

With Algorithmic Accountability, Different Remedies Bear Different Costs for Consumers



*Automated systems and decision making have transformed the ways in which our data is processed and analysed and, accordingly, how companies are able to use it. There are fears that data can be used to discriminate against vulnerable users in ways which are ‘unaccountable’. In this post, **Seeta Peña Gangadharan**, Acting Director of the LSE Media Policy Project, outlines some tools available to allow users greater control over how their data is used and argues that, too often, the burden lies with the consumer rather than the companies designing these automated systems.*

Explore, don't exploit.

– Anonymous data scientist, speaking on ethics and big data

To those of us who think about algorithmic power and accountability (and who are oblivious to the machine learning [reference](#)), the “explore, don't exploit” phrase sounds like a reasonable rubric to inform the development and operation of predictive, automated systems.

Platform services and other products dependent on personal data and powered by algorithms should not exploit or hurt users. Users should not be treated differently by automated systems because of their race, health status, residential location, or some other sensitive attribute. They should not be excluded from society because of errors in datasets or meaningless correlations resulting from data analysis. Nor should they be targeted and taken advantage of because automated systems have accurately inferred they are vulnerable, high-risk populations.

Instead, automated systems should explore relationships in massive datasets and make predictions or arrive at decisions in ways that are appropriate and reflect a process of integrity. And data scientists and the companies that control these systems have the power to make this so.

Unfortunately, many of the proposals about how to hold automated computer systems to account place a greater burden on users than on those responsible for creating these technologies. The bulk of solutions to the problem of unaccountable data-driven systems run on false expectations that consumers can comprehend and act upon information about how a system ought to be working. Instead of focusing on what companies can do, these solutions turn attention to the individual. Even solutions which require some action on the part of companies and which claim to protect consumers, may be placing an undue burden on the user to deal with problems of data-driven systems.

Let users decide.

At one end of the solutions spectrum lies the personal data locker or vault. Businesses around the world are developing products which aim to put “individuals in control” of their personal data. As [reported](#) in a World Economic Forum paper, personal data lockers allow individuals to “set the rules around permissions for collection, usage and sharing of data in different contexts and for different types and sensitivities of data.” This is the ultimate end-user solution: assuage the slightest concern about data-driven systems by giving consumers a product that sets the terms of personal data usage.

Encourage data literacy.



Leaving aside law and systems design, some critics of the “black box society” have called for new ways of teaching and learning about data-driven systems. The idea is not unlike what was said of media literacy in the 20th century: literacy leads to meaningful inclusion in society. Individuals need to explore how automated computer systems work, play with **data** or algorithmic models, or **identify** hidden biases. In so doing, they can become better consumers, exercise their rights, and be better prepared to face challenges and opportunities in automated systems.

Require transparency of automated computer systems.

Speaking primarily about the US context, Frank Pasquale calls for new legal powers to compel companies to open their “black boxes.” One such **proposal** demands that companies reveal both the data and the algorithms used to make determinations about a particular individual. For example a bank that relies on an automated system to assess potential borrowers would have to reveal what factored into a rejected loan. Algorithms, Pasquale says, are not *that* complex. With a little bit of access and adequately designed software tools to inspect such systems, consumers can figure out whether they’re being taken for a ride and make a complaint to an appropriate body, such as the US Federal Trade Commission.

Empower the consumer’s right to object.

Pasquale’s proposal has a European corollary: under the **General Data Protection Regulation**, consumers have the right to approach companies, such as those in the business of automated decision making, and demand explanation about which data companies are using and for what purpose. Lawmakers presume that once armed with such explanations, consumers will be able to contest these particular uses, and the ability of automated computer systems to run wild—or unsupervised—will be held in check.

Audit automated decision making.

Different from the consumer-centred perspective, one alternate proposal offers an engineering alternative. The proposal—discussed by Josh Kroll **here**—focuses on technical mechanisms that let companies demonstrate the integrity of automated decisions. Using computer science, software verification, and cryptographic techniques, systems engineers can audit whether computer systems randomly arrive at a particular outcome, such as recommending a particular kind of loan to a person, ascribing an individual a specific credit score, or pulling someone out of an airport security line for additional checks.

Of these five proposals, the one that least burdens the end user is the last one. It places emphasis on companies—not individuals—to assess the fairness of an automated computer system. The audit furthermore has the potential for multiple beneficiaries beyond the end user: a company that uses the test can use results to make course corrections; policymakers or other stakeholders who need to evaluate algorithmic fairness across different contexts and over time; researchers and journalists who can use the information to debate the cost or benefit of an automated computer system to society.

Transparency efforts—like the consumer protections mentioned above—have multiple beneficiaries as well. But they tend to assume that the consumer will be able to have the time to act upon wrongdoing, adequately make sense of data dashboards, or systematically detect problems in automated decision making.

And while data literacy efforts can have a positive social impact, they typically intersect with debates about algorithmic power well after—versus during—the development of technologies. In other words, it’s too late. Users—knowledgeable or not—are forced into a “take it or leave it” bind. Likewise for personal data lockers—though to an even greater extreme than for data literacy efforts. In addition, the data locker proposal presumes a perfect market for personal data. when in fact **profound asymmetries exist**.



That's not to say that users shouldn't play a role in evaluating data-driven products. They should. And they will. But sharing that responsibility with the creators and operators of automated computer systems ensures that users won't shoulder an unfair burden of detecting when these technologies run afoul. And that will go a long way in protecting individuals and preventing them from being exploited, misused, or misrepresented.

This blog gives the views of the author and does not represent the position of the LSE Media Policy Project blog, nor of the London School of Economics and Political Science.

This post was published to coincide with a workshop held in January 2016 by the Media Policy Project, 'Algorithmic Power and Accountability in Black Box Platforms'. This was the second of a series of workshops organised throughout 2015 and 2016 by the Media Policy Project as part of a grant from the LSE's Higher Education Innovation Fund (HEIF5). To read a summary of the workshop, please click [here](#).

April 8th, 2016 | [Algorithmic Accountability, Featured](#) | [1 Comment](#)

☺

