AI services (such as vision) for supplementary processing[38], and that they *may* use customer data from other services (such as their video analysis service)[39]. It is unclear whether and to what extent Microsoft uses customer data from other AI services for supplementary processing, though documentation implies that customer data is used in this way in relation to certain services but not for others[40]. Microsoft retain provision in their service agreement *permitting* them to use customer data for 'ongoing improvement' (such as improving efficacy) of its online services, including Azure[41]. Providers may financially incentivise customers to permit access to customer data (Google, for instance, discounts

[36] Google Cloud, 'Cloud Speech-to-Text: Data logging' <https://cloud.google.com/speech-to-text/docs/data-logging> accessed 13 November 2020; see also Google Cloud, 'Cloud Speech-to-Text: Terms for opt-in for data logging' <https://cloud.google.com/speech-to-text/docs/data-logging-terms> accessed 13 November 2020. Note that Google does not use customer data to improve all its AI services – for example, customer data is not used to improve its Cloud Vision models (Google Cloud, 'Cloud Vision API: Data Usage FAQ' <https://cloud.google.com/vision/docs/data-usage?hl=en> accessed 13 November 2020).

[37] Amazon Web Services, 'Amazon Rekognition FAQs' <https://aws.amazon.com/rekognition/faqs/?nc=sn&loc=7> accessed 13 November 2020.

[38] Microsoft Azure, 'Computer Vision' <https://azure.microsoft.com/en-gb/services/cognitive-services/computer-vision/#faqs> accessed 29 March 2021.

[39] Microsoft Azure, 'Analyze videos in near real time' <https://docs.microsoft.com/en-gb/azure/cognitive-services/computer-vision/vision-api-how-to-topics/howtoanalyzevideo_vision> accessed 29 March 2021.

[40] Microsoft Azure, 'Azure Cognitive Services' <https://azure.microsoft.com/en-gb/support/legal/cognitive-services-compliance-and-privacy> accessed 29 March 2021.

[41] Microsoft, 'Online Services Data Protection Addendum' (July 2020), 6 <https://www.microsoft.com/en-us/licensing/product-licensing/products> accessed 13 November 2020; see also: Microsoft 'Data management at Microsoft' <https://www.microsoft.com/en-gb/trust-center/privacy/data-management> accessed 13 November 2020.

speech recognition services for customers who opt-in to 'data logging'[42], which permits Google's use of customer data to 'refine' their services). Though supplementary processing is beneficial to the provider (and indirectly beneficial to customers through improved models), it is essentially at the providers' discretion as it is not *necessary* to provide the service itself.

3. Legal responsibilities and liabilities

We now highlight some legal issues arising from AIaaS in relation to European data protection and intermediary liability law, focusing primarily on the roles, responsibilities, and potential liabilities of providers. In particular, we assess how providers' use of customer input data to train their models in AIaaS affects the assignment of roles in data protection law in light of recent CJEU jurisprudence, whether supplementary processing is likely to have a valid legal basis in GDPR, and whether the nature of AIaaS itself affects providers' protection from liability for illegal activity involving their services. As we repeatedly highlight, many of the potential legal pitfalls for AIaaS providers relate to their own activities (such as around supplementary processing) and the fact that, where services are offered generically on a turn-key basis, they have little knowledge of what customers are doing with their services. More fundamentally, we also question whether current legal frameworks are suitable for the complex, networked, and dynamic relationships found in AIaaS.

3.1. Data protection

GDPR provides a framework governing the processing of personal data[43], defined broadly to include any information relating to an identified or identifiable natural person. Under GDPR, any natural or legal person (from here: '*entity')* involved in processing personal data will be either a data *controller*[44] or a data *processor*[45]. Processing means any operation performed

[42] Google Cloud, 'Cloud Text-to-Speech: Pricing' <https://cloud.google.com/speech-to-text/pricing> accessed 13 November 2020.

[43] GDPR art 4(1).

[44] GDPR art 4(7).

[45] GDPR art 4(8).

on personal data (including, for example, collection, storage, transmission, and analysis)[46]. The AIaaS processing chain consists of various operations performed at each stage (see Table 1). All processing of personal data covered by GDPR[47] must be based in one of the lawful grounds specified therein[48].

Collection stage	Transfer stage	Analysis stage	Return stage

Collecting;
recording;
organisation;
structuring; storage
	Disclosure by transmission	Adaptation or alteration;
		structuring;
		organisation;
		alignment or combination;
		consultation
			Disclosure by transmission

Table 1. Some processing operations[49] performed at each stage of the AIaaS processing chain. This is neither an exhaustive list nor are all operations necessarily performed in each instance of AIaaS – for example, the 'collection' stage may not always involve storage.

Data will be *personal data* where two questions are answered affirmatively: (1) does the data relate to a natural person? If so, then (2) is that person identifiable from that data? In many cases, data processed in the AIaaS chain will clearly relate to a natural person. Sometimes the individual will clearly be identifiable – obvious examples include in voice recognition, facial recognition, or other biometric identification services; where faces, images, or voice recordings of individuals are otherwise being analysed; or where direct identifiers (such as names, email addresses, unique ID numbers, and so on) are defined inputs being processed. In other cases, the question of identifiability is less straightforward. According to GDPR, an 'identifiable' person is one who can be identified, directly or

[46] GDPR art 4(2).

[47] GDPR does not apply to some kinds of personal data processing (GDPR art 2). The processing of personal data by law enforcement agencies, for example, is regulated by the Law Enforcement Directive (Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016) OJ L 119/89).

[48] GDPR art 6, art 9.

[49] As set out in GDPR art 4(2).

indirectly[50]. According to the CJEU, to be personal data, information need not by itself allow an individual to be identified[51], nor must all information needed to identify an individual be held by one person[52]. Indeed, GDPR itself contemplates circumstances where controllers process personal data but are unable to themselves identify the data subject (for instance, if the purposes of processing do not require them to identify data subjects then they are not obliged to acquire additional identifying information for the sole purposes of complying with GDPR[53]). Just because a controller does not know who the data subject is, or cannot itself identify them, that does not mean that they are not identifiable. Taking the AIaaS example of speech transcription (voice-to-text) services; clearly the voice belongs to an individual, even if the provider does not know their identity.

The fundamental question in relation to identifiability is whether the person to whom the data relates can be distinguished from others[54], either through that data alone or in combination with other data. Determining whether this is possible, according to GDPR's recitals, means taking into account all means reasonably likely to be used by the controller or by someone else to identify that person either directly or indirectly[55]. In making such a determination, factors such as the costs and time needed for identification should be taken into account, considering the available technology and potential technological developments[56]. The CJEU has held that identification would not be reasonably likely if it is prohibited by law or is practically impossible (requiring disproportionate time, cost, and effort), such that the risk of identification is in reality insignificant[57]. Providers may in some (but not all) cases be reasonably likely to be able to distinguish individuals from others. However, customers will in many or most cases be in such a position, as they often explicitly and directly interact with third-parties. Moreover, many AI services inherently involve

[50] GDPR art 4(1).
[51] Case C-582/14 *Breyer v Bundesrepublik Deutschland* [2016] ('*Breyer*') para 41. While this case related to the Data Protection Directive, which was superseded by GDPR, the definition of 'personal data' in the Directive was the same as in GDPR.
[52] *Breyer* para 43.
[53] See, for example, GDPR art 11.
[54] See Frederik J Zuiderveen Borgesius, 'Singling out people without knowing their names - Behavioural targeting, pseudonymous data, and the new Data Protection Regulation' [2016] *Computer Law & Security Review* 32, 256-271.
[55] GDPR recital 26.
[56] GDPR recital 26.
[57] *Breyer* para 46.

personal data; again considering speech transcription, though the identity of the speaker may not be clear, the fact that a voice is unique distinguishes it from others.

Many AI services will therefore involve processing personal data, including for audience analytics, voice recognition or speech transcription, facial detection, analysis, or recognition, as well as those that process sound, images, and text and so on. Customers will usually have some idea of whether they process personal data in AIaaS or not, particularly when their application directly interacts with or monitors third parties. For providers, however, the ability to determine which data is non-personal data, which is 'ordinary' personal data, and which is special category data[58] is more limited. For some services, such as biometric identification (which inherently involves special category data[59]), it may be obvious that personal or special category data is involved. Similarly, where AI services are offered to customers on a consultancy basis, the provider may have detailed knowledge of how the customer will use the service and what kinds of data are likely to be processed. In many cases, though, particularly where services are provisioned as 'turn-key', AIaaS providers will have little to no direct knowledge of what the input data transferred from customers relates to (particularly in more generic services, such as object recognition). This situation arises from the nature of AI services themselves – as providers offer these services generically, potentially to millions of customers each with their own use cases and deployments and with few (if any) checks by the provider on what each customer will use the service for, providers will be unaware of what kind of data they will process (except, again, for services where personal or special category data is inherent, such as biometric identification).

We therefore argue that, in practice, to avoid inadvertently processing personal data unlawfully, AIaaS customers and providers should apply data protection law's standards to all processing in the AIaaS chain (whether it in fact involves personal data or not). This is particularly so given that data protection law's application is irrespective of whether processing also involves the same operations performed on non-personal data without distinguishing between the two[60]. Without safeguards, there is therefore a serious risk of

[58] GDPR art 9.
[59] GDPR art 9(1).
[60] Case C-131/12 *Google Spain v AEPD and Mario Costeja González* [2014] ('*Google Spain*') para 28.

providers inadvertently processing personal data without meeting data protection law's standards. Moreover, fines imposed on controllers and processors for infringing GDPR can take into account situations where they have acted negligently[61] (which, we argue, would include processing personal data unlawfully on the mistaken assumption that it was not personal data).

While all of GDPR's requirements will apply, several issues are particularly relevant for AIaaS. Due to the complex interactions of third-parties[62], customers, and providers, the assignment of the roles of data controller and processor in the AIaaS processing chain is not simple and may conflict with how providers themselves envision their responsibilities. Moreover, the complex, networked, and dynamic nature of AIaaS makes it difficult for providers to manage data protection responsibilities and obligations, such as around legal bases for processing. As such, we now provide a high-level analysis of data protection issues arising from certain common practices of providers to indicate the general legal situation for AIaaS as typically offered – as a model-based service provided generically to a variety of customers on a turn-key basis. As our focus is on the legal position of providers, we assess their real-world practices against GDPR and CJEU case law, rather than detailing specific use cases. However, in practice – particularly where AI services operate on a consultancy basis, or where models are built or customised solely for specific customers – we note that there may be arrangements or permutations that do not align with the below.

3.1.1. Controllers and processors

The bulk of GDPR's compliance obligations fall on controllers, though processors are also under specific obligations. As such, the obligations that providers and customers will have in relation to the AIaaS processing chain will depend on whether they are acting as a controller or as a processor at each stage. At minimum, for processing for which they are a controller,

[61] GDPR art 83.

[62] In our analysis, we do not mean 'third-party' as defined in GDPR (GDPR art 4(10): "a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data"). We use it as discussed in the 'Artificial Intelligence as a Service' section of this paper.

they must implement the data protection principles[63] of lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. They must ensure that there is a valid basis in law for any processing of personal data[64]. They must also take technical and organisational measures to ensure that their processing complies with GDPR more generally and to be able to demonstrate compliance[65], to implement data protection by design and by default[66], and to ensure a level of security for the processing appropriate to the risk it presents to the rights and freedoms of natural persons[67].

