Luminate
Building stronger societies

# The Data Delusion: protecting individual data isn't enough when the harm is collective

Author: Martin Tisné, Managing Director, Luminate

Editor: Marietje Schaake, International Policy Director, Stanford University's Cyber Policy Center

July 2020

## The threat of digital discrimination

On March 17, 2018, questions about data privacy exploded with the scandal of the previously unknown consulting company Cambridge Analytica. Lawmakers are still grappling with updating laws to counter the harms of big data and AI.

In the Spring of 2020, the COVID-19 pandemic brought questions about sufficient legal protections back to the public debate, with urgent warnings about the privacy implications of contact tracing apps.[1] But the surveillance consequences of the pandemic's aftermath are much bigger than any app: transport, education, health systems and offices are being turned into vast surveillance networks. If we only consider individual trade-offs between privacy sacrifices and alleged health benefits, we will miss the point. The collective nature of big data means people are more impacted by other people's data than by data about them. Like climate change, the threat is societal and personal.

**"The collective nature of big data means people are more impacted by other people's data than by data about them. Like climate change, the threat is societal and personal."**

In the era of big data and AI, people can suffer because of how the sum of individual data is analysed and sorted into groups by algorithms. Novel forms of collective data-driven harms are appearing as a result: online housing, job and credit ads discriminating on the basis of race and gender, women disqualified from jobs on the basis of gender and foreign actors targeting light-right groups, pulling them to the far-right.[2] Our public debate, governments, and laws are ill-equipped to deal with these collective, as opposed to individual, harms.

## Data is the new $CO_2$

As with $CO_2$, data privacy goes far beyond the individual. We are prisoners of other people's consent. If you compare the impact of data-driven harms to those of $CO_2$, it becomes clear how impacts are societal, not individual. My neighbour's car emissions, factory smoke from a different continent, affect me more than my own small carbon footprint ever will. This collective threat of climate change is well reflected in environmental law and it underpins the (political) logic of emissions reductions and the Paris accords.[3]

Individuals may enjoy short-term benefits from what will harm the collective in the long term. Thinking optimistically, the Coronacrisis could open the path to laws dealing with collective data-driven harms. More likely, the clash between society's immediate and understandable healthcare fears will be pitted against privacy protections. For example, the UK health minister said that "no one should constrain work on responding to coronavirus due to data protection laws".[4] Even the European Commission's Data Strategy focuses mostly on empowering individuals with regards to "their" data.[5] The need for collective data rights continues to be ignored.

## From collective to individual rights, and back

Data rights were historically not as individualized as they are today. Human rights law at the end of the Second World War focused largely on protecting groups. The Nazi regime had oppressed and massacred Jews, Roma and other persecuted peoples on the basis of their belonging to a minority group. The collective harm wrought by a pernicious state was articulated with the concept of genocide: a new concept to describe crimes committed "with intent to destroy, in whole or in part, a national, ethnical, racial or religious group." The aim was then to protect groups from future genocidal crimes.[6]

In the 1970s, the pendulum began to swing in the direction of individual privacy, with the rise of computing. The Organisation for Economic Development and Cooperation (OECD) developed a set of privacy guidelines in 1980. These guidelines popularized the notion that individuals should give informed consent for any information used for and about them. [7] During the same period, the 1978 French data protection law enshrined the notion that people's personal data must be collected and processed fairly and lawfully for specified, explicit, and legitimate purposes, and with the consent of the person themselves (referred to as the "data subject"). [8] The French law in turn inspired the European Union 1995 Directive on personal data protection, which inspired the 2018 General Data Protection Regulation (GDPR) often called the gold standard of data protection laws. Today, data rights are seen as 'individual rights' and individualisation of data rights has become a cornerstone of data protection laws around the world.[9]

## Why the individualist fallacy suits Big Tech

When media design professor David Carroll sought to retrieve data about him from Cambridge Analytica, he filed a legal claim under the UK's data protection law. Prof. Carroll then challenged the company's liquidation, citing the public interest in accountability and independent oversight. Court documents show that he believed learning more about how his individual data was being collected and used would shed light on the impact of big data and AI on the collective, on democracy. His appeal was dismissed.[11] The case shows how hard it is for individuals to seek remedy for collective harms, as opposed to personal privacy invasions.

