In: Emre Bayamlıoğlu, Irina Baraluic, Liisa Janssens and Mireille Hildebrandt (eds), BEING PROFILED:COGITAS ERGO SUM. 10 Years of Profiling the European Citizen, 2018: Amsterdam University Press, 72-75. DOI 10.5117/9789463722124/CH12.

On the presumption of innocence in data-driven government. Are we asking the right question?

Linnet Taylor[1]*

Abstract

The presumption of innocence is a principle of fundamental importance to the rule of law, but one of limited use if we wish to protect people from unfairness in data-driven government. This is due to the growth in complexity of the field of indirect profiling – the practice whereby profiles are created to sort individuals into groups based on particular characteristics. This contribution argues that the use of complex algorithmic analytics, combined with the long commercial value chain of the data used for profiling, make the presumption of innocence irrelevant, as by the time effects on individuals occur, they are no longer traceable to particular moments of data collection or sorting.

Keywords: Algorithms, data value chains, predictive policing, migration, transparency

Introduction

This provocation will argue that the presumption of innocence is a principle of fundamental importance to the rule of law, but that it is of limited use if we wish to protect people from unfairness in data-driven government. As identified by Jacquet-Chiffelle (2008) in Profiling the European Citizen, indirect profiling (assuming, based on data analytics, that an individual fits a particular group profile) was a practice that presented challenges to privacy, autonomy and fairness in 2008. This practice has increased exponentially with the addition of a myriad new data sources, becoming more entrepreneurial (Pasquale 2015) with ubiquitous sensing and distributed data governance. In response, we need new, broader framings of our rights in relation to data profiling. We can no longer assume that the most important data harms relate to individual data subjects as potential rights claimants, and stem from targeted governmental data processing. If we do this, we are effectively searching for our keys under the lamppost, where the light falls.

(Re)defining the question

The presumption of innocence is a key principle that allows us to contest governmental practices of data processing and profiling. Is it all we need to consider, however, given ubiquitous and continual data collection on our behaviour and movements? Or do we need, as well as principles to ensure just treatment of citizens by states, principles to ensure the just treatment of anyone, by anyone with the power to collect and process data? I will use two (semi)hypothetical cases to support my contention, both of which raise questions as to whether the liberal individual framing of rights in relation to data processing is sufficient to help with the challenges we are now facing (Cohen 2019).

In order to discover whether the question the presumption of innocence answers is actually the question that faces us, we should begin from the contemporary landscape of data collection. The proliferation of sensors and the growth in sensing technologies mean that today the majority of digital signals used in profiling come not from individuals engaging consciously with authorities or firms, but from our contact with environments and devices that sense our actions and behaviour.

Under these conditions the presumption of innocence may not be the most useful route to justice: profiling practices that use data collected from environmental sensing, or behavioural and location traces, has a more complex relationship to suspicion or innocence than classic forms of 'volunteered' data such as administrative data gathered by public authorities. Traditionally governmental institutions involved in profiling have identified particular individuals as potential targets based on their membership of a category of interest, resulting in a process of 'blacklisting', 'greenlisting' or 'greylisting' (Broeders and Hampshire 2013). In this case, it is relevant to cite the presumption of innocence as a counter to the clear harm of blacklisting. However, we see processes emerging today on an entrepreneurial basis which instead of starting from established suspect categories (such as people who have downloaded particular documents or belong to particular online groups), mine general data in order to discover anomalies that may relate to suspicious behaviour. The act of focusing on individuals within those categories is only remotely connected to this discovery process, and may not be part of the process at all. The following examples will help to explain this claim.

Two illustrative cases

Case 1: A private-sector consultant to the EU's Space Agency ESA aims to track the paths of undocumented migrants into Europe. The project leaders use various data sources including satellite images of human mobility through North Africa, social media output, local online reports and migrants' mobile calling records as they travel through the desert. The datasets are combined and fed into a machine learning process designed to guess at migrants' place of origin, and thus their likely type of claim to asylum once they make contact with migration authorities. The consultants then sell their consulting services to various of those authorities, and as contractors, use it to determine where to look for migrants who are outliers in terms of successful asylum claims – those from more peaceful or democratic countries – who are predicted to be 'safe' to turn around and send directly home. At no point are migrants targeted as individuals by authorities as a result of the analysis – it is one of several streaming information sources available to various authorities, who make decisions about groups, based on profiles. The system can also identify migrant groups who, if prevented from claiming asylum, would lead to a high-profile human rights problem, and they can be escorted to a place where they can make their claims. It is important to note that this logic is problematic not only because of the right to claim asylum, but also because place of origin is not a valid indicator for the basis of asylum claims.

Case 2: Aminata, a young woman from West Africa, is on a one-day visit to a European city. She stops for a drink on her way through a living lab: an area of semi-public space where the right to surveil the street is awarded by the municipality to any corporation wishing to test its products or services on the public (one example is Stratumseind in the Dutch city of Eindhoven). As Aminata walks down the street, smart lampposts collect data on the way she is moving, her facial expression, skin colour and clothing, the signals her phone is picking up from the nearby antennae and the signals it is sending out to identify itself to those antennae and to local wi-fi points. Aminata is on her way to the airport, without any plans to return to Europe.

