BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

House of Lords Select Committee on Artificial Intelligence

Big Brother Watch Response

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaign group. We campaign to give individuals more control over their personal data, and hold to account those who fail to respect our privacy, whether private companies, government departments or local authorities. We have produced unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

INTRODUCTION:

Artificial intelligence (AI) is becoming an unavoidable element of 21st Century life.

AI currently takes many forms including search engines, voice recognition, product or service recommendation systems, photographic analysis and recognition, targeted advertising, and virtual assistants such as Apple's Siri, Microsoft's Cortana, Amazon's Alexa and Google Home.

AI influences the products we purchase, the news we read, the adverts we see and potentially who we vote for. AI is also becoming crucial to the functioning of the economy, being used to carry out trades, decide credit scores, and calculate and decide on financing and lending.

Large scale datasets are the fuel for many, if not all AI initiatives. The large scale acquisition, retention and use of both industrial and personal data brings privacy, security and data protection issues to the fore. This is particularly so if AI is to be used to simulate human decision-making, at which point the very serious problems of biased and prejudiced AI must also be raised.

DEFINITION OF 'ARTIFICIAL INTELLIGENCE (AI)'

We have followed a wide interpretation of AI, including machine learning, which concerns the imitation of human intelligence in an artificial manner, by computer programs, systems or algorithms. This technology can be used to analyse data and make decisions in a similar way to a human.

RESPONSE:

IMPACT ON SOCIETY

Question 3: How can the general public best be prepared for more widespread use of artificial intelligence?

Prepare the public by increasing their understanding and engagement

1. AI is already around us, making important decisions for and about people. However, alarmingly, most people are unaware of what AI is and how it works. This clearly needs to change, but we believe there is a need to go back to basics and engage in educating people about what their data is, as well as the value and importance of their data. Following this, explanation of AI can then flow naturally; the public will understand the fundamental issue that personal and commercial data will power AI, that such data is generated by people and that it can impact how people live.

2. AI, like data, is invisible. It runs in the background of online services like Amazon or Google, so the public are unable to see how it is used, what it is used for and what the benefits or potential

harms are. This leads people to be generally ignorant of what AI is and the extent to which it is currently used.[1] Most people will be unaware that the helpful recommendations they get when they visit a website are created using AI. Most people are also unaware that it is their personal data that fuels AI. It would be helpful for the public to understand that a "smart" product like one powered by AI does not start smart – it only becomes smart because it is trained on information that we give to it. The more it learns about us, the smarter it becomes, but obviously that requires us to tell it everything we can and provide it with large amounts of personal data.

3. The General Data Protection Regulation, in the form of the new Data Protection Bill, will help these conversations to take place, particularly in relation to get people to engage with their rights and responsibilities when it comes to data. But further work can and indeed must be done by Government to alter their current approach as demonstrated in Part 5 of the Digital Economy Act of keeping people at arm's length from their data, to ensuring and encouraging people the right of control over how their data is used.

PUBLIC PERCEPTION

Question 5: Should efforts be made to improve the public's understanding of, and engagement with, artificial intelligence? If so, how?

Public awareness of AI

4. The public must be informed of the affects and effects of AI on their privacy, their security and their data protection. The public know they have an 'online footprint' but rarely understand how they can control access to that data and prevent it from being used for AI purposes or for other purposes than those they can easily see and control. Educational work needs to be given priority to ensure people understand their role and duty of responsibility as a digital citizen.

Transparency and Interpretability of AI

5. Whilst the corporate concerns regarding the intellectual property of AI and algorithms are well known, we must be very careful not to place greater emphasis on, and protection of, the rights of corporations, over the rights of the citizen whose data is being used to fuel the products and services offered by the public and private sectors.

6. Because AI can fundamentally impact a person's life, moves should be undertaken to ensure that the transparency of AI programs is standard, particularly when AI is used to make a decision affecting people or impact how people live their lives. The public must always be fully aware of when they are subject to, or affected or impacted by a decision made by AI. Increased transparency and accountability of public-facing AI, including the methods behind the system, and the reasons for decisions, will not only benefit society as a whole in terms of open source information but will increase public trust and confidence and subsequently, public engagement with AI systems.

7. We welcome the moves in the General Data Protection Regulation (GDPR) towards greater protection over automated machine-based decision-making and profiling, however the protections offered are just the start: as AI and interconnected technologies take greater hold, work to ensure the protection of people's digital lives will need to be monitored closely.

[1] The Royal Society, *Machine learning: the power and promise of computers that learn by example* (April 2017), pg85. (https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf) Last accessed 24/08/2017.

Privacy and cyber-security

8. Promoting the fundamental importance of protecting privacy in AI systems, such as the 'privacy by design' approach, should be encouraged as an industry standard. If the public are confident that the systems they use are protecting their private information, and that they themselves are in control, their confidence in the technology will improve. Privacy by design and security by design are well established concepts encouraged to ensure that from the very beginning, during the research and development of a project, the security and privacy of data, of the system, and of the individual using the system are built into the design, and not left as an afterthought at the end of production.

