Data Privacy in Emerging Technologies at a Global Scale

Author: Alexander Matthews

Professional Skills - Spring Term 2021
Date: 24th March 2021

University of Sussex
Engineering and Informatics

Abstract

This report was written to highlight the importance of balance when regulating developing technologies and to provide some key areas where balance is particularly important. The report discusses different approaches taken by different regions, as well as some of the problems that can arise from these. Addressing some of the issues around regulations on a global level is also a key part of this report, to demonstrate scenarios from which lessons can be learnt.

Contents

1 Introduction

This report will first discuss the differences in approach between the US and the EU around Regulating emerging technologies, as well as finding the best solution which is a combination of both approaches. Regulating the fields on a global scale requires careful planning of the scope of the regulations, how they might be interpreted and the differences between cultures which are all discussed in Section 3 of this report. After considering all of these topics, the report will conclude that a balance is required in order to keep the field fair and controlled while also allowing the new technologies to develop and provide benefits to society.

2 Different Approaches

The United States of America and the European Union have taken different approaches in tackling the problems that new data dependant technologies have uncovered, that is the emerging fields of technology which require data of any type in very large quantities in order to operate as intended (such as Artificial Intelligence, Machine Learning and Big Data to name just a few). In this section, the difference between their approaches will be discussed as well as deciding which points should be drawn from the two approaches.

2.1 EU Approach

The EU [is] exploring a "hard" regulatory approach with legally enforceable rights (Wachter, Mittelstadt, and Floridi 2017), which looks to make robotics and AI accountable by making them fair, transparent and explainable. The EU introduced the GDPR (General Data Protection Regulation) to enable individuals to have more control over their personal data, and ensuring companies are held accountable if they don't adhere to the regulations. This was part of the effort to make sure the use of personal data is transparent, while still giving organisations the chance to progress and enhance their autonomous developments.

Organisations are reluctant to remove humans from the equation when it comes to high-risk areas (such as transport), which means the GDPR laws may not apply to many circumstances as the accountability cannot solely rest on the AI/robot's shoulders. This makes it difficult to determine accountability, which highlights one of the key issues that arise when taking this "hard" regulatory approach like the EU have done.

2.2 US Approach

In the US however, the governing bodies and organisations are trying to promote *ethical design, education and self-regulation [rather] than on individual*

rights (Wachter, Mittelstadt, and Floridi 2017). The US do still have some regulations to protect individual's personal data such as the FCRA (Fair Credit Reporting Act), which ensures customers are notified with reasons for adverse actions. However, this doesn't provide consumers reassurance that the organisation will receive justice if they misuse the data, which the GDPR in the EU tries to do.

The US is home to some of the largest tech companies in the world, the likes of Google, Amazon and a lot of social media sites which all use new data dependant technology. To help in encouraging the education and good ethical design, these large tech companies have their own advice and educational web-pages with principles they follow and advise *(See Appendices A and B)*. This can increase the trust within the general public of these firms and the technologies they are using to better understand the needs of their customers, so that they can offer products and services to improve their quality of life.

2.3 Conclusions drawn from the Different Approaches

To ensure the general public are not negatively impacted by these new technologies, the regulatory bodies and governments need to combine the approaches of both the EU and US. This will result in the best possible chance that all groups benefit without being adversely impacted. The education and promotion of self-regulation which the US is pushing should be encouraged; but to ensure the public can feel reassured that they are protected, there needs to be regulations which are enforceable by law while being easily understood and clear for all parties. This would potentially increase the acceptance of these new technologies, bringing more support for them and thus helping them develop and thrive.

3 Key Topics to Consider at a Global Scale

There are some fundamental problems when trying to implement global regulations and laws, such as interpretation and ensuring the correct balance is struck between restrictions on companies and the rights of the stakeholders (which is quite often the general public). Both the issues around interpretation and balance will be discussed in this section, with an example to highlight the pros and cons that should be considered to ensure a fair and appropriate conclusion can be drawn.