As of August 2020, AWS, Microsoft Azure, and Google Cloud each specify in their service agreements that they will act as a processor for their services, including AI services, and that customers will typically be the controller[68] (note though that Microsoft claim to be an "independent" – i.e. separate – data controller for a small number of services[69]). However, while contractual relationships can guide courts and regulators, the roles of controller and processor based on the factual position and cannot be assigned definitively in contract[70] – where an entity in practice determines the purposes and means of processing (i.e. *why* personal data is being processed and *how* it is being processed[71]), they will be a controller[72]. Processors merely process personal data for and at the direction of controllers[73]. More than one entity can be a controller for the same processing; in that situation, they will either act

[63] GDPR art 5.
[64] GDPR arts 5, 6, and 9.
[65] GDPR art 24.
[66] GDPR art 25.
[67] GDPR art 32.
[68] Amazon, 'AWS GDPR DATA PROCESSING ADDENDUM', section 1.1 <https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf> accessed 13 November 2020; Microsoft, 'Online Services Data Protection Addendum' (July 2020), 7 <https://www.microsoft.com/en-us/licensing/product-licensing/products> accessed 13 November 2020 (see also Microsoft Azure, 'Azure Cognitive Services' <https://azure.microsoft.com/en-gb/support/legal/cognitive-services-compliance-and-privacy> accessed 13 November 2020); Google Cloud, 'Data Processing and Security Terms (Customers)', section 5.1 <https://cloud.google.com/terms/data-processing-terms> accessed 13 November 2020.
[69] Microsoft Azure, 'Azure Cognitive Services' <https://azure.microsoft.com/en-gb/support/legal/cognitive-services-compliance-and-privacy> 29 March 2021.
[70] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (2010) 00264/10/EN WP169, 10-11.
[71] Article 29 WP (n 72), 14.
[72] GDPR art 4(7), art 28(10).
[73] GDPR art 4(8), art 28.

separately as controllers, or, where they jointly determine the purposes and means, will act together as *joint* controllers. In either case, all controllers are subject to GDPR.

The leading CJEU cases on assigning controllership (separately or jointly)[74] are *Google Spain*[75], *Wirtschaftsakademie*[76], *Jehovah's Witnesses*[77], and *FashionID*[78]. Several key points distil from these cases:

1) The concept of 'controller' should be understood broadly, to ensure complete and effective protection for data subjects[79].
2) An entity will take part in determining the purposes and means of processing – and will therefore be a controller – where they 'exert influence' over the processing for their own purposes[80], such as to help achieve their goals[81] or for their own commercial benefit or economic interests[82] (though exercising *control* over the personal data in question is not required[83]). This can include, *inter alia*, defining parameters, according to the objectives of that entity, that have an influence on the processing in question[84]; contributing to determining the purposes of another controller's processing[85]; and making processing by other controllers possible[86].
3) Where multiple entities are involved, having *access* to personal data is not a prerequisite for any one of those entities being a controller for the processing[87].
4) Joint controllership does not exempt any one controller from compliance obligations[88], nor does using another controller's platform for the processing mean that a controller can escape those obligations[89].

[74] While these cases related to the Data Protection Directive, which was superseded by GDPR, the definition of 'data controller' in the Directive is the same as in GDPR. As such, they can be read across to GDPR.
[75] *Google Spain*.
[76] Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] ('*Wirtschaftsakademie*').
[77] Case C-25/17 *Tietosuojavaltuutettu v. Jehovan Todistajat* [2018] ('*Jehovah's Witnesses*').
[78] Case C-40/17 *FashionID GmbH & Co. KG v Verbraucherzentrale NRW e.V.* [2019] ('*FashionID*').
[79] *Google Spain* para 34.
[80] *Jehovah's Witnesses* para 68; *FashionID* para 68.
[81] *Jehovah's Witnesses* para 71.
[82] *FashionID* para 80.
[83] *Google Spain* para 34.
[84] *Wirtschaftsakademie* paras 36-39.
[85] *Wirtschaftsakademie* para 31
[86] *FashionID* paras 75, 78.
[87] *Wirtschaftsakademie* para 38; *Jehovah's Witnesses* para 69; *FashionID* para 82.
[88] *Google Spain* para 40.
[89] *Wirtschaftsakademie* para 40.

5) Joint controllership does not, however, necessarily imply joint *responsibility* for *all* stages of processing[90]. Processing may involve several operations performed on personal data at different stages[91]. Different actors may be involved at these different stages of processing to different degrees[92]. Those different actors may therefore be (joint) controllers for operations performed at certain stages of processing, but cannot be controllers for operations performed at stages that precede or are subsequent to stages for which they determine the purposes and means[93].

3.1.2. Assigning controllership

Straightforwardly, as with most other cloud services[94], customers will always be controllers for the entire AIaaS processing chain, as throughout they determine the purposes and means of processing (a position reflected in AWS, Microsoft Azure, and Google Cloud service agreements). For example, where customers offer to active third-parties functionality that relies on AIaaS, they essentially delegate the processing that enables, facilitates, and underpins that functionality to the provider. In that case, they not only enable the provider's processing of third parties' data, but also determine the processing's means (analysis by that AIaaS provider) and purposes (realising the functionality offered by the customer to third-parties). Where customers input data obtained from passive third-parties to an audience analytics service (for example), they similarly determine the processing's means (analysis by that AIaaS provider) and purposes (providing insight into third-parties' behaviour). In both cases, customers are clearly controllers for that processing. This remains the case however the data is transferred to the provider, including where input data does not pass through the customer's (owned or managed) equipment as it is transferred between third-parties and providers – for example, where it is transmitted directly from their application's end-users (i.e. third-parties) to a provider's AI service. In that scenario, while they do not process the data on hardware or infrastructure that they own, manage, or

[90] *Jehovah's Witnesses* para 66; *Wirtschaftsakademie* para 43; *FashionID* paras 70-74.
[91] *FashionID* para 72.
[92] *Jehovah's Witnesses* para 66; *Wirtschaftsakademie* para 43; *FashionID* para 70.
[93] *FashionID* paras 70-74.
[94] Millard (n 7).

direct, customers still determine the purposes and means of processing in the AIaaS chain. Their application determines how the data is processed in line with their operational decisions and business practices, making and receiving responses from the API calls necessary for the AIaaS processing chain to run.

Due to the differences between providers' activities in AIaaS and other cloud services, in particular around supplementary processing, determining their role is more complicated. Whether providers determine the *purposes* of processing will, following the CJEU jurisprudence discussed above, depend on whether they influence or undertake any processing for their own purposes other than directly connected to providing the AIaaS service itself[95]. In our view, if an AIaaS provider is merely analysing input data and returning outputs to customers and engaging in ancillary processing necessary for providing the service – for instance, for billing, security, or legal and regulatory compliance – then it will act as a processor[96] (see Fig 4). In that case, the customer determines the purposes.

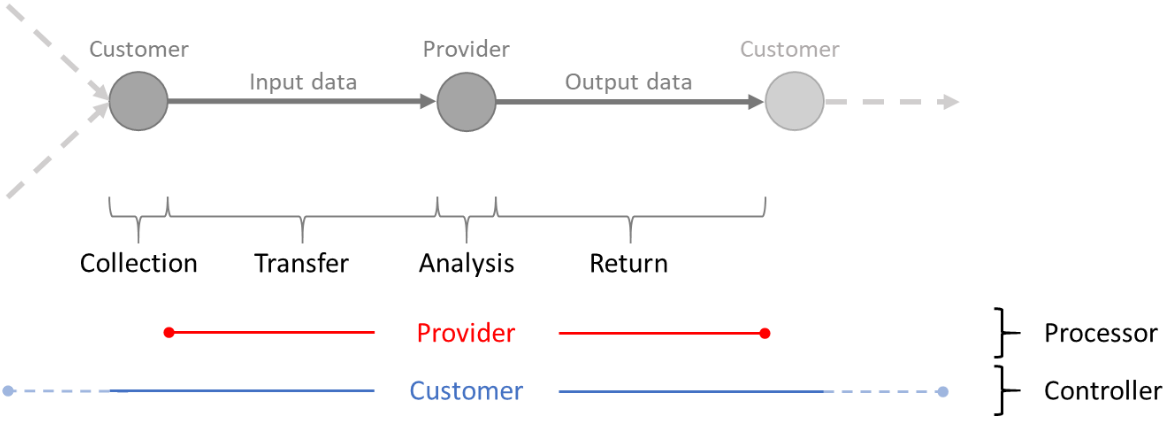

Figure 4. Role assignments in the AIaaS chain where providers do not *influence the processing of input or output data for their own purposes. Here, customers are controllers for* ***all stages*** *and likely also for any subsequent processing that they perform. AIaaS providers act as processors for their customers in the* ***transfer***, ***analysis***, *and* ***return*** *stages.*

[95] See *Jehovah's Witnesses* paras 65-68; *Wirtschaftsakademie* para 31; *FashionID* paras 68-69.

[96] Microsoft's service agreement says that they will 'comply with *the obligations of* an independent data controller under GDPR' [emphasis added] in relation to some ancillary processing, though notably – unlike in some other areas of their service agreement – they do not claim to actually *be* a controller for that processing (Microsoft, 'Online Services Data Protection Addendum' (July 2020) p.7 <https://www.microsoft.com/en-us/licensing/product-licensing/products> accessed 13 November 2020).

If, however, the provider also does anything else with the customer input or output data for their own purposes (for instance, improving or updating their models or systems[97]) then their position would be different. Though we acknowledge that publicly available information on the precise details of providers' supplementary processing is limited (see §2.3), the key legal question for us hinges on whether providers process personal data for their own purposes other than as *necessary* for providing the requested service to the customer. Supplementary processing is not part of the AIaaS processing chain itself. It forms a separate processing chain, a separate set of operations performed by the provider, with separate purposes determined by the provider. Providers would, in that case, influence the purposes for processing operations in the AIaaS chain for their own commercial benefit[98] at the transfer and (where model outputs are used for supplementary processing) analysis stages, as those purpose would then include *facilitating* that supplementary processing. However, providers would not influence the collection stage, as the customer undertakes processing at that stage prior to the provider's involvement[99]. Nor would they influence the return stage, as output data is transmitted to the customer at a point in the chain logically separate from and subsequent to the provider's supplementary processing (though chronologically that processing may occur on copies of the output data after the return stage is complete).

In relation to the *means* of processing, the situation is again complicated. 'Means' doesn't just relate to narrow technical details of hardware or software (what the European Data Protection Board ('EDPB') calls the 'non-essential means'), but to broader questions of which data will be processed, in what ways, for how long, and so on (the 'essential means', closely linked with the purpose)[100]. Where providers engage in supplementary processing, we argue, they play a role in determining the means of processing for the transfer and

[97] Note that this remains the case even where customer data is aggregated or where metadata (i.e. data about customer data) is used to improve services, as aggregation of data or derivation of metadata would itself involve operations performed on the personal data provided by the customer and would thus constitute processing.

[98] See, by analogy, *FashionID* para 80, where the fact that the processing served FashionID's own commercial advantage was a key consideration in finding that it was a controller.

[99] See *Jehovah's Witnesses* para 66, *Wirtschaftsakademie* para 43, and *FashionID* paras 70-74, where the Court reasoned that different entities can have a different degree of influence over different stages of processing.

[100] European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (2020), 13-15; Article 29 WP (n 70), 14.

analysis stages of the AIaaS chain. This is because processing at those stages effectively then supports two purposes: first, providing the AI service to the customer; second, facilitating the provider's supplementary processing. In effect, though the AIaaS chain and any supplementary processing are separate, operations performed in the transfer and analysis stages of the AIaaS chain facilitate that supplementary processing and thus fulfil that second purpose, determined by the provider. They therefore form the means by which that purpose is achieved. Providers therefore determine not just why processing at those stages occurs (in part, to facilitate their own supplementary processing) but how that purpose is pursued, which data will be processed, in what ways it will be, and so on (through their API, their systems, and their models). Indeed, as the CJEU held in *Jehovah's Witnesses*, "a natural or legal person who exerts influence over the processing of personal data, for his own purposes […] participates, as a result, in the determination of the purposes *and means* of that processing"[101] (emphasis added). The effect, according to the CJEU, is that the entity in question – in this context, the provider – acts as a controller[102].

