eLaw
Working Paper Series

No 2018/001 - ELAW– 24 April 2019

Profiling as Inferred Data

Amplifier Effects and Positive Feedback loops

Bart Custers

Universiteit
Leiden
eLaw

Profiling as inferred data. Amplifier effects and positive feedback loops

*Bart Custers**

Abstract

Extracting profiles and other hidden knowledge from large amounts of data via techniques like data mining and machine learning is often regarded as an input-output process in which knowledge (i.e., profiles) are extracted from raw data. In this provocation, a different perspective is taken, in which profiles are not regarded as knowledge, but rather as (new) data, namely as inferred data. Using this perspective, it is shown that profiles are not only an end result or an end product, but can also be reused as ingredients for further data analytics. However, in this way, profiling processes may function as amplifiers, amplifying bias and inaccuracies via positive feedback loops, that further entrench consequences for data subjects.

Effects of small disturbances (like incorrect or incomplete data, or flaws in the data analysis) may lead to an increase of the magnitude of perturbations. Obviously, this may have some serious consequences for data subjects. Profiling based on datasets from data brokers that contain large amounts of inferred data, may propagate any existing biased patterns, leading, for instance, to disparate impact. The reuse of inferred data may also lead to self-fulfilling prophecies – a phenomenon well-known in profiling. In case of inferred data, however, the effect might be much stronger: because of the self-reinforcing effect, patterns may be amplified and become much more entrenched. These effects may amplify inequality, undermine democracy and further push people into categories that are hard to break out.

From a legal perspective, under the EU General Data Protection Regulation (GDPR) inferred data may or may not be personal data. If so, people have a right to access the inferred data and to receive meaningful information about the logic involved in the data analytics. However, since data subjects have no right to access the algorithms and data of other data subject used in the analyses, it is impossible for them to check whether data is inferred correctly.

Keywords: profiling, inferred data, data mining, GDPR, algorithms

Introduction

In the data economy, many companies try to gain a competitive edge by extracting profiles and other hidden knowledge from large amounts of data via data mining and machine learning (Custers and Bachlechner 2018). This can be seen as an input-output process, in which knowledge (i.e., profiles) is extracted from raw data (Fayyad et al. 1996). Many kinds of data are used as ‘ingredients’, but often the analysis (i.e., ‘the recipe’) is supposed to remain confidential, as it may constitute the core business secrets of companies. Also the outcomes, i.e., the resulting profiles or extracted knowledge (such as new target groups or risk assessments), are often supposed to remain confidential, as it may be valuable commercial information for companies.

Profiles extracted from large datasets are often regarded as useful knowledge for subsequent decision-making and micro-targeting (Hildebrandt and Gutwirth 2008; Zarsky 2003). In this provocation, a different perspective is taken, in which profiles are not regarded as knowledge, but rather as (new) data, namely as inferred data. Using this perspective, it is shown that profiles are not only an end result or an end product, but can also be reused as ingredients for further data analytics. In this way, profiling processes may function as amplifiers, amplifying bias and inaccuracies via positive feedback loops, that further entrench consequences for data subjects.

Profiling: ascribing inferred data to people

Personal data is the basis of each process of profiling people, either as individuals or as groups (Custers 2013). After data is collected, it is analysed, usually in automated ways, using tools like data mining and machine learning. The data used for input is gathered in different ways: large volumes of data are generated by people themselves (e.g., via social media) as well as by technology, including sensors (e.g., cameras, microphones), trackers (e.g., RFID tags, web surfing behaviour) and other devices (e.g., mobile phones, wearables for self-surveillance/quantified self). In this way, profiles can be inferred from all kinds of data, including behavioural biometric data (Yannopoulos et al. 2008), location data (Fritsch 2008) or anonymised data (Schreurs et al. 2008).

Basic profiling techniques like regression, classification or clustering essentially ascribe attributes to people. This means that new attributes are inferred from available attributes, either from the same person or from other persons. These inferences may be precise (e.g., inferring age from the data of birth) or estimates (e.g., inferring intelligence or happiness from Facebook likes) (Kosinski et al. 2012). In this way, attributes a data subject does not want to disclose or attributes a data subject does not know can be predicted via data analytics and ascribed to that person. The key characteristic of inferred data is that it is data inferred from other data and not data directly or indirectly provided by data subjects.

Depending on factors like the total population, existing privacy laws and maturity of the data economy, it may differ from country to country in how many databases people are represented. In the EU it is reasonable to assume that people have their personal data in several hundreds or even several thousands of databases. Usually people are not aware of this and neither are they aware which data it concerns, for which purposes the data are processed, and how any resulting profiles may lead to decisions about them (Eurobarometer 2015). Many of these data have not been obtained directly from the data subjects, but are data obtained via data sharing and data reuse, sometimes via so-called data brokers as intermediaries (Custers and Ursic 2016).

Reusing inferred data: positive feedback loops

The reuse of inferred data may have advantages. Inferring data can be a tool to fill gaps in incomplete datasets or check the correctness of available data by matching inferred data with the contested data. In this way, datasets enriched with many inferred attributes are likely to have higher levels of completeness and accuracy. In big data analytics, completeness and correctness of data is not a strict condition, but obviously may contribute to getting more accurate and reliable results.