9. The impact of cybercrime is reported to cost the UK billions of pounds a year and is only set to grow as a problem.[2] It is therefore no longer acceptable for companies to sell devices which offer little to no protection for citizens and organisations alike. It is also not acceptable for public or private sector organisations to adopt technologies including AI without ensuring cyber-security protections are standard.

10. The encryption argument is contentious and one which is often presented, disingenuously, as a zero sum game. Whilst solutions for societal threats are consistently being sought, we must be careful not to undermine the security of all in a connected society as a reaction to other threats. The importance of end-to-end encryption as a much needed and fundamental tool for the security of the digital citizen in a digital world, which protects the security of more people than it harms, as well as organisations and national infrastructures, must be recognised and championed.

AI and the democratic process

11. The use of AI-driven analytics in relation to the democratic process is a growing area of concern. Analysis of people's data in order to determine how they may vote and what their specific areas of concern are nothing new, but the connectivity of communications, the impact of social media as a platform for sharing ideas and the ability to harvest, analyse and make conclusions from that data is a capability which is only now being realised, due to the capabilities of AI.

12. AI can analyse publicly available information people have posted online and draw personal insights from it.[3] Basic public datasets, such as Facebook 'likes', can be analysed to make predictions on people's political views.[4] This information is clearly of real value to political campaigns during elections.

13. There are restrictions on how much money can be spent by political parties during elections on campaigns, including online campaigns. However, there is an issue with the rise of 'dark advertisements' – an election-related message, targeted at a specific group or groups based on such publicly available information. The prevalence of these 'dark ads' during the 2017 General election was documented by the website 'Who Targets Me'.[5]

14. As with the use of traditional media in political campaigns, such data use for political purposes must be scrutinised. We welcome the investigation being undertaken by the Information

[2] National Crime Agency (2016) http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

[3] The Royal Society (2017), *Machine learning: the power and promise of computers that learn by example* (April 2017), pg90

[4] Kosinski M, Stilwell D, Graepel T (2013), *Private traits and attributes are predictable from digital records of human behaviours*, PNAS 110 5802-5805

[5] Who Targets Me website: https://whotargets.me/en/

Commissioner's Office into the use of data analytics for political purposes, but see this as just the start.

ETHICS

Question 8: What are the ethical implications of the development and use of artificial intelligence? How can any negative implications be resolved?

AI exhibiting and reinforcing bias

15. Data and the algorithms they populate are meant to be free from prejudice and bias. However it is well reported that bias and prejudice within data which is used to train AI can lead to bias and prejudice in the results.[6]

16. This happens in all aspects of AI, from advertising to insurance to healthcare. We have chosen to draw your attention to the problems of bias in AI in relation to policing and criminal justice.

17. For example, a US court computer program – Compas – designed to assess the risk of re-offending, was discovered to have "turned up significant racial disparities"; the algorithm "was particularly likely to false flag black defendants as future criminals, wrongly labelling them this way at almost twice the rate as white defendants".[7]

18. It was reported in May 2017 that Durham Police are preparing to use AI to decide whether, like the US Compas system, suspects should be kept in custody.[8] The system uses data beyond a suspect's offending history, including their postcode and their gender[9] to assess the risk of re-offending, and contributes to the decision whether to keep a suspect in custody or release them.

19. Systems such as those used by Durham police, facial biometric technology – another form of AI – and issues relating to bias and false positives being determined by poorly built algorithms, are a very real concern. Extensive research has been undertaken in the US outlining problems of AI in this area.[10] We draw this to your attention as there are increased moves to roll out facial biometric systems by UK police forces with vast investment coming from the Home Office. There has been no parliamentary scrutiny of these plans yet we know such technologies have been used at the Champions League Final in Cardiff this year, Notting Hill Carnival in 2016 and 2017 and Download Festival in Leicester in 2015. Furthermore we know that police forces are building their own facial biometric systems which are being used to make algorithms of people who are un-convicted of any crime or wrongdoing – challenging the concept of innocent until proven guilty.

20. Biased AI is an extremely serious concern in relation to fundamental civil liberties of equality and non-discrimination. Any such automated decision making must be subject to regulation and oversight. Intrusive surveillance technologies are consistently being purchased and rolled out by law enforcement, local authorities and official organisations without any debate in parliament, or any regulation or legislation. This is a very worrying trend, particularly when the technology is being trialled when its abilities are far from accurate.