**"The era of machine learning effectively renders individual denial of consent meaningless."**

The irony of history is that as governments and laws moved from protecting groups to protecting individuals, technology firms were moving the other direction, from analysing individual behaviour towards that of groups. The era of machine learning effectively renders individual denial of consent meaningless. Even if I refuse to use Facebook or Twitter or Amazon - the fact that everyone around me has joined means there are just as many datapoints about me to target.

As engineers and companies began to deploy increasingly complex algorithms, coupled with data gathered at scale, the market has evolved beyond transacting individual data, towards extracting value from collective data. The fact that laws remain focused on the individual puts them out of touch with the rapidly unfolding reality that technology and artificial intelligence creates. Our societies need collective and individual level data rights, similarly to non-discrimination law which covers individuals and groups.[10]

The value of an individual's data to Google or Facebook is marginal. For companies, the value lies in the inferences drawn from your interaction with others.[12] In 2018, Facebook generated $10/year income per active daily user.[13] The harms that the individual can demonstrate are thus minimal. Blending individuals into a class and tracking how that class responds to different stimuli means Google cannot say how data about you has been used. But the value of their processing of collective data is enormous. From those $10 per person per year, Facebook generated an annual net income of $22bn in 2018, while Alphabet generated $30bn. Companies with data analytics capabilities were found by PwC to have higher stock market values than peers within the same industry.[14]

The laws and thinking developed in the 1970s are no longer suited to deal with today's reality. The issue here is a fundamental mismatch between the logic of the market and the logic of the law.[15] Contemporary technology markets extracts value from collective data. Our laws respond to individual harms and have not changed to reflect changes in technology. Governments should change legal regimes to match the logic of the market. Perhaps urgency has been lacking so far because

the nature of the collective harms – much like $CO_2$ pollution – is invisible to the average person. Algorithms are cloaked in secrecy, their effects omnipresent but invisible. The notion of injustice, which can lead to awareness and legal claims, is evanescent when the injustice was committed invisibly, by a computer model (though designed by humans).[16] Collective action is therefore also less likely to take place.[17] The task at hand is to understand the nature of novel harms and make the invisible visible.

uploading public photos of themselves on a popular American dating website, as these were used by researchers controversially developing algorithms to ascertain people's sexuality based on their facial characteristics.[19] Individuals whose photos are used are not the only ones harmed necessarily. People whose sexuality is "identified" (however spuriously) via these techniques are the ones harmed via inferences made as a result of data collected and processed.[20]

**"Even if I refuse to use Facebook or Twitter or Amazon – the fact that everyone around me has joined means there are just as many data points about me to target."**

## Making the invisible visible: collective data-driven harms

The more collective the harm, the less people are protected and the less visible it is. The more the harm is individual, the more visible its impacts are and the more people are legally protected. If a person is discriminated against because of protected characteristics such as their age, gender or ethnicity, it will be visible to them and they will hopefully be in a position to seek redress. When a person is discriminated against due to an algorithmic decision, it is likely to be less visible and, currently, hard to seek redress.[18]

People tend to suffer from data-driven harms in three main ways. First, there are purely individual harms. For example, an individual is seen as unfit for employment due to data directly related to them (e.g. their age). Protections against these types of harms are well established in law.

Second, there are inferred harms. This is where the individual is inferred to be part of a group or category of people but the person whose data is used is not harmed. Consider people

Third, there are optimized harms. These are harms suffered as a result of how machine learning systems are optimized. YouTube's algorithm has concluded that people are drawn to content that is more extreme than what they are currently viewing and leads them to a path that, as academic and activist Zeynep Tufekci has written, might be harmless (from jogging to ultra-marathons) or damaging (from political rallies to conspiracy theories).[21] People are unwittingly profiled by the algorithm. As with all optimisation systems, YouTube's algorithm is single-mindedly focused on its users and does not focus on its externalities on non-users, minorities and anyone who is not on the system (i.e. society at large).