Where they engage in supplementary processing, AIaaS providers would therefore, we argue, be controllers for processing in the transfer and analysis stages of the chain[103]. However, following the Court holding in *FashionID* that entities cannot be controllers for operations in the chain of processing that precede or are subsequent to those for which they determine the purposes or means*[104]*, they are not controllers for processing after the analysis stage, as transmitting output data to and its subsequent use by customers does not serve the purpose of facilitating providers' supplementary processing. Instead, they are processors for this return stage. They do not play either role for any processing at or prior to the collection stage[105]. That providers who engage in supplementary processing are controllers for certain stages of the AIaaS processing chain is a potentially significant

[101] *Jehovah's Witnesses* para 68; *FashionID* para 68.
[102] *Jehovah's Witnesses* para 68; *Fashion* ID para 68.
[103] See, by analogy, *Jehovah's Witnesses* paras 68-69 and *FashionID* paras 70-74. The 'transfer' stage involves processing consisting of the operation of disclosure by transmission; the analysis stage involving processing consisting of the set of operations of use, consultation, and adaptation.
[104] FashionID paras 70-74: "natural or legal person cannot be considered to be a controller […] in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means".
[105] The 'collection' stage involving processing consisting of the set of operations of collection, recording, organisation, and structuring.

departure from the legal position found in traditional cloud services, which typically do not involve such supplementary processing, and arises directly from those supplementary processing activities of providers themselves. As discussed previously, the main AIaaS providers (AWS, Microsoft Azure, and Google Cloud) all engage in this supplementary processing for various AI services. In many cases, therefore, according to current real-world practice, the legal assignment of responsibilities in AIaaS stands contrary to claims in providers' service agreements that they are processors.

3.1.3. The relationship between controllers

Where customers and providers are both controllers for various stages of the AIaaS processing chain (that is to say, where providers engage in supplementary processing of customer data), the next question is whether they are joint controllers or separate controllers for the same processing. According to GDPR, multiple controllers will be joint controllers where they jointly determine the purposes and means of processing[106] – i.e. pursuing the same purposes using the same means. However, as the Article 29 Working Party acknowledged, many kind of 'pluralistic control' may arise in reality[107]. In complex, networked, multiparty environments – such as AIaaS – two controllers for the same processing may each pursue their own purposes which may or may not align to a greater or lesser degree. According to both the Working Party[108] and the EDPB[109], 'jointly' should mean "together with" or "not alone", depending on the arrangements between controllers. Following from the CJEU's jurisprudence in *Wirtschaftsakademie*, *Jehovah's Witnesses*, and *FashionID*, the EDPB says that joint controllership can arise where controllers make a 'common decision' about purposes and means (i.e. where they decide together[110]) or from 'converging decisions' about the same purposes and means[111] (for instance, where the processing is mutually beneficial, such as where it serves both parties' commercial or

[106] GDPR art 26(1).
[107] Article 29 WP (n 70), 18.
[108] Article 29 WP (n 70), 18.
[109] European Data Protection Board (n 100), 17.
[110] See, for example, *Jehovah's Witnesses* paras 70-71.
[111] European Data Protection Board (n 100), 18.

economic interest[112]). In the latter case, a key consideration is whether the processing would not be possible without both parties' participation[113]. Similarly, the European Data Protection Supervisor ('EDPS') suggests that where controllers do not converge on "the same general objective", they will potentially act as separate controllers[114] (the corollary being that where they *do* converge on such a same general objective, they are likely to be joint controllers).

As noted previously, the three main AIaaS providers' service agreements each specify that customer data may be used for supplementary processing (in some cases, this may be on an opt-in or out-out basis; in others, it may be covered by non-negotiable terms). Before using an AI service, customers necessarily agree to the terms of the relevant service agreements. Unless customers have opted-out of supplementary processing (or chosen not to opt-in, where that is possible), they may have agreed that the provider can their input data for that processing. If so, they will have agreed (implicitly or explicitly) to use the AI service on the basis of serving the additional purpose of facilitating the provider's supplementary processing. In that case, where supplementary processing takes place, the purposes of the customer's and provider's processing will converge: providing the AI service to the customer *and* facilitating the provider's supplementary processing. Though they have not made a common decision (that is to say, they have not decided on a *shared* purpose), their converging decisions – that the processing chain should serve two purposes to benefit each of them – mean that they will have jointly determined the processing's purposes and means[115]. Providers and customers would therefore in those circumstances be joint controllers for the transfer and (potentially[116]) analysis stages of the AIaaS processing chain.

[112] See, for example, *FashionID* para 80; *Wirtschaftsakademie* paras 34-39; European Data Protection Board (n 100), 19.

[113] European Data Protection Board (n 100), 18.

[114] European Data Protection Supervisor 'EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725' (2019), 24; see also Article 29 WP (n 70), 17-22.

[115] See, by analogy, *FashionID* para 80-81, where Fashion ID's (implicit) acceptance of Facebook's terms for embedding a social plugin to benefit FashionID on Fashion ID's website – including that personal data would be generated by the plugin and would be transmitted to Facebook for processing for Facebook's own purposes – was taken to mean that they jointly determined the purposes of processing. See also, by analogy, *Wirtschaftsakademie* paras 34-39, where Wirtschaftsakademie's implicit acceptance that administering a fan page for their own benefit would also permit Facebook to process data for its own purposes was taken to mean that they similarly jointly determined the purposes of processing.

[116] Depending on whether the supplementary processing involves the results or some other aspects of the analysis stage of the AIaaS chain.

If, however, providers use customer data for supplementary processing even after the customer has opted-out or not opted-in (where that choice has been offered), the provider will be a separate controller for those stages. Questions of that processing's lawfulness aside, the customer's purposes would then not converge with the provider's, and they would not therefore jointly determine the purposes and means.

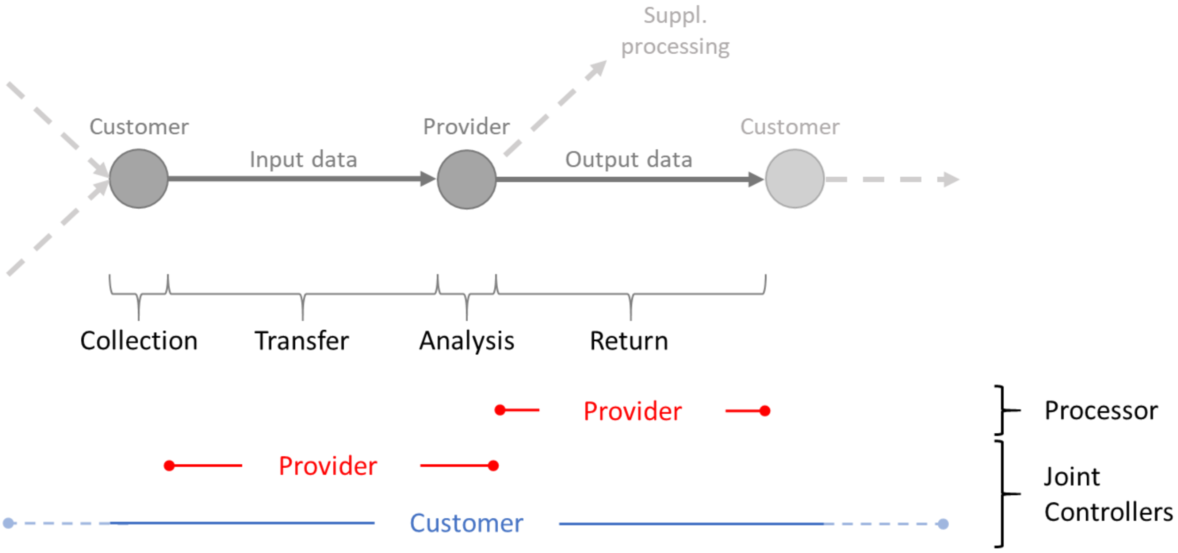

Figure 5. Role assignment in the AIaaS chain where providers do *influence the processing of customer data for their own purposes (i.e. to facilitate supplementary processing, here using input data and model outputs). Customers are controllers for the **transfer** and **analysis** stages, and are also controllers (either solely or jointly with others) for the **collection** stage and likely also for any subsequent processing that they perform. Providers are joint controllers with customers for the **transfer** and **analysis** stages and processors for the **return** stage.*

Whether providers engaging in supplementary processing are joint controllers with customers matters, as joint controllers share responsibility for various aspects of processing and must enter into formal arrangements to divide those responsibilities, including around fulfilling data subject rights[117]. They must make the 'essence' of this arrangement available to data subjects[118]. Yet, at the time of writing, none of the service agreements of Amazon, Microsoft, or Google provide for such a situation. Instead, as previously discussed, they each envisage themselves as processors for their (controller) customers (or, in the case of Microsoft, for a minority of services, as an "independent" – i.e. separate – controller). However, even following *FashionID*, it remains unclear exactly what the consequences are

[117] GDPR art 26.
[118] GDPR art 26(2).

for joint controllers who do not properly arrange their relationship[119]. GDPR itself does not specify any particular enforcement powers relating to joint controllership, though the corrective powers afforded to supervisory authorities – including warnings, orders to comply, and bans on processing[120] and significant fines[121] – would be available.

3.1.4. Controllership for supplementary processing

While our analysis indicates that providers who engage in supplementary processing are joint controllers with customers for the transfer and analysis stages of the AIaaS processing chain, we argue that providers are sole controllers for the supplementary processing itself. Again, it is important to distinguish here between (a) processing of customer data undertaken as part of the AIaaS chain (i.e. to provide the AI service to the customer and to *facilitate* supplementary processing) and (b) processing of customer data undertaken separately by the provider *as part of* their supplementary processing. The latter set of operations will often involve data logically separate from (and often chronologically after) the AIaaS processing chain. As such, supplementary processing forms its own separate processing chain, serving only the provider's purposes (of course, in a more abstract sense customers may also benefit from general improvements to the providers' service). Though engaging in this supplementary processing makes the provider a joint controller for the transfer and analysis stages of the AIaaS chain, the customer cannot be a controller for the separate supplementary processing chain as they influence neither its purposes nor its means[122]. As such, only the provider can be a data controller for that supplementary processing.

[119] René Mahieu, Joris van Hoboken, and Hadi Asghari, 'Responsibility for Data Protection in a Networked World: On the Queston of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe' (2019) 10 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 1.

[120] GDPR art 58.

[121] GDPR art 86(4).

[122] See, by analogy, *Fashion ID* paras 76 and 85, where the Court found that it would be impossible for Fashion ID to determine purposes and means for Facebook's subsequent and separate processing undertaken for Facebook's own purposes.

3.1.5. Legal bases for processing

Controllers must have a valid legal basis for processing personal data[123]. As controllers for the entire AIaaS chain, customers will require a legal basis for processing throughout. In cases where providers are controllers for the transfer and analysis stages (i.e. where they engage in supplementary processing), they will also require a legal basis for processing in those stages, as well as for their supplementary processing. GDPR sets out several possible legal bases[124]. For 'ordinary' personal data, six bases for processing are available. Those likely to be relevant for commercial AIaaS include where the data subject has given their *consent* to processing for specific purposes[125]; where processing is *necessary for the performance of a contract* to which the data subject is party[126]; and where processing is *necessary for the purposes of the legitimate interests of the controller* (unless those interests are overridden by the interests or fundamental rights and freedoms of data subjects)[127]. Processing special category data is prohibited unless one of ten specified exemptions to that prohibition applies. Generally only two are likely to be available for AIaaS – where the data subject has given e*xplicit consent* to processing for specified purposes[128], and where processing is *necessary for reasons of substantial public interest* and is done on the basis of an EU or domestic law that meets certain requirements[129]. We discuss first these potential legal bases for processing in the AIaaS chain, and then for providers' supplementary processing.