[6] The Guardian (2017) https://www.theguardian.com/technology/2017/apr/13/ai-programs-exhibit-racist-and-sexist-biases-research-reveals

[7] ProPublica (2016) https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

[8] BBC News (2017) http://www.bbc.co.uk/news/technology-39857645

[9] *Ibid*

[10] The Atlantic (2016) https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/

AI and Privacy

21. It is an ongoing concern that the more data you have the better the outcomes are. This is a misnomer: the quality of data is critical, not the quantity. Citizens consistently raise concern about the lack of control over the data they are asked to provide, in order to access or benefit from a service; we have seen this from our own research.[11] As AI grows the need for more and more data in order to support the system's ability to learn, grow, and, subsequently apply learning will be phenomenal. As a result, there is the potential that vast amounts of sensitive and or personally identifiable data will be collected, such as being 'scraped' from the internet. This is a huge concern for people's personal privacy.

22. Whilst education will be critical, a different approach must be encouraged by Government. For example, the Digital Economy Act uses the word "wellbeing" as a reason for bulk data sharing. "Wellbeing" is ill-defined and has been heavily criticised by the Supreme Court during the Scottish Parliament's controversial Named Person Scheme which intended on sharing the data of all Scottish children with a non-adult parent in order to protect them. The overarching view was that "wellbeing" falls short of the standard data protection view that data should only be used when "vital". Such nudge tactics in the area of data, privacy and AI are worrying and must be addressed.

Anonymisation

23. The analytical capabilities of AI in the 'big data' environment have the potential to completely undermine formed notions of privacy, especially in the context of 'anonymised' data. We have consistently raised concern about the promises of anonymisation as a panacea.

24. There are countless studies where researchers have re-identified people from anonymised datasets. We would recommend the committee look at the work of Professor Latanya Sweeny Phd (Professor of Government and Technology at Harvard University, Director of the Data Privacy Lab and former Chief Technologist at the Federal Trade Commission) who proved that 100% re-identification was possible even when the data was anonymised.[12] By taking the South Korean Resident Registration Number – which closely matches the makeup of the UK's NHS number – Professor Sweeny was able to re-identify all citizens using two entirely different methods.

Consent

25. We welcome the moves in the GDPR to improve the way citizens are required to give consent to how their data is used and what protections organisations must undertake to ensure informed consent has been given. However there remains little requirement for organisations to fully inform people of who their data might be shared with and for what specific purpose. This remains a very serious concern. If citizens' data is to become part of the product – as we see with many AI technologies – there should be far greater transparency of how data will be acquired, used, shared and stored, with specific informed consent to be given and withdrawn if necessary, with no detriment to the individual.

[11] Big Brother Watch (2015) https://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/03/Big-Brother-Watch-Polling-Results.pdf

[12] Technology Science (2015), De-anonymizing South Korean Registration Numbers Shared in Prescription Data, 29th September 2015: https://techscience.org/a/2015092901/

Question 9: In what situations is a relative lack of transparency in artificial intelligence systems (so-called 'black boxing') acceptable? When should it not be permissible?

Transparency and interpretability of AI

26. Certain forms of AI such as neural networks or 'black-box' systems can be virtually impossible to audit because of their very nature: a process which is hidden and always changing. This can result in a serious accountability deficit. An example of this is the risk of re-offending algorithm used by Durham Police. If the decision making process is unknown and cannot be analysed, this precludes fundamental and basic principles of oversight and accountability, and runs the risk of limiting a judge's ability to render a fully informed decision.[13]

27. If we don't fully understand the AI we create or whose decisions we are subject to, we won't be able to predict or pre-empt failures, and we won't be able to address their failings. If an individual is subject to a decision by AI, but is not able to know the reasons for the decision, or the decision-making process, this results in an unacceptable accountability deficit.

28. Automated decision-making systems are already in use and are governed by Section 12 of the current Data Protection Act. We are pleased to see the protections emphasised in the GDPR with what is effectively a challenge to the "computer says no" approach to decision making and the encouragement of a human point of view as a right. However, the more widespread use of more advanced AI programs must also be subject to the same regulation, and there must not be loopholes. In the same way that a public body must be publicly accountable, where AI programs involve, affect or impact the public, they too must be accountable, but they must also be transparent; the programming of AI and its inner-workings must be open for scrutiny.

THE ROLE OF THE GOVERNMENT

Question 10: What role should the Government take in the development and use of artificial intelligence in the United Kingdom? Should artificial intelligence be regulated? If so, how?

29. Artificial Intelligence clearly has the potential to be immensely powerful and provide a wealth of benefits to individuals and society as a whole, but for the benefits to be achieved protections will need to be put in place to ensure that individuals are not put at risk by machine learning, algorithmic bias or poor data protection.

30. Government has the opportunity to lead the way in establishing a new approach to how we live in a connected society, as opposed to falling in line with the approach taken by big business.

31. We would like to see independent oversight of AI in the form of a regulatory or supervisory body to provide legal and technical scrutiny of AI technology and algorithms.

32. With regard to the use of AI technologies for policing or in the criminal justice system, any system which uses machine learning, AI or algorithms to police society must be subject to independent scrutiny and parliamentary debate before it is implemented.

[13] Wired (2017) https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/?intcid=inline_amp