Our countries' legal systems and policy arsenals are ill-equipped to respond to the latter two data-driven harms. Data protection, as currently framed, is premised on a relationship between data controllers and data subjects. As technology becomes increasingly sophisticated, that connection between data controllers and data subjects falters. It is not always clear who the controller is nor which subject has been harmed. A legal vacuum will arise – and possibly already exists – and accountability falls away.[22]

As the world moves further online due to the Coronavirus, companies and governments will collect a lot more information about people through data gathering. This will likely increase the use of automated decisions, for example on how to allocate resources. And with more automation, there will be even greater equity implications. Data processing may decide who gets to have access to education, welfare or to the judicial system. Research over the past five years has shown how the negative impacts of automated decision-making on people fall disproportionately on those already marginalised in society, such as people of colour, women and immigrants. [23]

The 21st century catch to the data privacy and discrimination problem is that the members of the public no longer know which group they are part of or not, only the algorithm does. Many people will not even know that they are being profiled or discriminated.[24] The conversation needs to be reframed around automation and power and which groups will be adversely impacted.

Solutions lie in hard accountability, strong regulatory oversight of data-driven decision making, and the ability to audit and inspect the decisions and impacts of algorithms on society.

## Regulating automation is regulating power: the case for hard accountability

Rather than regulating how people consent to their data being used in order to protect their privacy, policymakers should regulate automation, starting with black box algorithms that collect, sort and classify data. That will take a whole new method of regulation. Members of the public need information, public scrutiny and accountability on and for the disparate impacts of the huge amounts of automation that are pointed at them every second of the day.

In the European Union, the GDPR is weak on automation and collective harms.[25] The accountability of algorithmic decision systems are mainly covered by articles 13-15 and 22 but these are limited to decisions that are wholly automated, that use personal data, and that are deemed "significant decisions" thus eluding many of the smaller harms detailed earlier, which cumulatively amount to significant collective harms.[26] GDPR further individualises data-driven harms by requiring the person who suffered the harm to be at the centre of any claim resulting from it. That would be like requiring that a case on the $CO_2$ emissions of an entire country depend on its provable impacts on one person.[27]

> "Our societies need collective and individual level data rights, similarly to non-discrimination law which covers individuals and groups."

Three elements are needed to ensure hard accountability: (1) clear transparency about where and when automated decisions take place[28] and their impact on people and groups, (2) the right to give meaningful public input and call those in authority to justify their decisions, and (3) the ability to enforce sanctions.[29] A Public Interest Data Bill should encapsulate these three points.

**Clear transparency**

The focus should be on public scrutiny of automated decision making and the types of transparency that lead to accountability.[30] This includes revealing the existing, purpose and training data behind the algorithms, as well as their impacts – whether they led to disparate outcomes, and on which groups. Clear and targeted transparency sheds light on the algorithms and the institutions that deploy them, e.g. revealing information about institutional performance (e.g. use of facial recognition cameras by the police and their impact), and are explicit about what gets measured, by whom and how. But transparency remains a necessary but not sufficient condition for accountability. [31] For that, meaningful public input and the possibility to enforce sanctions are needed.

"Solutions lie in hard accountability, strong regulatory oversight of data-driven decision making, and the ability to audit and inspect the decisions and impacts of algorithms on society."

**Public participation**

The public has a fundamental right to call those in power to justify their decisions. This "right to demand answers" should not be limited to consultative participation where people are asked for their input and officials move on. It should include empowered participation where public input is mandated prior to the roll-out of an algorithm in society. For example, algorithmic impact assessments should provide members of the public the possibility to give meaningful input into the use of automated decision making, expanding such assessments as a tool for community-driven decision making.

**Sanctions**

Finally, the power to sanction is key for these reforms to succeed and for accountability to be achieved. The GDPR has been hobbled by the lack of funding and capacity of data protection commissioners across Europe. Despite the GDPR's power to impose fines of up to 4% of a company's annual turn-over, few such fines have been meted out and half of Europe data protection regulators only have five or fewer technical experts.[32] But data protection or information commissions cannot be solely responsible for the accountability of algorithms as our societies are transformed by artificial intelligence. Companies and governments need laws that restrict data usage and automation, above and beyond implications for people's personal data. For this, societies will also need the modernisation of sectoral laws such as labour law, criminal law, genetic law, environmental law and discrimination law.[33] For example, laws that regulate the public administration could already be applied here. Administrative law could be used to mandate greater accountability of automated decision making used by the public sector.[34] Labour laws could be adapted to account for the role of technology in managing employer/employee relations.[35]

