Senators Schumer, Rounds , Heinrich, Young,

I bring you greetings from Brooklyn, New York and thank you for this kind invitation to the forum. My name is Mutale Nkonde, I am a policy fellow at the Oxford Internet Institute, and founder and leader of AI for the People.

In order to increase the identification of liability in the privacy space we can look at policies or legislative actions which are increasing AI accountability and use them as a model for privacy legislation.

Current work being done on AI Liability in Congress

People/organization that should be consulted	Potential Model	How this Contributes to Approaching Liability in AI Legislation
Lead House Sponsor Congresswoman Yvette Clarke, (D 9-NY) Lead Senate Sponsor Senate Sponsor Corey Booker, (D2-NJ)	H.R. 5628[1]	**A MODEL FOR EMBEDDING PRIVACY INTO THE MANUFACTURING PROCESS** This can be done by adding impact assessment during the testing and validation part of the engineering process. Therefore regulators can identify privacy breaches and disparate impact **before** the technology goes live.
Lead House Sponsor Congressman Frank Pallone ,(D6-NJ) Lead Senate Sponsor Roger Wicker (R 1-MS)	H.R 8152[2]	**A MODEL FOR PRIVACY BY DESIGN** Section 101.Data minimization, which stops companies from gathering excess information from consumers.

[1] H.R 5628, (September 21, 2023), *Algorithmic Accountability Act of 2023,* read the bill here https://www.govinfo.gov/app/details/BILLS-118hr5628ih

[2] H.R 8152, (December 20, 2022), *American Privacy and Protection Act,* read the bill here https://www.govtrack.us/congress/bills/117/hr8152/text

LEGISLATION SHOULD ADDRESS: PROBLEMS WITH ESTABLISHING LIABILITY

Designing for privacy: looking at ways to decrease privacy violations at the design stage

Definition of Design Defects that appear before the product is manufactured in 47 states the plaintiff (the aggrieved party or victim) has a burden of proof to prove the existence of a design defect[3].

- **Why this is inadequate within AI Environments:** In this legal framework consumers have to identify and prove the harm before taking legal action. However due to the lack of transparency into how AI systems work, how will consumers know when and how their data is stolen?

- **How AI liability is currently being considered by lawmakers.** In September 2023, Congresswoman Yvette Clarke from New York's 9th District reintroduced H.R 5628 *The Algorithmic Accountability Act of 2023*. in Section 12 of impact assessments, so regulators can anticipate the liabilities of said technologies **before they hit the market**[4].

- **Why is impact assessment so important? :** In the privacy setting understanding if the product presents a privacy risk can stop large data breaches becoming a reality. This can be done by mandating companies conduct impact assessment during the testing and validation of the design process of technologies used in high stakes decision making, which impact people within the protected classes most heavily.

- **How to Design with Privacy In Mind:** Lawmakers should pass legislation to earmark funds to recruit and develop a class of civil servants whose role is to interpret the impact assessments provided by companies that produce AI systems involved in high stakes decision making. Create federal guidelines and standards they have to reach before being given permission to enter the US.

[3] Cornell School of Law, Product Liability, find the fact sheet here https://www.law.cornell.edu/wex/products_liability#:~:text=With%20 regard%20to%20 products%20 liability,will%20be%20liable%20for%20it.

[4] H.R 3044, (May 2, 2023), *Real Political Ads Act,* read the bill here https://www.congress.gov/118/bills/hr3044/BILLS-118hr3044ih.pdf

LEGISLATION SHOULD : REMOVE THE BURDEN OR PROOF ON THE CONSUMER

One area this can be done is in the manufacturing process.

Definition of Manufacturing Defects: Manufacturing defects occur during the construction or production of the item[5].

- **How Can the Manufacturing of AI Systems Lead to Privacy Disclosures:** AI systems take in more information than they need to manufacture products, but what happens to this information once it is gathered? It is simply labeled as data fog and can be sold to third parties who then create products that encroach on our privacy.
- **What was the source of harm?** One example of this is the company Fog Data Science which buys the geolocation data from our smartphones and has created a subscription service for law enforcement agencies that are happy to gain access to a massive, searchable database of where people are located[6]. This could be viewed as a warrantless search which is in violation of the fourth amendment and struck down by the second circuit during New York City's Stop and Frisk era[7].
- **How can data minimization prevent this** In Section 101 of the American Privacy and Data Protection Act of 2022[8] Congressman Pallone asks that companies only gather the information they need. This prevents excess information about the American people being held by companies and moves us towards privacy first manufacturing practices.
- **How Does This Reduce the Burden of Proof On the Consumer?:** This is an example of how the government can set the rules of the road for engineering practices and moves us towards the rights respecting AI environment outlined in the White House Executive Order on AI.