Unbeknownst to her, however, a fight has broken out in one of the bars as she passed by. All the data on people in the area at the time is later mined by the company running the living lab, and Aminata shows up as an anomaly in the dataset: her face, skin colour and her phone plan's origin are outliers. The following year this analysis is added to a hundred others by the next company using the living lab. It sells its data on to a national firm, which uses it to train a model designed to algorithmically identify risks to public order in the urban environment. This model is marketed as a service to any organisation interested in this task, including consultants to the police.

Aminata's data are in the model, but by now they only come into play in combination with the data of others, and under certain conditions – particular questions relating to types of incident or urban environment – in a process which would not be transparent to the firm running the model. Where 'N=all incidents and people present' no outlier is excluded, and due to a coincidental mix of conditions, people with some of Aminata's characteristics become flagged by the model as related to violence. This influences municipal and law enforcement policy towards African migrants negatively in various ways, but is never made explicit in policy or guidelines.

Both these cases demonstrate ways in which data mining is used to create profiles, but where models built on large and diverse datasets to create 'evidence' in ways that are opaque to the user. When data is aggregated and sold by one user to another, it becomes impossible to check its original meaning. Yet completeness often becomes a synonym for reliability: a dataset reflecting all the violent incidents in a street, or all the migrants passing through North Africa, is likely to be seen as more reliable than one showing just a few, or one that disaggregates individual event data to understand more about causation. Aggregation facilitates decision-making at the same time as concealing meaning. Furthermore, though, the individual is neither identifiable nor individually analytically important in the dataset. It is their characteristics in relation to the larger group that provide the means for prediction (for more on this, see Taylor, Floridi, & van der Sloot 2017). It is also in relation to these generalisations (based on 'types, not tokens', Floridi 2014) that decision-making is done. Increasingly, when we are affected by data-driven governance it is not because of our own data but because of others', which has travelled amongst users and through models entirely within the private sector. The question of presumption of innocence becomes less relevant in the more vague, diffuse practice of risk prediction, based on data whose origin can no longer be traced, and which has never been attached to a single identity?

What exactly, then, is being challenged by such profiling? It may be best phrased as the right to resist inclusion in the database – any database. This is not a right data protection can address: instead it relates to privacy, and is fundamentally a political question. I should be able to choose how components of my identity are used by others, and to resist their arbitrary inclusion in processes that involve exerting power over anyone's options and behaviour. Although framed as individual rights, in this case privacy and autonomy must extend beyond the individual and also become conceptualised in relation to all of us at once – the people in this street, the people in that region of the desert. In cases such as these the need to exert our rights materialises in relation to the final destination and purpose of data about us, but cannot be predicted at the moment the data is collected. The mobile network operator, the living lab's temporary director, or the social media company cannot predict how the data they provide will be used. Conversely, the state (if it is involved) becomes less likely to know the reliability or origin of the data it is using in relation to a particular problem, or the way in which its processing affects its ability to answer the question.

Combating invisible harms

It is salutary to remember that Edward Snowden made his revelations about government surveillance while working for the private consulting firm Booz Allen Hamilton, which was providing commercial consulting services to the US government. Increasingly, problems for which governments are answerable will have many invisible authors against whom we have few enforceable rights.

I have argued that where profiling is an entrepreneurial service and risk assessment and pre-emption the aim, the presumption of innocence becomes relevant at the end of a long line of actions. The single, identifiable subject, the single identifiable watcher and the auditable data supply chain that ends with a governmental actor are increasingly a fiction. Instead we are seeing the emergence of an entrepreneurial free-for-all which conceals data's origins, paths, purposes and reliability. In relation to this, we will need human rights that can be claimed against any data collector, that are pre-emptive and that are powerfully enforced by government. Given the billions generated by this growing market for data, however, a remedy seems as far away as it did when Hidebrandt and Gutwirth published their volume in 2008.

Notes

* Linnet Taylor is Assistant Professor of Data Ethics, Law and Policy at the Tilburg Institute for Law, Technology, and Society (TILT).

[1] This research has received funding from the European Research Council under the European Union's Horizon 2020 Programme / ERC Grant Agreement n. [757247]

References

Broeders, Dennis, and James Hampshire. 2013. "Dreaming of Seamless Borders: ICTs and the Pre-Emptive Governance of Mobility in Europe." Journal of Ethnic and Migration Studies 39(8): 1201–18. doi: /10.1080/1369183X.2013.787512.

Cohen, Julie E. 2019. "Turning Privacy Inside Out." Theoretical Inquiries in Law 20(1): 8–36.

Economist. 2018. "Does China's Digital Police State Have Echoes in the West?" The Economist, May 31, 2018. https://www.economist.com/leaders/2018/05/31/does-chinas-digital-police-state-have-echoes-in-the-west.

Floridi, Luciano. 2014. "Open Data, Data Protection, and Group Privacy." Philosophy & Technology 27(1): 1–3. https://doi.org/10.1007/s13347-014-0157-8.

Jaquet-Chiffelle, David-Olivier. 2008. "Reply: Direct and Indirect Profiling in the Light of Virtual Persons. To: Defining Profiling: A New Type of Knowledge?" In Profiling the European Citizen, edited by Mireille Hildebrandt and Serge Gutwirth, 17–45. Dordrecht: Springer.

Pasquale, Frank. 2015. The Black Box Society. Cambridge, MA: Harvard University Press.

Taylor, Linnet, Luciano Floridi, and Bart van der Sloot, eds. 2017. Group Privacy: New Challenges of Data Technologies. Dordrecht: Springe.