We focus here on special category data for two reasons. First, the available bases for processing special category data are more restrictive and potentially more difficult to fulfil. Second, the difficulties in distinguishing non-personal, 'ordinary' personal, and special category data, and the additional requirements for special category data and potentially

[123] GDPR arts 5, 6, and 9.
[124] GDPR arts 5, 6, and 9.
[125] GDPR art 6(1)(a).
[126] GDPR art 6(1)(b).
[127] GDPR art 6(1)(f).
[128] GDPR art 9(2)(a).
[129] GDPR art 9(2)(g); the requirements are that the law is proportionate to the aim pursued, respects the essence of the right to data protection, and provides for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

serious penalties arising from unlawful processing[130], mean the safest approach for providers may be to treat all input data as special category data. Though this is potentially quite burdensome for providers, the need for this precautionary approach arises directly from the nature of turn-key AI services and the practices of providers themselves – as we argue above, their supplementary processing positions them as controllers for certain stages of the AIaaS chain. They do not, however, require their own legal basis for processing (and therefore do not need to take such a precautionary approach) where they do not engage in supplementary processing. In that case, following our preceding analysis, they are processors acting under the instruction of their controller customers. Providers should therefore balance any benefits they realise through supplementary processing against the legal risks they may incur as a result.

Where special category data is in fact processed in the AIaaS chain, customers and providers as controllers will usually need to have the explicit consent of data subjects for the purposes for which the AIaaS processing chain is executing[131]. This is because the restrictive nature of the 'substantial public interest' exemption means that it will generally be inapplicable to AIaaS. For that exemption to apply, the processing must be *necessary* (there must be no alternative or more privacy-preserving means of achieving the same outcome[132]), and it must be based on an appropriate EU or domestic law. In the UK, for instance, this law is the Data Protection Act 2018, which sets out 22 conditions in which 'substantial public interest' might apply[133]. These conditions are narrow and generally require controllers to meet certain criteria (and many, such as 'administration of justice and parliamentary purposes'[134], 'political parties'[135], and 'elected representatives responding to requests'[136], are unlikely to be relevant). Thirteen of those conditions require controllers to justify not obtaining explicit

[130] GDPR art 58, art 83.

[131] This is not to say that explicit consent is the only ground on which providers can rely for any of their processing; for 'ordinary' personal data, they may be able to use consent, contract, and legitimate interests. We do, though, argue that, due to the difficulties in distinguishing special category data, this would involve considerable risk for providers.

[132] European Data Protection Supervisor, 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' (2017) <hhttps://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf> accessed 13 November 2020.

[133] Data Protection Act 2018 ('DPA 2018'), sch 1, pt 2.

[134] DPA 2018, sch 1, pt 2, para 7.

[135] DPA 2018, sch 1, pt 2, para 22.

[136] DPA 2018, sch 1, pt 2, para 23.

consent, and 11 require controllers to demonstrate the substantial public interest[137]. The Information Commissioner's Office (the UK's supervisory authority) emphases that processing must be in the *public* interest – not simply a private or commercial interest – and that controllers "should be able to make specific arguments about the concrete wider benefits of [their] processing"[138]. The 'substantial public interest' exemption will therefore not apply to most commercial use of AIaaS. Explicit consent thus appears to be the only exemption available in most circumstances.

This raises the question of when and by whom explicit consent should be obtained from data subjects. In *FashionID*, the CJEU held that it was a joint controller's duty to obtain consent from data subjects for the set of processing operations for which it is actually a controller, but not for prior or subsequent operations[139]. In that case, the operations for which FashionID was a joint controller took place at the beginning of the processing chain. The Court determined that consent must therefore be obtained by FashionID prior to performing those operations[140]. According to the Court, because it was the data subject visiting FashionID's website that triggered the rest of the processing chain, it was incumbent upon FashionID itself – rather than on controllers involved later in the chain – to obtain consent so as to ensure timely protection of the data subject's personal data[141]. The analogous stage of the AIaaS processing chain is the collection stage, for which the customer is the sole controller. As such, it would be incumbent on the customer to obtain explicit

[137] See table at Information Commissioner's Office, 'Guide to the General Data Protection Regulation: What are the substantial public interest conditions?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-substantial-public-interest-conditions> accessed 13 November 2020

[138] Information Commissioner's Office, 'Guide to the General Data Protection Regulation: What are the substantial public interest conditions?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-substantial-public-interest-conditions> accessed 13 November 2020; Some private companies that wish to deploy live facial recognition systems have argued that they can rely on the 'substantial public interest' ground for preventing and detecting crime. We find this argument unconvincing. While preventing or detecting crime may be in the public interest, the deployment of facial recognition does not, in our view, meet the necessity test (unless we are to believe that there has until now been an epidemic of crime that only augmenting the already extensive use of CCTV with facial recognition systems deployed by a private company can possibly prevent). Nor do we agree that deploying facial recognition systems in a shopping centre, for example, is in the substantial interest of the public, rather than principally in the interests of the private owner of the shopping centre and their commercial tenants.

[139] *FashionID* paras 100-102.

[140] *FashionID* para 102.

[141] *FashionID* para 102.

consent from the data subject for processing special category data. As the customer is also a controller for the entirety of the AIaaS processing chain, they should obtain explicit consent from data subjects for all processing operations in that chain[142]. GDPR says that where different purposes are pursued by the same processing – such as where the AIaaS processing chain serves the additional purpose of facilitating supplementary processing – consent should be given for each of those purposes[143]. The customer would in that case need to obtain *separate explicit consent* from data subjects for the processing in the AIaaS chain for each of the purposes of providing the service to customers *and* of facilitating providers' supplementary processing.

This presents some complications for AIaaS. Aside from whether any explicit consent meets GDPR's high standards[144], actually obtaining explicit consent from data subjects may not be straightforward. Customers will likely be able to seek that consent where data subjects are active third-parties (i.e. where data subjects use aspects of a customer's application which rely on AIaaS for functionality). They will also likely be in such a position where they directly interact with passive third-parties in some way (where, for instance, data subjects use aspects of a customer's application which *do not* rely on AIaaS for functionality and the customer is using AIaaS to analyse their behaviour). But it is not clear how customers could obtain explicit consent where they do not directly interact with passive third parties (where customers are, for instance, directly or indirectly surveilling a physical space). Providers who are joint controllers for the transfer and analysis stages of the AIaaS chain – having little to no interaction with third-parties – may choose to rely on the express assurances of customers that explicit consent has been obtained from data subjects for their processing. They would, though, risk processing special category data unlawfully where the customer has in fact failed to obtain valid explicit consent. Providers may be able to mitigate this risk somewhat by requiring some form of evidence from the customer that the data subject has actually explicitly consented. However, though Google Cloud does require customers to

[142] This situation would be significantly complicated where active third-parties are also controllers for the AIaaS processing. Precisely when and by whom explicit consent should be obtained (where necessary) is likely in that case to depend largely on the specific circumstances; as such, we do not explore this scenario here.
[143] GDPR recital 32; European Data Protection Board 'Guidelines 05/2020 on consent under Regulation 2016/679' (version 1.1 2020), 12.
[144] GDPR art 4(11), art 7, recital 32; Article 29 Data Protection Working Party, 'Guidelines on consent under Regulation 2016/679' (2018) 17/EN WP259 rev.01, 18; see also European Data Protection Board (n 143), 21.

obtain and maintain any consents necessary to permit processing[145], none of the service agreements of the three main providers require that any consents obtained by customers be *evidenced* – or indeed any assurances relating to legal bases for processing (perhaps because providers consider themselves processors, not controllers).

For providers' supplementary processing[146], things are yet more difficult. As discussed, due to the nature of AI services, providers will likely have less of an idea than their customers whether they are processing special category data (except where implicit, such as for biometric services). If they are, they may in theory (depending on the circumstances and subject to the qualifications relating to this ground for processing discussed previously) rely on the substantial public interest exemption for monitoring for criminal use of their AI service, or (perhaps) for reducing bias in their models[147], but not for other forms of supplementary processing[148]. However, the generic, turn-key nature of most AI services and the need to avoid unlawful processing again presents a challenge. As providers will in many cases not know whether the customer data they retain for supplementary processing originates with end-users of customers' applications, and will similarly have no reliable way of determining whether it is special category data (if indeed it is personal data at all), we argue that providers should in practice rely on the *explicit* consent basis for that processing.

However, as we note previously, customers' obligation to obtain explicit consent extends only to processing for which they are actually a controller[149] – i.e. to processing in the AIaaS chain itself – and so would not cover the provider's supplementary processing. Providers would therefore need to have customers obtain evidenced, valid explicit consent on their behalf from the data subjects for each purpose pursued by their supplementary processing, *and* make that evidence available to the provider so that consent can be demonstrated by the provider if necessary. However, as providers do not provide customers with detailed

[145] Google Cloud, 'Terms of Service' section 3.2 <https://cloud.google.com/terms> accessed 13 November 2020.

[146] Bearing in mind that if they are not engaging in that processing then they will be data processors and the question of them obtaining explicit consent for any of their processing becomes moot.

[147] The UK's Data Protection Act 2018, for instance, includes 'equality of opportunity or treatment' as a condition for the substantial public interest exemption (DPA 2018, sch 1, pt 2, para 8).

[148] Although if only 'ordinary' personal data is being processed, then providers may for some purposes be able to rely on the ground relating to the legitimate interests of the data controller (GDPR art 6(1)(f)).

[149] *FashionID* paras 100-102.

information about their supplementary processing, customers are not positioned to obtain fully informed, specific consent from data subjects, as GDPR requires[150]. Moreover, for consent to be freely given – another GDPR requirement[151] – data subjects must have the real option of refusing consent to the provider's supplementary processing without suffering any detriment or loss of service[152]. Yet, in many cases, providers do not give customers the opportunity to opt in or out of supplementary processing, let alone to do so on each service request (as would be necessary to account for the wishes of each data subject).

Further, though the main AIaaS providers all engage in some supplementary processing, and though they may ask *customers* for permission to use their input data to improve models (through an opt-in or opt-out), it is not clear that those providers have implemented the necessary measures to obtain the valid explicit consent of *data subjects*. Again, AWS, Microsoft Azure, and Google Cloud service agreements contain no provisions relating to evidencing consent. While this is not necessarily a problem for 'ordinary' personal data (where non-consent grounds may be available[153]), we therefore suggest that supplementary processing that actually *does* involve special category data is in many cases currently being done unlawfully. Indeed, though not all data will be special category data, much supplementary processing will involve special category data in some way. As a result, as sole controllers for their supplementary processing, AIaaS providers are potentially engaged in widespread, systematic, and sustained violations of GDPR – in particular, of the first data protection principle[154], of the prohibition on processing special category data without a valid legal basis[155], and, potentially, of the obligations to inform data subjects about their processing and data subjects' rights relating to it[156]. They have, as a result, left themselves

[150] GDPR art 4(11), art 7, recital 32.
[151] GDPR art 4(11), art 7, recital 32.
[152] GDPR art 7(4), recitals 42-43; though refusal of explicit consent to the processing necessary to provide the core functionality of the AI service (i.e. operations performed in the AIaaS processing chain for the purpose of providing the service) could quite reasonably result in withdrawing the service from the data subject.
[153] Potentially legitimate interests and contract, depending on the circumstances (GDPR art 6). Note, though, that AIaaS providers would still need to provide information to data subjects about their supplementary processing and data subjects' rights relating to it, including, where the provider's legitimate interests are relied on, inform data subjects of their right to object to that processing (GDPR art 14).
[154] GDPR art 5(1)(a).
[155] GDPR art 9.
[156] GDPR art 14.

open to enforcement action by supervisory authorities (including, but not limited to, warnings, fines of up to 4% of global revenue[157], or, significantly for a major cloud provider, bans on processing[158]), not to mention judicial remedies[159] and claims in tort for compensation for any material or non-material damage resulting from the processing[160].

