Section 2 - An ecosystem of trust – additional answers

Do you have any other concerns about AI that are not mentioned above? Please specify:

A healthy and trustworthy ecosystem for AI will include a clear and concise framework which includes strong rights, effective protection of those rights, and the capability to enforce those rights. One of the risks of using AI is its capability to manipulate in a way that is not obvious to the casual observer or until a later point in time. Academic scholarship also suggests that manipulation is neglected and underdeveloped in legal thinking.[1] However, our legal systems ensures protection for the *integrity of the person*; for example, Article 3 of the European Union Charter of Fundamental Rights and Freedoms guarantees that every citizen has the right to respect for his or her physical and *mental* integrity, while the Court of Justice of the European Union (CJEU) has stated that the right to human integrity is part of Union law.[2] However, Article 3 jurisprudence is limited and, so far, has only been interpreted in a way that ensures the State is constrained from commoditizing and interfering with the physical integrity of human beings or through the lens of privacy law to ensure the state is constrained from interfering with the moral and psychological integrity of human beings.[3] Hildebrandt, for example, has argued that privacy is 'the right to "incomputability" of the self: there is an intimate area that should not be computed/counted/commoditized'.[4] Others have referred to the importance of and respect for the right to 'decisional privacy' as justification for constraint on surveillance capitalism.[5] Yet manipulative AI is only presently regulated when it makes up part of a transaction (consumer protection), or when it affects the rights of data subjects. Yet there are many examples where AI would fall outside of the scope of current European regulators. Accordingly, we endorse the position of Professors Julia Black and Andrew Murray who have argued that in some instances it will be more appropriate to look at the effects of AI (ex-post) than to create a prohibitive (ex-ante) regulatory regime. However, some forms of AI should be deemed high-risk and should be subject to certain (ex-ante) controls with stronger ex-post enforcement rights.[6]

More specifically, adding to the concerns identified in the White Paper, we suggest looking at further concerns identified in the literature, and relying on the key values and principles of the EU and member states' law : 1. The principle of fairness more generally, not limited to anti-discrimination laws only; 2. The effects that AI can have on legal certainty in many context, particularly in judiciary and public service; 3. The effects on the rule of law principle; 4. Due process more generally, to include criminal, civil and administrative processes; 5. The effects on democratic process and the functioning of democracy (elections and manipulation).

If you wish, please indicate the AI application or use that is most concerning ("high-risk") from your perspective:

There are many potential existing and future applications and uses of AI that could be considered high risk. In our view, these are the key examples (the list is not exhaustive, as new applications will develop): public health and health care; public administration and public services, including public transport and judiciary; banking and financial sector; cybersecurity; energy and waste management; elections and democratic processes; news and the media; law enforcement, including surveillance; private surveillance; recruitment; biometric ID systems.

In addition to the existing EU legislation, in particular the data protection framework, including the General Data Protection Regulation and the Law Enforcement Directive, or, where relevant, the new possibly mandatory requirements foreseen above (see question above), do you think that the use of

---

[1] Pichierri and Leiser, "*Post-Panoptic Surveillance: State-Sponsored Manipulation*", (forthcoming, 2020).
[2] Case C-377/98 *Netherlands v European Parliament and Council* [2001] ECR-I 7079
[3] *X and Y v the Netherlands* (Application no. 8978/80, 26 March 1985); *Botta v Italy* (Application n. 21439/93, 24 February 1998); B*ensai v the United Kingdom* (Application n. 44599/98, 6 February 2001); *Estate of Kresten* (Application n. 1338/03).
[4] Hildebrandt, M. (2019). *Privacy as protection of the incomputable self: From agnostic to agonistic machine learning*. Theoretical Inquiries in Law, 20(1), 83-121.
[5] Zuboff S., *Big other: surveillance capitalism and the prospects of an information civilization*, in *Journal of Information Technology*, Vol. 30, 2015, pp. 75–89; Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. Profile Books.
[6] Black, J., & Murray, A. D. (2019). *Regulating AI and machine learning: setting the regulatory agenda. European Journal of Law and Technology*.

remote biometric identification systems (e.g. face recognition) and other technologies which may be used in public spaces need to be subject to further EU-level guidelines or regulation:

The European Union's framework for the processing of personal data is not remotely sufficient for regulating all of the various types of AI and AI-based systems operating in public spaces. Both AI and AI-based systems risk affecting society in unimaginable ways; accordingly, mitigating any unforeseen effects will be of paramount importance. The European Union should lead the way through the creation of a European-wide AI Regulator enabled with strong investigatory, enforcement powers, and the staff needed to undertake and implement both. Not all AI will be powered by personal data; in fact, there is a persuasive argument that all data (including personal) entering an AI environment ceases to relate to an identifiable living person by the nature of what is actually in the black box.[7] Furthermore, the GDPR is a risk-based and prohibitive regime. AI has already been deployed. A new AI Supervisor can work alongside, but independent of, the data and consumer protection authorities and provide regulatory oversight in areas that do not fall within their competences. For example, a framework for the proper regulation of AI could ensure AI technologies deemed high-risk only are deployed through a licensing and authorisation regime. The data protection framework is setup to regulate only actors (limited by *personal* scope) that satisfy the GDPR's *material* scope. Furthermore, the regulator could design and new rules that draw on established principles like *fairness* in the consumer protection regime and *accountability* and *transparency* from the data protection regime and would be free to assess whether the effects of the AI on the consumer or the data subject was fair and transparent (assuming these are regulatory objectives). Regardless of whether a new supervisory body for the use of AI is created, measures for incentivizing further collaboration between the data and consumer protection regulators are needed.

Moreover, another challenge for the data protection framework is determining the relevant regime when a private actor is using personal data that would be of interest to law enforcement authorities. It is neither clear nor agreed that AI technologies would fall under the remit of the Law Enforcement Directive or the GDPR. Not all parts of a biometric identification system may be processing personal data, nor processing purely for a specific law enforcement purpose. But the use of AI may have considerable, especially psychological effects on its users/targets. Unfortunately, the data protection authorities are not empowered to halt manipulative AI. The data protection regime is not overly focussed on the effects of data processing. Yet the risk of manipulation should be considered as a likely outcome of the use of AI. On some occasions, AI will be able to be brought under the umbrella of under the realm of product safety and the consumer protection regime; on others, data protection will be the relevant regulator. However, there are a wealth of possibilities for the deployment and use of AI that do not fall neatly within the regulators' scope. Thus, a supervisory body is needed to advise, investigate, protect against the harms associated with AI, and empowered with the ability to bring strong enforcement measures. Any framework must oblige member states to provide the right to collective redress or to ask a national body to raise actions on behalf of the collective interest.

Do you have any further suggestion on a voluntary labelling system?

We agree that there is a need for an EU-wide approach, to avoid fragmentation in the internal market, and its potential effects on trust in AI more generally. We suggest that, before classifying an AI system 'low-risk', there is a carefully assessment against the known and potential harms they may cause (physical, material, personhood, rights and freedoms, please see the first answer in this section). We support the option of voluntary labelling, with mandatory ex ante and ex post requirements for those companies who opt in. The 'AI Trust Seal' schemes should be assessed/vetted/approved by the designated independent AI regulator, as indicated above. There needs to be an audit and oversight mechanism by the regulator, and a mandatory requirement that the scheme includes enforcement mechanisms against the decisions made by the system.

Do you have any further suggestion on the assessment of compliance?

N/A

---

[7] Leiser and Dechesne, "*Governing machine learning models: Challenging the personal data presumption*", International Data Pricacy Law, (forthcoming, May 2020).

What is the best way to ensure all AI is trustworthy, secure, and in respect of European values?

A healthy and trustworthy ecosystem for AI will include a clear and concise framework which includes strong rights, effective protection of those rights, and the capability to enforce those rights. One way to ensure AI is readily accepted by and empowers consumers is to provide the legal basis for the incorporation of a user's ethical priorities into smart contracts. As many technological innovations using AI will be used in conjunction with an obligation, one way to mitigate the power imbalance between consumers and traders is for the law to empower consumers with the right to integrate ethical considerations into their user profiles. Rather than compiling copious amount of personal data in order to deliver targeted advertising, the user has the right to inject 'script' that limits the types of AI-powered marketing and advertising they receive to those that match the ethical preferences of the user.

Many AI technologies will not use personal data nor be directed at consumers (e.g. smart cameras that improve efficiency by adjusting to current traffic flows through machine learning). However, these efficiencies will have unseen consequences as AI-powered optimization techniques can result in adverse effects. In the above example, it is not clear which European regulator or framework would ensure the right of redress for the individual/collective body (local resident, neighbourhood committee) affected by the deployment of AI. The law already requires adequate record keeping and technological robustness, but there is certainly room for the development of AI-Impact, mandatory human rights impact, and ethical impact assessments as additional *ex-ante* deployment tools. For high risk AI, a licensing regime, prior-authorization scheme, and a 'blacklist' of unacceptable AI in all instances could be maintained.

Trust in AI will require not only include transparency, but auditing of certain varieties and uses. The regime will have to determine how to comply and reconcile existing regulatory requirements. For example, what happens when an AI dataset contains personal data subject to a deletion request with a requirement that accurate and comprehensive data sets are subject to scrutiny and audit, especially when it is not clear how the AI was using the personal data in the first place. Not only is a strong regulator needed, but the staff and support to ensure adequate enforcement is a real possibility, rather than an imaginary threat. The regime should also ensure member states provide for collective redress.