HOW REFRAMING PRIVACY WOULD UPHOLD DEMOCRACY IN THE DIGITAL AGE

AI and algorithmic decision making are everywhere, and increasingly determine what happens to us, as well as editing the news and adverts we see, acting as our gateway to reality. The world is grappling with these consequences of AI. Many countries, businesses and organizations are equipping themselves with policies, guidelines and strategies to harness the benefits of this technology while tempering the risks. I argue that privacy can continue to make an effective and substantial contribution to upholding human rights and democracy in our datafied societies – but this can only happen if we reframe privacy as a public concept, making privacy law more dynamic on the way.

Ivana Bartoletti*

TPQ
Winter 2021/22

* Ivana Bartoletti is the Global Chief Privacy Officer at Wipro Technologies, and the Founder of the Women Leading in AI Network. Author of An Artificial Revolution: on Power, Politics and AI (Indigo Press), Ivana is a Visiting Policy Fellow at the University of Oxford.

The birth of the internet promised to bring freedom, to connect people globally, break barriers and help achieve liberty, democracy and equality. However, the digital ecosystem that we now inhabit does not deliver on those original ideals.

We live with the consequences of political inaction around digital governance, including weaponized social media, cyber-intrusions that prey on the vulnerabilities of internet architecture, the distorting marketplace of AI-informed predictions about individual internet users' future behaviours, and information monopolies that threaten democratic discourse online.

The good news of the last year is that these negative results have started to be challenged by countries and blocs around the globe. On 21 April 2021, the European Commission presented a proposal for a Regulation concerning artificial intelligence (AI), – the AI Act, for short. This draft AI Act seeks to lay down harmonised rules for the development, placement on the market and use of AI systems. It takes account of their widely varying characteristics and risks, including outright prohibitions and a more nuanced conformity assessment system adapted from EU product safety law. This recognizes that while AI offers us all tremendous opportunities, it carries risks for the fundamental rights of individuals.

In parallel, the EU is proposing a full range of legislative tools aiming to address market dominance and rein in the power of large tech companies. A similar approach is being taken in other countries, from the U.S. to China.[1] For example, Beijing has clipped the wings of its once seemingly untouchable technology giants in a dramatic clash between public and private power and, despite the potentially chilling effects on innovation and economic growth, China's regulators look set to continue high profile enforcement actions in 2022, furthering President Xi Jinping's bid for "common prosperity."

Meanwhile in the U.S., the FTC (Federal Trade Commission) has underscored the links between the protection of privacy and competition law and, under the leadership of its chair, Lina Khan, is enforcing antitrust law and investigating companies.

At the same time, we have witnessed a few years of the exposure of data mishandling and the unfair treatment of women and P.O.C. (People of Colour) in tech, leading to unprecedented levels of tech activism. Unionization of tech workers has surged alongside the awareness that technology is far from neutral: it is embedded into the existing structures of our societies and is very efficient at entrenching existing

[1] Brian Liu and Raquel Leslie, "China's Tech Crackdown: A Year-in-Review," *Lawfare*, 7 January 2022, available at: https://www.lawfareblog.com/chinas-tech-crackdown-year-review (last accessed: 20 February 2022).

inequalities and indeed escalating them.

Within this context, 'ethics' became the new buzzword: over 180 different sets of guidelines have been published to try and define and implement the key principles when developing a fair, responsible and trustworthy use of AI.

My own view is that the debate around ethics has been positive. The incredible contributions of superb advocates including Joy Boulanwini have been crucial to bring these issues into the mainstream. Facebook's decision to delete one billion "faceprints" of real people (used as part of a facial recognition system for photo tagging) would not have happened without the relentless and powerful work of Boulanwini and numerous others.

> *"As AI systems increasingly place allocative functions in our society (on whether we receive a loan, for example), it appears increasingly complex to conceive privacy merely as a set of individual rights that one is entitled to exercise."*

Many in this impressive army of committed ethicists will share my concern about how ethics programmes are being swallowed up by existing tech company mind-sets and practices, and too often just subsumed with a smile. The key point is that ´when ethical ideals are at odds with a company's bottom line, they are met with resistance'[2]. Furthermore, even if individuals genuinely want to create impactful and meaningful change, companies seem adept at taking ethics under their corporate affairs mantle, without properly examining let alone addressing their business strategies and processes.

This is why I argue that privacy and data protection law can make a significant contribution to how we uphold human and social rights in the age of AI and algorithmic decision making. Now more than ever, I am convinced we need to reflect on how privacy, as currently conceived, is tested by big data and AI. In this vein, I hold that the pervasiveness of AI, profiling and algorithmic functions require us to adapt existing legislation in a more progressive and aspirational way.

[2] Andrew Marantz, "Silicon Valley's Crisis of Conscience", *The New Yorker*, 26 August 2019. https://www.newyorker.com/magazine/2019/08/26/silicon-valleys-crisis-of-conscience (last accessed: 20 February 2022).