3.2. Intermediary liability

AI services are often offered 'turn-key', with few checks by providers as to the identity or intentions of customers or the actual purposes to which they are put in practice. There is therefore potential for misuse to support illegal activity. This could involve a wide range of possible activity – for example, financial crime, fraud, harassment, intellectual property infringements, or liability arising in tort for harm caused by use of services. While customers are likely directly liable for illegal use of AI services, there is also the question of whether providers may face some liability for enabling, facilitating, underpinning – or, indeed, undertaking – that illegality.

The EU's E-Commerce Directive offers providers of *information society services* ("any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services"[161]) some protection from liability for illegal user activity. Under the Directive, protection is potentially available to service providers for any of three activities: *(i)* acting as a 'mere conduit' (transmitting information between individuals at their direction – for example, ISPs and messaging services)[162], *(ii)* 'caching' (in this context, a technical activity associated with acting as a conduit)[163], and, on a more qualified basis, *(iii)* 'hosting'[164] (storing information provided by recipients of the service). Whether AIaaS

[157] GDPR art 83(5).
[158] GDPR art 58.
[159] GDPR art 78.
[160] GDPR art 79.
[161] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations [1998] OJ L 204/37 ('Technical Standards and Regulations Directive') art 1 (as amended by Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations [1998] OJ L 217/18); see also E-Commerce Directive recital 18.
[162] E-Commerce Directive art 12.
[163] E-Commerce Directive art 13.
[164] E-Commerce Directive art 14.

providers are eligible for protection will depend on (a) whether AIaaS is an information society service, and, if so, (b) whether providers' activity falls into one of these three categories. If they are eligible for protection, whether they actually have that protection will depend on meeting any specified conditions.

As with other cloud services, AIaaS is an information society service. AIaaS is normally provided for remuneration (providers typically bill customers for their usage). It is provided at a distance by electronic means (over a network, typically the internet). It is provided at the individual request of recipients (defined in the Directive to include any natural or legal person who uses an information society service[165]; either customers or active third-parties). AIaaS is thus a service normally provided by remuneration, at a distance, by electronic means, at the individual request of recipients. AIaaS providers are therefore 'service providers' within the scope of the Directive[166].

AIaaS providers do not act as mere conduits. To do so, they would need to transmit information provided by recipients (customers or third-parties) to others without selecting or modifying the transmitted information[167]. As AIaaS providers analyse input data using their models and then return novel outputs to recipients, they do not simply transmit that data without modifying it. Nor, consequently, are they caching in connection with acting as a conduit. They are therefore not eligible for protections available for acting as a mere conduit or for caching.

More traditional cloud services are often covered by the hosting protection[168]. To qualify, storing information provided by recipients is a necessary but not sufficient aspect of the service provider's activity. In storing that information, the service provider must, according to the CJEU, act neutrally in relation to the information, and their activity must be passive and merely technical[169]. AIaaS providers are not therefore engaged in hosting as defined;

[165] E-Commerce Directive art 2(d).
[166] E-Commerce Directive art 2(b): "any natural or legal person providing an information society service".
[167] E-Commerce Directive art 12.
[168] Jasper P Sluijs, Pierre Larouche, and Wolf Sauter (2012) 'Cloud Computing in the EU Policy Sphere' (2012) 3 *Journal of Intellectual Property, Information Technology and e-Commerce Law* 1.
[169] Case C-324/09 *L'Oréal SA and Others v eBay International AG and Others* [2011] ('*L'Oreal v eBay*') para 113; Cases C-236/08 *Google France SARL and Google Inc. v Louis Vuitton*, C-237/08 *Google France SARL v Viaticum*

they do not store information provided by recipients as part of providing the AI service in any meaningful sense (though some data may be stored as part of the provider's supplementary processing, this is not part of the service itself). Nor is their activity 'passive' or 'merely technical' – they actively analyse customer input data using their own complex algorithmic systems to probabilistically generate new information which they then return to customers; in doing so they often also directly benefit both financially and, where supplementary processing is involved, by improving the models that they offer. We therefore argue that AIaaS providers have no available protection from liability for illegal activity carried out using their AI services.

However, even if this is incorrect and AIaaS providers do somehow act as hosts, we argue that they still operate beyond the Directive's protections. The CJEU has held that, to avail of protection, service providers must act as an *intermediary* service provider[170]. The Directive's recitals state that liability protection is limited to activities that are of a "mere technical, automatic and passive nature, which implies … neither knowledge of nor control over the information which is transmitted or stored"[171]. According to the CJEU, this means that service providers are not *intermediary* service providers – and therefore not eligible for protection – where they (a) take an active role in relation to information that would (b) give them either *knowledge* of or *control* over that information[172] (note that 'control' here does not relate to being a controller in data protection law). It is not our position that AIaaS providers have actual knowledge of input data transmitted to them by customers. However, providers use systems they have designed, developed, and deployed to undertake the analysis of customer data, inputted in line with the provider's specifications, to produce new information (in line with the system building and model training undertaken by the providers' engineers), and to return that new information generated by the providers to customers as part of the commercial service offered by those providers. Providers do thus exercise control over that data.

SA and Luteciel SARL, and C-238/08 *Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others* [2010] ('*Google France and Google*') para 114.

[170] E-Commerce Directive s 4; *Google France and Google* para 112.

[171] E-Commerce Directive recital 42.

[172] E-Commerce Directive recital 42; *Google France and Google* para 114; *L'Oreal v eBay* para 113.

AIaaS providers are therefore not protected from liability for illegal activity of customers using their AI services, whether they are considered to somehow 'host' information or not. AIaaS as a distinct activity developed after the E-Commerce Directive's adoption in 2000 and thus sits outside its liability shields. This is not to say that providers are *necessarily* liable for customers' illegality, but the fact that AIaaS providers analyse customer inputs and then return novel outputs to customers means that it is information produced by those providers on which the illegal activity is based and depends. As AIaaS enables, facilitates, and underpins application functionality, providers' analyses and outputs are integral rather than incidental to that activity. Without the Directive's protection, providers are thus in a position of significant uncertainty as to whether, when, and to what extent they could be liable for illegal activity by customers using their services.

3.3. Challenges for existing law

The issues identified above are potentially problematic for AIaaS providers and customers alike. But they also highlight that these legal concepts and arrangements originated before today's more complex, networked, and dynamic processing architectures and relationships emerged. The political economy of data processing also differs, with new information economy business models, increasingly dominant platforms, and heavily asymmetric power dynamics. This calls into question whether existing frameworks can adequately address these newer developments.

With the Data Protection Directive, the concepts of controller and processor entered EU law at a time when processing was understood in a more 'linear' way[173]. In principle, one entity would control the processing architecture[174] and may delegate some or all aspects to another, who would be essentially subordinate. In GDPR, this dominant-subordinate understanding of the controller-processor relationship remained essentially unchanged: controllers determine how and why processing takes place and are largely responsible for compliance; processors act under their instruction and on their behalf[175]. However, as

[173] Omer Tene, 'Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws' (2013) 74 *Ohio State Law Journal* 1217.

[174] Mahieu et al (n 119).

[175] Although GDPR did assign more compliance obligations to processors than in the Data Protection Directive.

others have noted[176], the increasingly complex, networked, and dynamic nature of contemporary processing environments challenges this understanding of roles and responsibilities and thus data protection law's ability to effectively protect data subjects. In its cases on controllership, the CJEU has attempted to shape data protection to these newer realities[177]. Leaving it to the Court to develop the law as disputes come before it, however, has inevitably resulted in a piecemeal response. The effect has been failure to comprehensively account for how the law can adapt.

Following our controllership analysis, in some circumstances there could be three potential controllers for some of the AIaaS chain – the provider, the customer, and a third-party. This could arise where customers provide services to other entities who are themselves controllers (for example, where the customer offers an application to a third-party that is itself processing data for its own commercial activities). What roles and relationships they take – three separate controllers; three joint controllers; two joint controllers and one separate controller; two separate sets of two joint controllers; a processor and two separate controllers; a processor and two joint controllers; or two processors and a sole controller – is heavily circumstantial. Neatly dividing responsibilities may be impracticable. This arrangement could conceivably be even more complicated, since, in contemporary environments, third-parties' applications may themselves connect with those of yet others[178]. This illustrates the challenges of assigning responsibilities under current law in these complex, networked, dynamic environments. Where many third-party controllers transiently engage with the customer's application, and thus also with the provider's service, it is not clear how roles and responsibilities could reliably be assigned to ensure a high level of protection. Nor is it clear how data subjects could understand these data processing relationships or effectively exercise their rights against each controller, or how supervisory authorities could obtain meaningful insight into these processing activities to

[176] Seda Gürses and Joris van Hoboken, 'Privacy after the Agile Turn' in Jules Polonetsky, Omer Tene, and Evan Selinger (eds) *Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2017); Mahieu et al (n 119); Lilian Edwards, Michèle Finck, Michael Veale, Nicolo Zingales, 'Data subjects as data controllers: a Fashion(able) concept?' [2019] *Internet Policy Review*; Christopher Millard, Christopher Kuner, Fred H Cate, Orla Lynskey, Nora Ni Loideain, and Dan Jerker B Svantesson 'At this rate, everyone will be a [joint] controller of personal data!' (2019) 9 *International Data Privacy Law* 4.

[177] *Jehovah's Witnesses*, *Wirtschaftsakademie*, *FashionID.*

[178] See, for example, Jatinder Singh, Christopher Millard, Chris Reed, Jennifer Cobbe, and Jon Crowcroft, 'Accountability in the IoT: Systems, Law, and Ways Forward' (2018) 51 *IEEE Computer* 7.

oversee them. While key concepts and principles of data protection law developed at a time when data processing involved relatively *stable* relationships between data subjects, controllers, and processors (for instance, the then-emerging automated processing of employee records), they do not easily translate to the relatively *unstable* nature of many contemporary networked arrangements.

Moreover, the dominant-subordinate understanding of controller-processor relationships, still depicted in GDPR, does not reflect the actual power dynamics in many contemporary environments. Though customers are sometimes afforded some choice, turn-key AI services are offered generically as determined by the provider's standard form contracts[179]. These contracts may affect the legal position of customers regarding joint controllership and other responsibilities, yet customers can usually do little if anything to influence them[180]. Large companies with technical expertise and market power will of course use AI services, perhaps on a consultancy basis involving close cooperation with the provider, though still typically through the provider's specified contractual arrangements (effectively positioning providers to influence activities of large firms in many other sectors). But it is also likely that many customers will be small organisations with little technical knowledge or expertise, much less the power that larger companies may possess. In that event, are we really to believe that, as the law would have it, the customer is the dominant party in that relationship, with control over the data processing architecture, and Amazon, Google, or Microsoft are merely its subordinate? In reality, there may be sizable technical, financial, informational, and power asymmetries between the two, and providers will exercise significant influence over how and in what ways data is processed in AI services and for what kinds of purposes they can be used.