**Precedent**

Examples exist of draft bills that have sought to fill this gap. In the United States, an effort was undertaken in 2019 to enact an Algorithmic Accountability Act, that subsequently stalled in Congress, aiming to determine whether private sector algorithms resulted in discrimination or not. The Act would have required firms to undertake algorithmic impact assessments in certain situations to check for bias or discrimination.[36] In France, the Digital Republic Law (Loi Pour Une République Numérique) today applies to administrative decisions taken by public sector algorithmic systems but could provide a blueprint for future laws. It provides access to how important automation was to the ultimate decision. It also opens up access to the data used and its source, as well as any treatment parameters and weightings if used in decisions that affected people and provides information on the outcome of the automated process. In contrast, GDPR provides restrictions but only on the use of personal data in fully automated decisions.[37]

## Conclusion

Privacy concerns surrounding COVID-19 brought to the surface a number of systemic mismatches between individual privacy law and the value of collective data processing. The pandemic accelerates the risk of inequality and new harms dramatically as surveillance and data gathering are accelerated in the name of ending the health crisis. Most of those suffering will be already marginalised and vulnerable in our societies. Similar to the collective nature of the threat of climate change, our governments and policy makers must change the way they think about the regulatory response. They need to consider data's collective as well as the individual impact.

# A public interest data bill

## Clear transparency

Require that firms and governments open up the data and source code behind high-risk algorithms and define which are deemed "high-risk" in relation to evidence on the disparate impacts of those algorithms on the population (e.g. whether they fall disproportionality on marginalised communities).

---

Require that firms and governments publish algorithmic impact assessments assessing the outcomes of the algorithmic treatment on groups as well as any collective data-driven harms. Ensure the results of such assessments are published openly. Ensure these precede the roll-out of high-risk AI deployments and renew these on a regular schedule.[38]

---

Ensure full transparency and accountability of automation:

- Tweaks to algorithms that might seem small or insignificant when considered alone, can add up to substantial collective impact when taken together- they would be included. These should not be limited to 'decisions' made by an algorithm nor to those decisions needing to be 'significant' as is currently the case with GDPR article 22.[39]
- Apply both to decisions that are fully, as well as partly automated.[40]
- Require transparency and accountability for how a decision was made based on a computer model, not simply explaining the model in abstract. (The degree and the mode of contribution of the algorithmic processing to the decision taken.[41])
- Cover decisions beyond those that use personal data. For example, this would cover self-driving cars, or data that was once personal and then supposedly anonymised. People are impacted by data that is not personal, and by personal data that is not about them.

## Public participation

Provide members of the public the possibility to give meaningful input into the use of automated decision making (including but not limited to input into algorithmic impact assessments).

---

Ensure that public participation is empowered and not merely consultative.

## Sanctions

Ensure the ability to enforce sanctions for non-compliance.

---

Fund and resource accountability bodies adequately, including oversight bodies for sectoral laws such as labour law, criminal law, genetic law, environmental law and discrimination, in addition to data protection agencies.

## Relevance to groups as well as individuals

Enable persons as well as organisations to lodge requests.[42]

---

Provide access to the treatment parameters and, where appropriate, their weighting, applied to the situation of the person(s) or groups concerned.

### About the Author

Martin Tisné is Managing Director at Luminate, a global philanthropic organization. He is responsible for Luminate's Data & Digital Rights impact area, work in Europe, and policy and advocacy. Alongside the Obama White House, Martin founded the Open Government Partnership and helped it grow to a 70+ country initiative. He also initiated the International Open Data Charter, the G8 Open Data Charter, and the G20's commitment to open data principles. Martin is the co-founder of Publish What You Fund, a global campaign for foreign aid transparency, and Integrity Watch Afghanistan, the country's leading anti-corruption NGO. Twitter: @martintisne

### About the Editor

Marietje Schaake is the international policy director at Stanford University's Cyber Policy Center and international policy fellow at Stanford's Institute for Human-Centered Artificial Intelligence. She was named President of the Cyber Peace Institute.

Between 2009 and 2019, Marietje served as a Member of European Parliament for the Dutch liberal democratic party where she focused on trade, foreign affairs and technology policies. Marietje is affiliated with a number of non-profits including the European Council on Foreign Relations and the Observer Research Foundation in India and writes a monthly column for the Financial Times and a bi-monthly column for the Dutch NRC newspaper.