3.1 Scope of the Regulations

A problem the EU has run into, is the level at which they set the regulations. For example, making a regulation very low level and specific makes it much easier to enforce, as there is a clear black and white line between what is allowed and what isn't. However, this makes the creation of the regulations a

lot more complex and creates overlaps between regulations which might conflict with each other. This can be avoided by ensuring all of the regulations are high level and don't go into specifics, but this leaves them more susceptible to interpretation *(discussed in Section 3.2)*.

Certain types of AI programs and robotics may need to follow different regulations to other types, as they may require access to data in a different manner. This could mean each sub-field of program and robot would require unique regulations, which would become extremely difficult to enforce as it brings up the question about whether *there [are] specific criteria they must meet to be able to qualify* (Tavani 2018).

3.2 Interpretation of the Regulations

As discussed earlier, there are benefits to having high-level regulations. However, this approach is open to different interpretations by different groups, which can cause problems when it comes to enforcement. Different cultures may weight certain values as more important compared to another culture or they may define fairness differently. Therefore, regulations need to be specific enough that they cannot be interpreted in different ways, but not conflict with other principles or regulations in other sub-fields of robotics and AI. This highlights the need for balance, which is a common theme with the topics discussed throughout this report and will be once again highlighted in the next sub-section and the report's conclusion.

3.3 Balance of Data Privacy for the Stakeholders

Countries with governments that hold a lot of info about the population are able to use this info to improve health care and infrastructure, whereas a country with more privacy rights will struggle to do this a lot more. For example, a country's public transport infrastructure could be greatly improved by gathering data on the general public's journeys. This will benefit the users by making their journey's cheaper, easier, safer and quicker, but at the expense of their data being shared by the government with the companies contracted to improve the system. Therefore, if there were suitable regulations in place, the public might feel more at ease and the company wouldn't have the opportunity to abuse this trust. This scenario is a good example to show how the balance can be fairly equal between the companies wanting to use the data, the government and the stakeholders (the general public), and this is the sort of approach that will likely be the best to take.

4 Conclusion

Throughout this report a key theme has been striking a balance, from a combination of the EU and US approach to the types of regulations and the benefits of different cultures. This balance is what will ensure the regulations are as restrictive as they need to be, while also giving companies and governments the chance to use the new technologies to enhance lives. The most important balance though, is that the general public benefit from the use of their personal data while not feeling like they are being adversely affected.

5 Appendices

Appendix A

Google have a page dedicated to the principles they follow and believe the sector should adhere to, which is listed below:

https://www.blog.google/technology/ai/ai-principles/

Appendix B

Organisations in the US have been set up specifically to tackle the problem of AI ethics and principles, with advice and tenets which their partners follow:

https://www.partnershiponai.org/tenets/

References

Koch, Christoph (2007). *33rd International Conference on Very Large Data Bases : University of Vienna, Austria, September 23-27 2007 : conference proceedings*. [Association for Computing Machinery], p. 1444. ISBN: 9781595936493.

Mehmood, Abid et al. (2016). "Protection of big data privacy". In: *IEEE Access* 4, pp. 1821–1834. ISSN: 21693536. DOI: 10.1109/ACCESS.2016.2558446.

Tavani, Herman T. (Mar. 2018). "Can social robots qualify for moral consideration? Reframing the question about robot rights". In: *Information (Switzerland)* 9 (4). ISSN: 20782489. DOI: 10.3390/info9040073.

Wachter, S, B Mittelstadt, and L Floridi (2017). *Transparent, explainable, and accountable AI for robotics*, p. 6080.

Whittlestone, Jess et al. (Jan. 2019). "The role and limits of principles in AI ethics: Towards a focus on tensions". In: Association for Computing Machinery, Inc, pp. 195–200. ISBN: 9781450363242. DOI: 10.1145/3306618.3314289.

Xu, Lei et al. (2014). "Information security in big data: Privacy and data mining". In: *IEEE Access* 2, pp. 1149–1176. ISSN: 21693536. DOI: 10.1109/ACCESS.2014.2362522.

Zadeh, Lotfi A (2001). *A New Direction in AI: Towards a Computational Theory of Perceptions*.