GDPR is silent on what level of influence over processing actually constitutes determining its means, and the CJEU is yet to consider that question in any depth. As we indicated previously, the Article 29 Working Party has indicated that some aspects (such as relating to specifics of hardware and software) can be delegated to processors, whereas 'essential elements' relating to questions of the 'core of lawfulness of processing' – what is processed,

[179] Millard (n 7), chs 3 and 4.
[180] Millard (n 7).

for how long, and so on – are 'inherently reserved' to controllers[181]. The European Data Protection Supervisor[182] and the European Data Protection Board both take the same view[183]. Yet, in AIaaS, providers – merely processors under a traditional understanding, unless they undertake supplementary processing – greatly influence the analysis of input data and thus the service's outputs through development of their models (design, training, testing, and so on)[184]. Moreover, the model-driven nature of AI services means that how they operate, and thus how they drive customers' application functionality, is inherently probabilistic and depends on the ML processes undertaken by the provider in building the service. This is unlike more traditional cloud services, which typically support application deployment rather than underpinning particular functionality, and where the specifics of what a service supports are (or can be) better defined. As such, providers' engineering of their models plays a key role in realising customers' application functionality. At the same time, customers are largely prevented from understanding how this engineering occurs or how it might impact their functionality; given the statistical nature of ML models, the complexity of AI systems and engineering processes, intellectual property restrictions, and providers' general lack of transparency regarding the specifics underpinning their services.

There is also the question of who actually determines the purposes of processing in environments such as AIaaS. Consolidation around three providers means that each can influence the shape of the AI services market as a whole, and thus the range of purposes for which AIaaS may be used. Smaller providers do exist, but the fact that the major AIaaS providers are also the dominant cloud providers means that customers may be 'locked in' to a provider's ecosystem. In other cases, the customer's choice of provider may depend on which provider permits their intended purpose, with the effect that providers' policy decisions can in turn influence the means of processing (some providers, for example,

[181] Article 29 WP (n 70), 14-15.

[182] European Data Protection Supervisor (n 100), 9.

[183] European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (2020), 13-15

[184] The UK's Information Commissioner's Office, for instance, suggests that where providers decide questions relating to model design and development they may be considered to be data controllers (Information Commissioner's Office, 'Guide to Data Protection: What are the accountability and governance implications of AI?' <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/what-are-the-accountability-and-governance-implications-of-ai/#howshouldweunderstand> accessed 13 November 2020.

choose not to offer facial recognition services[185]). Additionally, barriers to entry for new AI technologies – technical expertise, large quantities of data, and significant financial resources – and the fact that AIaaS providers typically make available *the* state-of-the-art at low cost, will likely mean that AIaaS may be the only way that many companies can realistically integrate AI capabilities into their applications and workflows[186]. In effect, three dominant companies would make decisions that influence how and why many other companies in many other sectors wishing to use 'AI' could do so. None of these factors may on their own mean that providers definitively determine the purposes of any particular processing, but they do together provide something akin to a *terroir*[187] for processing. That is to say, these factors, determined by providers, together influence the general environment in which AIaaS operates and the bounds of what purposes are possible, with potentially consequential effects on customers' applications. The law's traditionally narrower understanding of what it means to influence the purposes and means of processing cannot contend with these more structural aspects, which, given the political economy of contemporary data processing, are inevitably bound up in power dynamics and other factors beyond customers' control.

Data protection may be able to confront these challenges. As AIaaS enables, facilitates, and directly underpins customers' application functionality (rather than just supporting deployment), a reasonable position for the law to take may be that, where AI services are offered turn-key[188], providers always take part in determining the purposes and means of processing in the AIaaS chain, and are therefore always controllers, regardless of any supplementary processing. This would result from providers (i) developing the model and

[185] BBC News, 'IBM abandons 'biased' facial recognition tech' (9 June 2020) <https://www.bbc.co.uk/news/technology-52978191> accessed 13 November 2020; Abner Li 'Google Cloud won't sell facial recognition tech yet, 'working through' policy questions' (13 December 2018) <https://9to5google.com/2018/12/13/google-not-selling-face-recognition/> accessed 13 November 2020.

[186] Seyyed Ahmad Javadi, Richard Cloete, Jennifer Cobbe, Michelle Seng Ah Lee and Jatinder Singh, 'Monitoring Misuse for Accountable 'Artificial Intelligence as a Service' (2020) *Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics, and Society (AIES '20), ACM, New York, NY, USA, 2020* <https://dl.acm.org/doi/10.1145/3375627.3375873> accessed 13 November 2020; Seyyed Ahmad Javadi, Chris Norval, Richard Cloete, and Jatinder Singh, 'Monitoring AI Services for Misuse' (2021) *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society (AIES '21), ACM, Virtual Event, USA, 2021*.

[187] https://dictionary.cambridge.org/dictionary/english/terroir.

[188] Services offered on a consultancy basis typically allow customers much greater latitude in defining their relationship with the provider and the service offered.

supporting systems and thus determining its (probabilistic) analyses and outputs and the purposes for which it is intended, (ii) deciding which services to offer to customers (particularly where customers are 'locked in' to the provider's cloud platform), and (iii) putting restrictions on use beyond prohibiting illegal activity. Perhaps, though, trying to squeeze complex, networked, dynamic processing chains and relationships like those in AIaaS into comparatively simplistic data protection frameworks with neatly delineated and assigned roles and responsibilities does not work at all. Data protection law attempts to apply the same understanding of roles and responsibilities across all data processing arrangements, from simple ones with a single controller and no processors through to complex, networked, multi-party scenarios. But this idealised understanding of data processing relationships largely ignores the transient, dynamic nature of many contemporary arrangements as well as their power asymmetries and the role of providers in society's technical infrastructure. As a result, data protection law increasingly does not bear close connection with reality. To confront these developments, we should perhaps consider whether specific data processing frameworks – a *lex specialis* – would be more appropriate for certain sectors or for certain activities.

Legal reform would also provide an opportunity to address the gap in liability protection identified above. Some protection for providers is plainly desirable, lest it become essentially impossible to offer AI services without significant legal risk. But providers' role in enabling, facilitating, and underpinning customer's application functionality arguably calls for greater consideration of whether the kinds of protection afforded by the E-Commerce Directive would be suitable for AIaaS. As with data protection law, that Directive originated at a time when service providers largely took a more passive role than in AIaaS. Perhaps, given AIaaS providers' more active involvement in application functionality, they should face some liability where they have not proactively taken steps to mitigate against the possibility of illegal activity. These steps could involve, for instance, ending the practice of offering AI services turn-key and instead operating an expanded customer onboarding process, with 'know your customer'-esque background checks, customer consulting and application vetting, requiring specifications of envisaged use in line with well-defined and context-specific terms of service provisions, and then verifying compliance and adherence to service agreements on an ongoing basis[189]. It would of course be impossible to prevent all illegality, and unreasonable to expect providers to do so, but if – as seems likely – AIaaS will be how many people and organisations use AI technologies in future, offering some protection to providers in exchange for taking mitigating steps such as these could help reduce its potential for illegal use by customers.

4. Considerations for legal reform

While the starting point for legal reform is to address the problems with data protection law and the gap in liability protection for providers, discussed above, legislators, regulators, and policymakers should also consider issues arising from AIaaS and the activities, responsibilities, and role of providers beyond data protection and intermediary liability. The emergence of AIaaS as an internet-enabled commercially supplied 'smart' infrastructure service, positioning providers at the core of new functionality in both physical and virtual spaces across society, is relevant to wider policy discussions around internet and platform law and regulation as well as the regulation of AI. As we now discuss, AIaaS potentially both exacerbates various problems with AI and brings new ones, in a way that is underappreciated and requires attention from legislators, regulators, and policymakers alike.

In discussing issues around AI, it is important to understand that these technologies are not simply impartial or passive tools[190], nor is offering them commercially as a service a neutral

[189] Javadi et al (n 186); these would be similar to some of the checks undertaken in, for instance, the banking and financial services industry

[190] Engin Bozdag, 'Bias in algorithmic filtering and personalisation' [2013] *Ethics in Information Technology* 15, 209-227 <https://link.springer.com/article/10.1007/s10676-013-9321-6> accessed 13 November 2020; Tarleton Gillespie, 'The Relevance of Algorithms' In Tarleton Gillespie, Pablo J Boczkowski, and Kirsten A Foot (eds), *Media Technologies: Essays on Communication, Materiality, and Society* (MIT Press 2014); Robin Hill, 'What An Algorithm Is' (2016) 29 *Philosophy and Technology* 35 <https://link.springer.com/article/10.1007/s13347-014-0184-5> accessed 13 November 2020; David Beer, 'The Social Power of Algorithms' (2017) 20 *Information, Communication & Society* 1 <http://eprints.whiterose.ac.uk/104026/1/Algorithms_editorial_final.pdf> accessed 13 November 2020; Natascha Just and Michael Latzer, 'Governance by algorithms: reality construction by algorithmic selection on the Internet' (2017) 39 *Media, Culture & Society* 2, 238-258 <https://journals.sagepub.com/doi/abs/10.1177/0163443716643157?journalCode=mcsa> accessed 13 November 2020.

act. They are contextual and contingent in nature, embedded within and a product of the wider socio-technical context of their development, deployment, and use[191]. Computer code establishes boundaries, norms, and capabilities, acting as architecture that permits or constrains behaviour[192], empowering some and potentially disempowering others. Systems' design encodes the goals, priorities, and normative assumptions of their designers and engineers, managers, and organisations. Through deployment and use they translate those goals, priorities, and normative assumptions into reality, producing societal effects and downstream consequences[193]. The normative nature of AI systems and their potentially profound and long-lasting impact on society when embedded into physical and virtual infrastructure requires careful attention.

That technologies such as AI produce societal effects confers significant power on those who control them. As AI services enable, facilitate, and underpin functionality in customer applications, AIaaS providers can engage in private ordering with potential 'regulatory' effects[194] on the behaviour of people and organisations using their services (either as customers or as third-parties). For the most part, providers determine the responses (if any) to the issues discussed below; they decide who gets access to what kind of services, on what terms, and for which purposes. As AIaaS plays an increasingly important societal infrastructural role, the lack of independent, public, accountable regulation and oversight will only become more problematic. Yet, facial recognition aside, many regulatory and policy discussions have largely ignored the market, infrastructural, and societal effects of AIaaS. The EU's proposed Artificial Intelligence Act[195], for instance, covers AI services[196] (among other things). This seeks to prohibit several activities (including law enforcement facial recognition and social scoring by public authorities)[197], while also addressing other particularly "high risk" activities through specific requirements intended to reduce that

[191] Rob Kitchin, 'Thinking critically about and researching algorithms' (2017) 20 *Information, Communication & Society* 1.

[192] Lawrence Lessig, *Code, and Other Laws of Cyberspace* (1999)

[193] Kitchin (n 198).

[194] Sylvie Delacroix, 'Beware of 'Algorithmic Regulation'' (2019) *SSRN* <https://ssrn.com/abstract=3327191> accessed 13 November 2020.

[195] Proposal for a Regulation of the European Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts ('Proposed Artificial Intelligence Act').

[196] Proposed Artificial Intelligence Act arts 1-2.

[197] Proposed Artificial Intelligence Act art 5.

risk[198]. Yet the Act as proposed is largely silent on the market and infrastructural effects of a future where companies and organisations of all kinds primarily use AI on a services basis, with most underlying computing handled by a few dominant providers. In the absence of effective regulation of AIaaS, these companies will set exercise ever-growing power over the technical infrastructure that supports digital society.