The Importance of Data Accuracy

In July last year, *Foodinho*, a subsidiary of GlovoApp23, was fined EUR 2.6 million by the Italian Supervisory Authority (SA) known as *Garante per la Protezione dei Dati Personali.* Foodinho was required to amend the way it processes its riders ('delivery drivers') data through a digital platform. On top of that, it was required to verify that the algorithms used to book and assign orders for food and other products do not result in discrimination.

In a joint operation by their supervisory authorities, Italy and Spain (through its AEPD) investigated the digital platform owned by *GlovoApp23*, as the holding company. They identified several infringements of privacy law, particularly in how the algorithms were used to handle employees. For instance, the company had failed to adequately inform its employees on the functioning of the system they were subject to; and it had not implemented suitable safeguards to ensure that the algorithmic results that were used to rate riders' performance were accurate and fair. Nor did the company have any procedures in place to enforce the right to obtain human intervention, to express one's point of view and contest the automated decisions taken using those algorithms – which in some cases excluded a rider from taking up assignments they wanted to work on.

Foodinho was ordered to check the accuracy and relevance of the data used by the system – chats, emails and phone calls between riders and customer care, geolocation at 15-second intervals, mapping of routes, estimated and actual delivery time, details on the handling of current and past orders, feedback from customers and partners, device battery level, etc. This order was also intended to minimize the risk of errors and biases that might for instance result in reducing delivery assignments to certain riders or excluding a rider altogether from the platform. Such risks are also related to the company's rating system, which, relying on the application of a mathematical formula, dished out penalties for riders who did not accept orders promptly enough, or rejected the orders, whilst rewarding riders who accepted orders swiftly or delivered the most orders. The rating takes into account delivered orders, check-ins performed within each booked slot a few minutes after the start of the slot and acceptance of the assigned order *within 30 seconds*.

The above is a clear example of a regulator leveraging existing data protection legislation in an algorithmic context.

The Limits of the Rights Argument in the Context of AI

The ubiquity of data collection poses challenges from a privacy and data protection

standpoint, and we now live in a fully datafied society. Datafication of our persons takes place through various systems that authenticate our identity, allowing us to fulfill our duties (e.g. to file an income tax return) or benefit from our rights (e.g. to enjoy family life, or to receive child benefits or housing subsidies)

So our personhood also expresses itself through a datafied identity.

The key question is how the existing conceptualization of privacy can cater for our datafied identities.

"The current draft EU AI Act proposes self assessments for high risk AI, except for facial recognition technology (FRT), following the product safety legislation already adopted in the EU through the CE marks."

As Daniel Solove[3] puts it, there are two dimensions to data. The first is that data is shared between people. Our datafed identities interact with each other. As Simeon de Brouwer observes, there are "privacy externalities" because people's decisions to allow the collection and use of their personal data can also reveal data about other people[4].

As Solove continues, ´rights also are limited when people's privacy decisions involve interrelated data. Interrelated data is somewhat different than shared data. Shared data involves facts that are directly connected between two or more people – such as genetic data. Interrelated data involves data that is not necessarily shared but that affects inferences made about others. In today's "inference economy," machine learning and other forms of algorithmic decision making work by making inferences based on data sets. Everyone's data in the data set is used to make inferences, which are often then used to make decisions affecting people. As Salomé Viljoen notes, "Data flows are designed to represent the ways that people are like one another and reveal meaningful things about one another; how we are alike biologically, interpersonally, politically, and economically. In sum, because a person's data might be the piece in a puzzle that also enables inferences to be made about others, that

[3] Daniel Solove, *The Limitations of Privacy Rights*, 1 February 2022, available at *SSRN*: https://ssrn.com/abstract=4024790 or http://dx.doi.org/10.2139/ssrn.4024790 (last accessed: 20 February 2022).

[4] Simeon de Brouwer, "Privacy Self-Management and the Issue of Privacy Externalities: Of Thwarted Expectations, and Harmful Exploitation", *Internet Policy Review*, Vol. 9, No. 4 (21 December 2020).

person's exercise of rights can affect other people – and vice versa´.

Within this context, the framing of privacy as an individual right presents a clear fallacy, and that is that it places the burden of control onto the individual in the face of an increasingly complex and opaque data extraction and handling. How is it conceivable for someone to identify, let alone challenge, the existing extraction of personal data which are inherently intertwined with all aspects of our life? This is a crucial issue we must reconcile with.

As AI systems increasingly place allocative functions in our society (on whether we receive a loan, for example), it appears increasingly complex to conceive privacy merely as a set of individual rights that one is entitled to exercise. How exactly is an individual supposed to understand the workings of an algorithm especially when it operates on inferential data, which may not even be fully considered personal data in the first place?[5]

Over recent times, a lot of discussions have focused on transparency, and transparency is indeed a key principle of the GDPR (General Data Protection Regulation). Transparency of an algorithm may be instrumental to understand where the bias may be coming from, and this is clearly present in recent regulatory developments. There are, however, serious issues with transparency.