### Author's Acknowledgments

I am extremely grateful to Salmana Ahmed, Madeleine Clare Elish, Kate Crawford, Polly Curtis, Jonathan Fox, Janet Haven, Swee Leng Harris, Gus Hosein, Karen Levy, Jim Peacock, Ravi Naik, David Robinson, Marietje Schaake, Ben Scott and Sandra Wachter for reviewing this paper in draft form and their hugely helpful comments.

I would also like to give special thanks to Adrien Abecassis, Julia Angwin, Azeem Azhar, Solon Barocas, Ailidh Callander, Simon Chignard, Sylvie Delacroix, Alix Dunn, Alex Goodman, Seda Gürses, Kieron O'Hara, Gry Hasselbalch, Carly Kind, Neil Lawrence, Sean Macdonald, Aiha Nguyen, Tanya O'Carrol, Reema Patel, Seeta Peña Gangadharan, Imogen Parker, Phil Sheldrake, Martha Spurrier, Katarzyna Szymielewicz, Linnet Taylor, Jeni Tennison, Zeynep Tufekci, Michael Veale, Henri Verdier, Stefaan Verhulst, Adrian Weller, Glen Weyl, Meredith Whittaker, and Caroline Wilson Palow for their advice. I am very grateful for their time.


## Luminate

Luminate is a global philanthropic organisation focused on empowering people and institutions to work together to build just and fair societies. We support innovative and courageous organisations and entrepreneurs around the world, and we advocate for the policies and actions that will drive change across four impact areas: Civic Empowerment, Data & Digital Rights, Financial Transparency, and Independent Media. We work with our partners to ensure that everyone has the opportunity to participate in and to shape the issues affecting their societies, and to make those in positions of power more responsive and accountable. Luminate was established in 2018 by philanthropists Pierre and Pam Omidyar. The organisation was founded by The Omidyar Group. www.luminategroup.com

Stanford | Cyber Policy Center
*Freeman Spogli Institute*

The Cyber Policy Center at the Freeman Spogli Institute for International Studies is Stanford University's premier center for the interdisciplinary study of issues at the nexus of technology, governance and public policy. Through research, policy engagement, and teaching, the Cyber Policy Center works to bring cutting-edge solutions to national governments, international institutions, and industry.

## Endnotes

1 See John Thornhill; Naomi Klein

2 Ali, Sapiezynski, Bogen, Korolova, Mislove and Rieke, "Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes", 2019 https://arxiv.org/abs/1904.02095

3 More recently in Holland, the Urgenda Climate Case against the Dutch Government established that the government had a legal duty to prevent dangerous climate change and must significantly reduce emissions to protect human rights.

4 https://twitter.com/MattHancock/status/1240189379676712960?s=20

5 https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy

6 Samantha Power, "A Problem From Hell", 2002.

7 https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

8 https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf

9 These range from the right to be informed, the right to access data, to rectify it, erase it, restrict its processing. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT As per the Charter of Fundamental Rights of the European Union: "everyone has the right to the protection of personal data concerning him or her."

10 I am grateful to Prof. Sandra Wachter for this comment. Please see Affinity Profiling and Discrimination by Association in Online Behavioural Advertising https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3388639

11 The liquidation judge noting that "the relevant 'interests' are Prof. Carroll's interests as a creditor, not his interests as a curious academic or as someone leading a campaign to establish a principle about the use of data or as someone who is unsettled by what might have happened to his data in the past. https://www.judiciary.uk/judgments/vincent-john-green-mark-newman-v-cambridge-analytica-uk-limited-others/

12 A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829

13 https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx

14 https://www.bennettinstitute.cam.ac.uk/publications/value-data-summary-report/ ; pwc.co.uk/issues/data-analytics/insights/putting-value-on-data.html

15 See Julie Cohen, "Between Truth and Power", 2019

16 A recent study of the use of AI in hiring in the UK determined that the auditing tools used to ensure compliance were not able to accurately determine bias in an AI system. Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547922

17 I am grateful to Prof. Wachter for this insight.

18 Pioneers in this field include E. Bloustein's "Group Privacy: The Right to Huddle" https://heinonline.org/HOL/LandingPage?handle=hein.journals/rutlj8&div=24&id=&page= ; Taylor, Floridi and van der Sloot (editors) of "Group Privacy: New Challenges of Data Technologies" https://www.springer.com/gp/book/9783319466064; Mittelstadt "From Individual to Group Privacy in Big Data Analytics" https://link.springer.com/article/10.1007/s13347-017-0253-7