We now discuss four issues arising from AIaaS in particular: (i) the amplification of general ethical problems with AI through the scale that can be reached with AIaaS; (ii) the data on which AIaaS models are trained; (iii) the potential growth in AI-augmented surveillance facilitated by AIaaS; and (iv) the potential for misuse and abuse of AI services. This is not a comprehensive overview of all potential concerns around AIaaS; rather, in accordance with the rest of this paper, we focus on some general issues relating to the activities, roles, and power of providers in AIaaS that are worthy of greater attention from legislators, regulators, and policymakers. We recognise, though, that AI services operate transnationally, challenging governance, regulation, and enforcement mechanisms.

Note that the processing chains and socio-technical processes around AIaaS are typically opaque, with providers making little information available. We do not, however, make specific arguments for transparency of providers’ systems and processes. Though such transparency may be useful (we note that the proposed AI Act includes relevant transparency requirements[199] and that transparency is the direction of travel of legal and regulatory frameworks), transparency will not itself address the problems arising from AIaaS[200]. Greater transparency of supplementary processing, for instance, might offer more information about providers' use of input data. But it would not address the legal problems arising from supplementary processing we identify above: providers not properly arranging their legal relationship with customers as joint controllers, for example, or lacking mechanisms to obtain data subjects’ consent to supplementary processing of special category data. Similarly, increased transparency in providers’ processes would not address

[198] Proposed Artificial Intelligence Act Title III.

[199] Proposed Artificial Intelligence Act arts 11-14, Title IV.

[200] For a fuller exploration of the limitations of the transparency and accountability framing, see Frank Pasquale, ‘The Second Wave of Algorithmic Accountability’ (2019) *Law and Political Economy Project* <https://lpeproject.org/blog/the-second-wave-of-algorithmic-accountability> accessed 2 June 2021.

the imbalances of power that produce the mismatch between the dominant-subordinate model envisaged by data protection law and the reality of provider-customer relationships. Our focus here is instead on the need for interventions that address the problems we identify below, rather than on making the processes and systems that contribute to these problems more transparent.

4.1. Ethical concerns and AIaaS

Ethical concerns regarding AI have been much discussed in recent years. However, much of this discussion has implicitly assumed that companies and organisations will generally develop AI in-house. Less discussed is that AI services – available cheaply at low marginal cost; with few checks on the customer's identity, background, or intentions; requiring little technical expertise; and easily integrated into other cloud services – will allow customers' AI-augmented applications to realise functionality at a scale that may otherwise be impossible. As a result, AIaaS potentially amplifies widely discussed problems relating to AI.

For instance, the potential for biases against different population groups has been widely identified[201]. Bias is a significant problem in ML and can develop in various ways – for example, training data could reflect structural societal marginalisation of people with particular characteristics (such as race, gender, disability, sexual orientation, and so on), or the biases and prejudices of system designers can be encoded in a model's representations and outputs[202]. Without mitigating steps, the model will inherit those biases and reproduce them in its operation. This could produce unlawfully discriminatory effects, potentially opening customers up to serious legal consequences.

The consolidation in the AIaaS market, the scale at which those providers operate, and the scale that can be reached by customers' applications potentially amplifies these problems. That each provider's AI services are offered to many customers who are themselves

[201] For an overview of academic work on bias and fairness in ML, see Sahil Verma and Julia Rubin, 'Fairness definitions explained' [2018] *FairWare '18: Proceedings of the International Workshop on Software Fairness.*

[202] Harini Suresh and John V Guttag, 'A Framework for Understanding Unintended Consequences of Machine Learning' [2019] arXiv preprint, arXiv:1901.10002 <https://arxiv.org/abs/1901.10002> accessed 29 March 2021.

engaged in a wide range of pursuits means that if systems are biased then – without corrective intervention – those issues are likely to propagate across many different applications operating in many different areas, with potentially wide-ranging (and possibly discriminatory) effects. For example, some systems failed to recognise Black women[203]; such biases in a provider's system would apply across their customer base and, from there, across customers' applications. While there is on-going work on dealing with ML biases, challenges will remain for AIaaS. A key problem with AIaaS is that many issues will manifest only in particular contexts (i.e. depending on the particulars of the customer's application and its environment of use), the scope for which providers – in offering generic and widely-applicable models, typically without knowledge of customers' specific deployments – are unlikely to have considered. This is known as the 'portability trap', where a model used in one context can cause harm when deployed in another[204]. Moreover, there are a range of ML fairness and bias measures and mitigations, some of which can conflict; providers will select and implement these according to their own concerns, priorities, and interests. The nature of their choices, omissions, and the values they embed could manifest differently in different application contexts. Again, due to the nature of AI services, providers are unlikely or unable to consider the range of potential consequences of their decisions in advance.

Various sets of principles for ethical AI have been proposed attempting to address these kinds of issues[205]. While these may usefully augment baseline legal and regulatory standards[206], they cannot replace legal and regulatory intervention. A fundamental problem is that ethics principles and other non-legal frameworks for AI are voluntary, leaving 'enforcement' to market forces. Though it may benefit providers commercially to be *seen* to address these issues to some extent to avoid negative publicity, commercial pressures alone are likely not sufficient to ensure that AIaaS providers take adequate steps to minimise the

[203] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' [2018] *Proceedings of Machine Learning Research,* 81.

[204] Andrew D Selbst, Danah Boyd, Sorelle Friedler, Suresh Venkatasubramanian, and Janet Vertesi, 'Fairness and Abstraction in Sociotechnical Systems' [2019] 2019 ACM Conference on Fairness, Accountability, and Transparency (FAT* 19) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3265913> accessed 29 March 2021.

[205] For a review of some proposed sets of AI ethics principles, see Thilo Hagedorff, 'The Ethics of AI Ethics: An Evaluation of Guidelines' [2020] *Minds & Machines* 30, 99-120.

[206] Elettra Bietti, 'From Ethics Washing to Ethics Bashing: A View on Tech Ethics from Within Moral Philosophy' [2020] *FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*.

risk of problems developing across their customer base. Though Google's decision to not offer facial recognition services, for example, is welcome, and we encourage other providers to do the same[207], fundamentally we argue that it shouldn't be up to these private companies to decide on critical public issues like this in the first place. In the absence of enforceable legal and regulatory frameworks to address the policy issues arising from AIaaS, providers are themselves empowered to essentially operate as their own regulators, generally promoting market considerations and commercial priorities above others. Providers' decisions take effect at scale, across their customer base, potentially affecting many applications and their users in a wide range of areas. However, the fact that AIaaS operates at scale as an infrastructure service does offer potential points of legal and regulatory intervention. Given AI services will likely be widely used in future, then regulating at this infrastructural level could potentially be an effective way to address some of the potential problems with the growing use of AI.

4.2. Model training data

Two key categories of policy problems relating to AI services arise from the data used in training their models: (1) issues arising from training data obtained from customers, and (2) issues arising from training data obtained elsewhere. We discuss the considerations these raise in turn.

4.2.1. Training data from customers

As we discuss above, providers' supplementary processing can include using customer data to improve the AI service's model. Often, this customer data will actually be *third-party data* – i.e. obtained from third-parties (such as application end-users or subjects of surveillance)

[207] IBM has already ceased offering facial recognition services (BBC News (n 165)). Amazon and Microsoft have chosen not to offer facial recognition to law enforcement in the US (Isobel Asher Hamilton, 'Outrage over police brutality has finally convinced Amazon, Microsoft, and IBM to rule out selling facial recognition tech to law enforcement. Here's what's going on' *Business Insider* (13 June 2020 <https://www.businessinsider.com/amazon-microsoft-ibm-halt-selling-facial-recognition-to-police-2020-6> accessed 13 November 2020).

and inputted to AIaaS by customers. Providers' use of this data to train models presents several concerns.

First, there are privacy concerns about providers using third-parties' data to train their models without the knowledge of those third-parties. AIaaS typically operates 'behind the scenes' of applications, giving end-users little information on the data flows and processing chains that underpin functionality. Third-parties may therefore not know that the application they are interfacing with itself relies on AI services provided by a separate organisation, let alone that their data may be used to train the underlying models. This is particularly concerning given that, in some cases, providers' employees or contractors may access customer data for labelling or to assess whether the model is functioning correctly. Amazon's Rekognition service, for instance, allows Amazon's "trusted employees"[208] to access facial and image recognition data supplied by customers. Where this customer data is actually *third-party* data, this represents a potentially serious privacy violation. Moreover, following our previous analysis (see §3.1.5), it is unclear how providers can lawfully use this data for supplementary processing given the potential to process special category data without first obtaining data subjects' explicit consent.

Second, there is a risk that, through 'model inversion attacks'[209], it may sometimes be possible to analyse a system's inputs and outputs to extract information about the model's training data (with varying degrees of accuracy). In some cases, this extracted information may contain personal data[210], and could therefore potentially reveal details about individuals. While this is a problem for machine learning models in various contexts, the potential privacy harms caused by such attacks in this context are exacerbated where third-party data supplied by multiple customers (which may as a result represent many data subjects) is present in the training data.

[208] Amazon Web Services (n 37).

[209] Michael Veale, Reuben Binns, and Lilian Edwards (2018) 'Algorithms that remember: model inversion attacks and data protection law' (2018) 376 *Philosophical Transactions of the Royal Society A* 2133.

[210] Veale et al (n 210).

Finally, access to customers' data and information about their real-world use of models gives providers an advantage over others in developing more sophisticated systems. More data allows for bigger and more representative training datasets. More use cases and information about customer deployments allows providers to assess their systems' operation in practice, potentially facilitating better testing and refinement of models. Supplementary processing thus both helps reduce the resources that providers need to devote to systems research and development, *and* allows them to integrate research and development into a process for which they are paid by customers. AIaaS providers can therefore (in theory) develop better, more accurate, and more generalisable systems at lower net cost than may otherwise be incurred. Moreover, consolidation of AI services around Amazon, Google, and Microsoft gives three already-dominant companies an advantage given they have access to large quantities of customer data and deployments. They can leverage that advantage to develop and improve models for use both in their AI services and in their activities in other sectors. This may fuel expansion in AI services as providers pursue evermore data and deployments for developing increasingly sophisticated systems. This could also contribute to further platform expansion and monopolisation, as those companies leverage their technical superiority over established actors in other sectors to expand their activities into other areas of economy. Beyond the direct benefits of improving their systems, this helps build institutional knowledge and capacity that can also be beneficial for these companies.

Given the questionable legality of processing special category data, the more general privacy concerns around the use of third-party data, and the contribution to platform power and monopolisation, prohibiting AIaaS providers from using customer data to train or improve models or systems should be seriously considered. Although this may drive AIaaS providers to obtain more training data from other sources, we note that currently they hardly refrain from doing so (as we discuss next), and that other regulatory mechanisms exist or could be brought into existence to address this issue (for example, GDPR's restrictions on repurposing[211], which, if properly enforced, could help).

[211] GDPR art 5.

4.2.2. *Training data from elsewhere*

As well as customer data, AIaaS providers typically rely on extensive data and technical supply chains that underpin their services by providing aggregated, cleaned, and labelled training data. Some sources of this data are uncontroversial. Some are questionable but mostly harmless – a commonly encountered example is Google's reCAPTCHA, whereby users verify that they are human by identifying everyday objects in images. In doing so, users label training data for Google's image recognition algorithms[212]; in effect, Google leverages their dominance of captcha systems to get end-users to do valuable work for free which then feeds into developing systems from which Google commercially benefits. Others, however, are considerably more problematic. Some providers of AI services have scraped websites for training data, for example[213]; Clearview – a smaller but controversial provider – scraped images of users from Facebook, Twitter, YouTube, Instagram, LinkedIn, and other major social platforms for their training datasets[214]. Clearview's facial recognition service is used by law enforcement agencies around the world and by commercial actors[215].