[5] Cornell School of Law, Product Liability, find the fact sheet here https://www.law.cornell.edu/wex/products_liability#:~:text=With%20regard%20to%20products%20liability,will%20be%20liable%20for%20it.

[6] Matthew Guariglia (August 31, 2022) What is Fog Data Science? Why is the Surveillance Company so Dangerous?, Electronic Frontier Foundation, read the article here https://www.eff.org/deeplinks/2022/06/what-fog-data-science-why-surveillance-company-so-dangerous

[7] Joseph Goldstein (August 12, 2013) Judge Rejects New York's Stop-and-Frisk Policy, New York Times, read the article here https://www.nytimes.com/2013/08/13/nyregion/stop-and-frisk-practice-violated-rights-judge-rules.html

[8] H.R 8152, (December 20, 2022), *American Privacy and Protection Act,* read the bill here https://www.govtrack.us/congress/bills/117/hr8152/text

LEGISLATION SHOULD ADDRESS: : DECEPTIVE MARKETING OF AI PRODUCTS

Seeking to reduce deceptive marketing practices reduces the presumption of privacy by consumer

Definition of Marking Defects: Defects in marketing deal with improper instructions and failures to warn consumers of latent dangers in the product[9].

- **How Can Deceptive Marketing Practices Breach Privacy:**Over the last few months there have been major concerns about the development of Chat GPT4 because it is manufactured by scooping up information on the internet which includes but is not limited to personal information and protected works without the knowledge and/or permission of impacted parties[10].
- **What was the source of harm?** This lack of disclosure can lead consumers who buy/and or lease AI products developed in this way to assume they have full rights to the programs but that is not necessarily true[11]. We can see the impacts of this in the art world. For example, in May 2023, the Supreme Court ruled against the Andy Warhol Foundation in *Andy Warhol Foundation for Visual Arts Inc. vs, Goldsmith et a*l in which foundation used a photo of Prince to create a silkscreen of the artist that had been licensed to Vanity Fair by the photographer Lynn Goldsmith. The Court ruled the foundation had violated Goldsmith's copyright because they did not seek permission to create the silk screen[12]
- **How legislation can prevent the illusion of privacy**. Legislation on secondary use of original works within the creation of AI products could close this loophole and in the

[9] Cornell School of Law, Product Liability, find the fact sheet here https://www.law.cornell.edu/wex/products_liability#:~:text=With%20regard%20to%20products%20liability,will%20be%20liable%20for%20it.

[10] Uri Gal, (February 9, 2023), ChatGPT is a data privacy nightmare. If you've ever posted online, you ought to be concerned, The Conservation, read the article here https://theconversation.com/chatgpt-is-a-data-privacy-nightmare-if-youve-ever-posted-online-you-ought-to-be-concerned-199283

[11] Gil Appel et al, Generative AI Has an Intellectual Property Problem, Harvard Business Review, find the article here https://hbr.org/2023/04/generative-ai-has-an-intellectual-property-problem

[12] United States Supreme Court,l (May 18, 2023), Andy Warhol Foundation for Visual Arts Inc. vs, Goldsmith et al, read the decision here https://www.supremecourt.gov/opinions/22pdf/21-869_87ad.pdf

creation of AI products by forcing them to seek permission for the source data used in the production of their products.

Recommendations

Three ways that Congress can write legislation that safeguards the privacy of US Consumers is by:

- **Developing Policy which incentivizes Transparency.** The use of consumer data without knowledge or consent of impacted people should be banned. And companies should secure the rights of information used in train datasets. There has not been a successful challenge to this using AI products but we can look to *Andy Warhol Foundation for Visual Arts Inc. vs, Goldsmith et a*l which ruled against the foundation because they did not seek permission from Lynn Goldsmith a photographer to create a new work. As indication that the use of datasets that include information from people and organizations without their permission will not be tolerated in the American context. Legislation could be used to make AI producers seek permission from the creators of their source data.

- **Developing Policy which incentivizes Privacy by Design:** The adoption of the use of impact assessments as boilerplate language across all AI legislation as offered in H.R 5628 *The Algorithmic Accountability Act of 2023* provides law makers with insights on impact technologies have on the American people before they go to market. This can be done at the testing and validation stage of the engineering process and can look at questions like, how easily can this system be compromised? Does this technology's functionality comply with existing discrimination laws and should companies consider the encryption of technologies that operate in highly sensitive verticals. For example transmission of healthcare data, to ensure the information transmitted remains private. This would have to be accompanied with legislation to earmark funding for a class of civil servants who can both interpret and create federal standards around AI safety.

- **Developing Policy which incentivizes Privacy First Manufacturing Processes.** In line with the American Privacy and Data Protection Act of 2022, which will prevent the excess collection of access data during the manufacturing process. This is not only privacy respecting but it prevents the sale of excess data to third party data brokers who may use it in ways that not only present new privacy concerns, but operate in violation to existing civil rights laws.