19 https://www.economist.com/science-and-technology/2017/09/09/advances-in-ai-are-used-to-spot-signs-of-sexuality

20 See Dr. Sandra Wachter "A right to reasonable inferences: re-thinking data protection law in the age of big data and AI" https://www.law.ox.ac.uk/business-law-blog/blog/2018/10/right-reasonable-inferences-re-thinking-data-protection-law-age-big

21 https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html

22 See Ravi Naik, 2020 https://jolt.law.harvard.edu/digest/the-gentle-civilizer-of-technology

23 https://www.theguardian.com/technology/series/automating-poverty

24 Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547922

25 https://gdpr-info.eu/

26 "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" Wachter, Floridi, Mittelstadt 2017 https://academic.oup.com/idpl/article/7/2/76/3860948; "Enslaving the algorithm: from a right to an explanation to a right to better decisions" Edwards and Veale 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3052831;

27 The law does allow for NGOs to take up complaints without being mandated by a specific person (the "data subject") but, again after intense lobbying, that section of the law was made optional and only three out of twenty-eight European countries chose to enact it. When NGOs can bring systemic claims on behalf of the public without needing to have a mandate from an individual, data-driven harms could be collectively safeguarded in the same way that environmental harms are. GDPR Section 80. (2) GDPR's main remedy to countering collective data-driven harms is either when the violation of a person's individual rights is symptomatic of the same violation being suffered by all or when a class action can be mounted. There are few such cases. That seemingly obscure section of the law points to a potentially interesting future trend. I am grateful to the team at Privacy International for their time spent explaining this point.

28 Sometimes referred to as the "Blade Runner Law" requiring an automated system or bot to declare itself as such and not camouflage itself as a human.

29 See Prof. Jonathan Fox's distinction between hard and soft accountability here https://www.tandfonline.com/doi/full/10.1080/09614520701469955

30 http://omidyar.com/sites/default/files/file_archive/Public%20Scrutiny%20of%20Automated%20Decisions.pdf

31 Jonathan Fox, "The uncertain relationship between transparency and accountability", 2007, https://www.tandfonline.com/doi/full/10.1080/09614520701469955; Fung, Graham, Weil "Full Disclosure: The Perils and Promise of Transparency", 2007

32 "GDPR accused of being toothless because of lack of resources", Financial Times 20th April 2020, https://www.ft.com/content/a915ae62-034e-4b13-b787-4b0ac2aaff7e

33 For an update of GDPR to cover such issues, see the conclusion of "A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI" https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829

34 Jennifer Cobbe, "Administrative Law and The Machines of Government", 2018 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3226913

35 In response to the optimisation used on Amazon workers, the best answer may be workers' rights and protections rather than laws specifically geared towards the technology used.

36 https://www.congress.gov/bill/116th-congress/house-bill/2231/all-info The bill was a promising start but also criticised for relying on the relatively weak enforcement power of the Federal Trade Commission, for not providing an opportunity for meaningful public input as environmental impact assessments do, and for failing to mandate a clear level of public transparency for the results of algorithmic impact assessments.

37 The French Digital Republic Law (Loi Pour Une République Numérique) is under-researched given the over-focus of the machine learning field on Anglo-Saxon examples and case studies. The law today applies to administrative decisions taken by public sector algorithmic systems but provides a blueprint for future laws. The French law provides access to how important automation was to the ultimate decision. It also opens up access to the data used and its source, as well as any treatment parameters and weightings if used in decisions that affected people. It also provides information on the outcome of the automated process. For example, a person could have access to data and the source code used in an algorithm that decided whether to award them a place to a public university or not, and how that decision was made and weighted (e.g. were their grades more important than where they live?). In contrast, GDPR provides restrictions but only on the use of personal data in fully automated decisions. also ref to Edwards and Veale, 2018

38 https://ainowinstitute.org/aiareport2018.html

39 As Dr. Michael Veale says "decisions that seem "insignificant" at the individual level may actually be very impactful at group level."

40 GDPR provisions for explainability and accountability of algorithms are restricted to decisions that are 100% automated. In reality, most automated decisions have a human involved at some point even if their involvement is superficial or substantially biased by the verdict of the algorithm.

41 https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000031366350&idArticle=LEGIARTI000034195881

42 See footnote 27