First, achieving a balance between regulatory compliance, stakeholder interests and commercially sensitive information may be challenging. Second, transparency encompasses many different issues and aspects, with no one-size-fits-all model. This is because transparency is subjective and depends on existing knowledge, not least the willingness, available time and capacity to process new information and investigate a specific issue.

The transparency of an artifact arguably lies in the context of where it operates. For example, an AI tool used in a medical setting requires different degrees of transparency based on who operates it. Precision medicine software will need to provide a different set of information criteria to a patient as opposed to a medic. The patient is usually not medically trained and likely to be focused on whether it cured or helped with their problem, whereas the medic will need to take a more critical and expert stance, accepting liability for both the raw output and their operation and/or interpretation of the software.

[5] Sandra Wachter and Ben Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI", *Columbia Business Law Review*, No. 2 (2019): p. 494–620, available at: https://doi.org/10.7916/cblr.v2019i2.3424 (last accessed: 2o February 2022).

There could be a technical way to alleviate the first issue (achieving a balance between regulatory compliance, stakeholder interests and commercially sensitive information). That might be through multi-party computation and other cryptographic solutions can be used to share the algorithms in, for example, litigation whilst refraining from sharing it.

The second issue (the varying and subjective nature of transparency) remains a clear obstacle to exercise of an individual right. Namely, how is the individual supported by transparency? Clearly, an AI product is too complex for transparency to be viewed like a list of ingredients on a food label. What is needed, for that transparency to be really meaningful and enable the exercise of a right? This is the key question that we need to deal with; otherwise low quality 'transparency' is going to harm those who need transparency the most as they are at the sharp end of algorithmic discrimination.

Solove suggests adding a public dimension to privacy without eliminating the individual rights angle – the point is that we have to recognize its limits. The risk is that individuals penalized by AI systems could be blamed for not having enquired about the model themselves, which is plainly unfair in the current opaque scenario where these systems have so often been deployed and developed.

A Public Dimension of Privacy

Adding a collective and public dimension to privacy means two things:

First, it means that more efforts have to be placed in ex-ante measures. The Canadian Algorithmic Impact Assessment (AIA) for public sector algorithms is a good example, and so is the recent AIA piloted by the Ada Lovelace Institute for the UK's National Health Service (NHS). Ex-ante measures were once again the champions from a privacy standpoint in two recent rulings. In the first ruling, Uber drivers from the United Kingdom and Portugal asked for access to their personal data and the right to transparency of algorithmic management. The Amsterdam District Court ruled in favour of disclosing some of the personal data used in automated decision-making and profiling of drivers. In the second judgment, the same court ordered Uber to reinstall five drivers dismissed by the company's algorithmic system. It was one of the first cases that used Article 22 of the GDPR, which provides rights of protection against unfair automated decision making.

In both cases the ex-ante assessment of the algorithm was crucial to temper the risks of unfair treatment – in this vein, Frank Pasquale argues that a licensing agency should be set up to ensure only algorithms that have undergone due process

should be allowed to enter the market. The current draft EU AI Act proposes self assessments for high risk AI, except for facial recognition technology (FRT), following the product safety legislation already adopted in the EU through the CE marks.

"A licensure regime for data and the AI it powers would enable citizens to democratically shape data's scope and proper use, rather than resigning ourselves to being increasingly influenced and shaped by forces beyond our control", argues Pasquale.[6]

A new public dimension of privacy demands that we adopt a less static approach to privacy. Privacy as it is enshrined in legislation right now caters for privacy harms as they are now – in a sense, it champions the status quo. But the status quo is untenable in the age of AI and algorithmic decision making. I believe that a formulation of privacy as an ´ideal´ may open the door to sustainable AI. If we can reframe privacy more as the enhancing of personal agency and autonomy and less as merely an individual right to be demanded, then the protection of the data is more clearly a means to safeguard the people behind it and their agency.If this approach works out, we should be able to conceptualise what it means for our personal information to have a true collective value, and what controls, enforcement and limitations we put around such valuable assets. By partly releasing the individual from the responsibility over her/his own privacy and putting the onus back onto the organizations, we would be taking the important first step. With data already being viewed as a commodity, it will clearly be a major battle to bring in a public dimension of privacy, but it is perhaps our best bet if we are to build full public confidence and participation in the benefits of AI.

[6] Frank Pasquale, "Licensure as Data Governance - Moving toward an industrial policy for artificial intelligence", *Knight Columbia*, 28 September 2021, available at: https://knightcolumbia.org/content/licensure-as-data-governance (last accessed: 20 February 2022).