Cross-border AIaaS data flows also facilitate concerning supply chain practices. Firstly, providers may obtain training data from countries with lax or no data protection or privacy laws and use that data to develop systems for use in jurisdictions with those protections[216]. Secondly, providers often contract with low-paid, precarious workers in the Global South to label and clean data that feeds into the development of services used in Europe[217].

[212] James O'Malley, 'Captcha if you can: how you've been training AI for years without realising it' *TechRadar* (12 January 2018) <https://www.techradar.com/news/captcha-if-you-can-how-youve-been-training-ai-for-years-without-realising-it> accessed 13 November 2020.

[213] Rachel Connolly, 'Scraping Faces' *London Review of Books* (28 January 2020) <https://www.lrb.co.uk/blog/2020/january/scraping-faces> accessed 13 November 2020.

[214] Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It' *The New York Times* (18 January 2020) <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> accessed 13 November 2020; Kate Cox, 'Facebook, YouTube order Clearview to stop scraping them for faces to match' *ArsTechnica* (7 February 2020) <https://arstechnica.com/tech-policy/2020/02/facebook-youtube-order-clearview-to-stop-scraping-them-for-faces-to-match> accessed 13 November 2020.

[215] Ryan Mac, Caroline Haskins, and Logan McDonald, 'Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA' Buzzfeed News (27 February 2020) <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement> accessed 13 November 2020.

[216] Kristina Irion, and Josephine Williams, 'Prospective Policy Study on Artificial Intelligence and EU Trade Policy' (2019) *Amsterdam: The Institute for information Law*.

[217] Noopur Raval, 'Automating Informality: On AI and Labour in the Global South' (2019) *Global Information Society Watch*; Irion and Williams (n 217); Madhumita Murgia, 'AI's new workforce: the data-labelling industry

Outsourcing in AI supply chains is similar to outsourcing in supply chains for physical products to evade workers' rights, environmental protections, and minimum wage laws. In effect, the cross-border nature of technical supply chains potentially allows AIaaS providers to outsource key work underpinning AI services to other jurisdictions – escaping privacy, data protection, employment, and possibly other laws – and then offer those services to European customers. Any future regulatory initiatives relating to AIaaS should consider whether AI systems offered as a service in the EU should be trained on data obtained, labelled, cleaned, and processed in accordance with European data protection, employment, and other relevant laws.

4.3. Surveillance

An overarching policy issue with AIaaS is how these services can enable AI-augmented surveillance. Internet-enabled surveillance (both public and private) has for some years crept into greater areas of contemporary life. AIaaS potentially facilitates a kind of AI-augmented 'Surveillance as a Service', particularly for those who would otherwise lack the technical capabilities or resources to develop systems of their own. Exacerbating these concerns is that physical spaces are increasingly monitored with cameras, microphones, and a range of sensors, collecting data from and about people in those spaces (potentially without those people's knowledge or their awareness of how it will be used). For example, AI services could help retailers track customers through their stores and analyse their behaviour; facial recognition or other biometric services could allow public spaces to be surveilled by public or private actors and otherwise 'anonymous' individuals identified and monitored; speech and voice recognition services could similarly be used to monitor otherwise private conversations and identify individuals by voice.

Rolling out AI-augmented surveillance systems cheaply and at scale, enabled by AIaaS, could potentially transform spaces (both physical and virtual) and relationships and power dynamics between watchers and watched. AI capabilities enable those undertaking surveillance to move from passively watching people (which can itself affect their choices,

spreads globally' Financial Times (24 July 2019) <https://www.ft.com/content/56dde36c-aa40-11e9-984c-fac8325aaa04> accessed 13 November 2020.

behaviour, and agency and produce differentials of power[218]), towards potentially identifying and analysing them to more actively, dynamically, and reflexively influence their behaviour[219] or subject them to further intervention or detention. Moreover, the prevalence and intractability of biases and errors in ML systems threatens to reinforce societal divisions and hierarchies along gender, racial, and ethnic lines. We thus echo assertions that introducing AI into video surveillance and other digital information-gathering infrastructure alters power dynamics in favour of those controlling previously "dumb" systems, requiring reconsideration of how to retain an appropriate balance of societal interests and fundamental rights and potentially limiting the expansion of digital infrastructure that might otherwise seem appropriate[220].

4.4. Misuse and abuse

The scale that customers can achieve with AIaaS affords significant potential for misuse, abuse, or undesirable use of AI services that produces serious effects. Providers therefore typically specify in their service agreements that customers cannot engage in or promote illegal or unlawful activity (the main providers generally refer at least to criminal activity, fraud, infringement of intellectual property rights, and defamation)[221]. Providers typically also impose other limitations on the purposes for which their services can be used. Amazon prohibits the use of AWS for harmful content such as worms, viruses, trojan horses, and so on; offensive content such as material that is obscene, abusive, or depicts non-consensual sexual activity; security violations; and network abuse such as Denial of Service attacks[222]. Microsoft prohibits the use of its services, *inter alia*, to violate rights of others; to spam or distribute malware; or in applications that could result in death, serious bodily injury, or

[218] Through what Foucault described as the disciplinary power of panopticism (Michel Foucault, Discipline and Punish (trans Alan Sheridan, Penguin 1991)).

[219] Bringing this kind of disciplinary power away from panopticism and closer to the kind of control through 'universal modulation' as described by Deleuze (Gilles Deleuze 'Postscript on the Societies of Control' (1992) 59 *October*, 3-7).

[220] Michael Veale, 'A Critical Take on the Policy Recommendations of the EU High-Level Expert Group on Artificial Intelligence' (2019) *UCL Working Paper Series, No. 8/2019* <https://ssrn.com/abstract=3475449> accessed 13 November 2020, 5-6.

[221] Amazon Web Services, 'AWS Acceptable Use Policy' <https://aws.amazon.com/aup/> accessed 13 November 2020; Microsoft, 'Online Services Terms' <https://www.microsoft.com/en-us/licensing/product-licensing/products#OST> accessed 13 November 2020; Google Cloud, 'Google Cloud Acceptable Use Policy' <https://cloud.google.com/terms/aup> accessed 13 November 2020.

[222] Amazon Web Services (n 222).

severe physical or environmental damage[223]. Google prohibits the use of its services, *inter alia*, to infringe rights of others; to distribute viruses, worms, trojan horses, and other malicious software; or for spam[224]. While the lack of liability protection for AIaaS should incentivise providers to proactively identify and prevent illegal use of their services, the primary incentives for providers to identify legal but undesirable use appear to be commercial pressures and risks of reputational damage (which have already driven several providers to prohibit law enforcement use of their facial recognition services[225]). However, methods for identifying illegal or prohibited use of AIaaS in practice appear to be little considered.

Other work has proposed several ways that AIaaS providers could attempt to identify possible misuse or abuse of their systems[226]. As previously discussed (§3.3), one potentially fruitful policy change would be to end the practice of offering AI services turn-key, instead consulting with and vetting customers and their applications, requiring specifications of envisaged use in line with well-defined and context-specific terms of service provisions, and verifying compliance and adherence to service agreements on an ongoing basis[227]. Interventions to limit the scale at which customers can use AI services would also potentially be beneficial; it is not a given that customers should use powerful models at scale without safeguards. Some relatively straightforward mechanisms for tackling the problems of scale include rate limiting (restricting the number and frequency of each customer's API requests and potentially of the customer's end-users) or limiting the extensiveness and detail of the request or response (for example, the number of objects that can be detailed in an image). These interventions should be within providers' current capabilities – Amazon and Microsoft already employ similar methods for certain services, such as those that process faces[228].

More complex monitoring by providers of customers' service usage to identify illegal activity or terms of service violations is theoretically possible, but not always practicable. However,

[223] Microsoft, 'Online Services Terms' (n 222).
[224] Google Cloud (n 222).
[225] Hamilton (n 208).
[226] Javadi et al (n 186).
[227] Javadi et al (n 186).
[228] Javadi et al (n 186).

various methods of assessing AIaaS usage are possible[229] – potentially either identifying suspicious usage patterns (from *metadata*) or examining customers' inputs and outputs (for example, a large number of people detected in an image recognition service would indicate that the service may be used for crowd surveillance). While these methods would not conclusively allow for all illegal activity or terms of service violations to be discovered, they could assist providers in identifying cases for further investigation. However, any such monitoring *must* be balanced against the potentially serious privacy issues that this would raise. As noted previously, customer data is often actually third-party data – systematic monitoring of this data by providers for indicators of misuse or abuse could potentially reveal end-user behaviours and activities. This kind of intervention could therefore be justified only by serious, overriding public policy interests and only where necessary and proportionate.

5. Conclusions and further research

AI services will be increasingly relied upon by a wide variety of applications. Three companies – Amazon, Microsoft, and Google – are particularly dominant in the AIaaS market, although others do have smaller market shares. Crucially, AIaaS moves cloud providers beyond merely offering supporting infrastructure for applications (as in traditional cloud services) to enabling, facilitating, and underpinning customers' application functionality. This shift in the role of AIaaS providers challenges legal understandings of the roles and responsibilities of actors in these complex, networked, and dynamic environments. Moreover, the nature of many AI services themselves – offered generically to potentially millions of customers on a turn-key basis – presents several legal complications for providers, as we have highlighted.

AIaaS also raises various underdiscussed issues relevant to any future legal or regulatory frameworks for AI services. Consolidation of AI services around a few companies that are already dominant in other areas of the economy further entrenches their position and

[229] Javadi et al (n 186).

confers upon them greater power to make decisions about the digital infrastructure that increasingly underpins society. The scale that can be achieved with AIaaS potentially exacerbates problems with bias in ML systems and the broader ethical questions around AI. The use of customer data to improve systems raises concerns about the privacy of third-parties, and the cross-border data and technical supply chains on which AI services rely potentially allow providers to avoid data protection law and workers' protections. The prospect of AI services augmenting surveillance that transforms power relations and balances of rights and interests in public and private spaces requires careful attention to ensure that people are protected. Finally, there is potential for AI services, available cheaply to deploy at scale, to be misused or to be repurposed for undesirable or problematic uses.

There are potential ways forward. The gap in liability protection for AIaaS and the fact that AI services are consolidated around a few providers opens space for regulatory interventions at this infrastructural level to address potential harms arising from the inappropriate or illegal misuse of AI. Through AI services, providers are more involved in customers' application functionality and should arguably hold more responsibility in exchange for protection from liability. AIaaS may allow more general ethical issues with AI to scale more easily and become more pronounced. Given the systemic risks this could cause, providers should take greater care around how, where, and why their services are used in customer applications. Moreover, AIaaS should feature in the ongoing AI-related discussions of legislators, regulators and policymakers. While AI services are at present typically offered by the major providers on a turn-key basis, introducing more comprehensive customer onboarding processes and ongoing monitoring could mitigate against potential misuse (though these must be balanced against the potentially serious privacy problems it could raise). Regulatory interventions to address problems arising from AIaaS supply chains could potentially also help.

In all, Artificial Intelligence as a Service challenges established understandings of roles and responsibilities of cloud providers in data protection law and of their responsibility for activities of their customers. The growing use of AI services raises data protection concerns, as well as arguably more significant issues around the societal power of dominant platforms through their control of digital infrastructure services and the potential for misuse and abuse of these powerful systems. As policymakers worldwide grapple with how to deal with AI more generally, these services – which may come to be the primary means by which many organisations and applications implement AI – should be front and centre in policy discussions and regulatory proposals.