At the same time, reusing inferred data as input for data analytics, particularly profiling processes, may turn profiling processes into amplifiers with positive (i.e., self-reinforcing) feedback loops. Effects of small disturbances (like incorrect or incomplete data, or flaws in the data analysis) may lead to an increase of the magnitude of perturbations. Obviously, this may have some serious consequences for data subjects. Profiling based on datasets from data brokers that contain large amounts of inferred data, may propagate any existing biased patterns, leading to disparate impact (Barocas and Selbst 2016). For instance, for profiling insurance premiums, a dataset with income data (directly obtained from data subjects) is less valuable than a dataset further enriched by the data broker with credit scores (inferred data). However, the credit scores may already be based on the income data, which means the insurance premium profiles are influenced twice by the original income data: directly and indirectly via the inferred credit scores. The reuse of inferred data may thus lead to self-fulfilling prophecies – a phenomenon well-known in profiling (Custers 2013). In case of inferred data, however, the effect might be much stronger: because of the self-reinforcing effect, patterns may be amplified and become much more entrenched. These effects may amplify inequality, undermine democracy and further push people into categories that are hard to break out (O'Neil 2016).

Inferred data under the GDPR

The GDPR provides data subjects with an extensive number of data subject rights, like rights to information, access, erasure and more. With regard to profiling, most of these rights seem to focus on the input data. The term inferred data occurs nowhere in the text of the GDPR, which clearly focuses on (personal) data, not on knowledge. A few rights, such as the right to object to profiling under certain conditions (Art. 21) and the right not to be subjected to automated individual decision-making (Art. 22) relate to the profiling process.

Data controllers should inform data subjects (upon request) about the existence of profiling processes and provide meaningful information about the logic involved and its consequences for the data subject (Art. 13.2f, 14.2g, and 15.1h). There is an extensive debate on how far this 'right to explanation' actually extends (Wachter et al. 2017; Veale and Edwards 2018; Selbst and Powles 2017; Kaminski 2018). However, few argue that there is an obligation for data controllers to disclose (1) the actual algorithms used, (2) the actual weighting of the data subject's data, and (3) data of other data subjects used in the profiling. Without such information, it is impossible for data subjects to check whether data is inferred correctly.

Companies may not be very keen to share algorithms and profiles as these can be considered trade secrets of vital interest, constituting their competitive edge. These companies may also suggest that profiles are corporate secrets because they may, via reverse engineering, enable disclosure of their analyses and software (Hildebrandt 2011, 23).

If inferred data is ascribed to groups or categories, it may not be personal data. However, in micro-targeting inferred data will often be ascribed to an identified or identifiable natural person, yielding personal data. If inferred data is personal data, there may still be practical issues with data subject rights. For instance, the right to rectification requires that data subjects show that the data are wrong. Proving that inferred data are wrong, is impossible for data subjects without access to analysis tools and the data of other data subjects used in the analysis. Obviously data subjects may object to the profiling altogether, but this may be too rigorous.

Data subjects may also consider transferring their data to other data controllers that provide more transparency on their profiling processes. This can be done via the right to data portability, prescribing that a data subject has the right to receive the personal data concerning him or her in a structured, commonly used and machine-readable format. However, this right does not include inferred data, as it is limited to only personal data which he or she has provided to a controller. This includes observed data, but not inferred or derived data (WP29

2016). In fact, a data controller may further limit the right to data portability by inferring data while deleting the original data on which the inferences are based, even if this is done in reversible ways (Madge 2017).

Wrap-up

Profiles are usually considered as knowledge extracted from data, but they can also be considered as (inferred) data that can be used as input for other profiling processes. Reuse of inferred data may contribute to improving the completeness and correctness of datasets. However, the reuse of inferred data may also turn profiling processes into amplifiers with positive (i.e., self-reinforcing) feedback loops. This may lead to propagation of existing biases in datasets and resulting patterns, amplifying inequalities and other issues related of profiling even stronger than in regular profiling practices. Looking at the GDPR, inferred data may or may not be personal data. If so, people have a right to access the inferred data and to receive meaningful information about the logic involved in the data analytics. However, since data subjects have no right to access the algorithms and data of other data subject used in the analyses, it is impossible for them to check whether data is inferred correctly.

***** Bart Custers, PhD MSc LLM, is associate professor and director of research at eLaw, the Center for Law and Digital Technologies at Leiden University.

References

Barocas, Solon, and Andrew Selbst. 2016. “Big Data's Disparate Impact” California Law Review 104(3): 671–732.

Custers, Bart. 2013. “Data Dilemmas in the Information Society.” In Discrimination and Privacy in the Information Society, edited by Bart Custers, Toon Calders, Bart Schermer, and Tal Zarsky, 3-26. Heidelberg: Springer.

Custers, Bart, and Helena Ursic. 2016. “Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection.” International Data Privacy Law 6(1): 4-15.

Custers, Bart, and Daniel Bachlechner. 2018. “Advancing the EU Data Economy: Conditions for Realizing the Full Potential of Data Reuse” Information Polity 22(4): 291-309.

Eurobarometer Survey 431. 2015. Attitudes on Data Protection and Electronic Identity in the European Union. Brussels, June 2015.

Fayyad, Usama, Gregory Piatetsky-Shapiro, and Padhraic Smyth. 1996. “The KDD Process for Extracting Useful Knowledge from Volumes of Data”, Communications of the ACM, 39(11): 27-34.

Hildebrandt, Mireille, and Serge Gutwirth, eds. 2008. Profiling the European Citizen: Cross-Disciplinary Perspectives. Dordrecht: Springer.

Hildebrandt, Mireille. 2011. “The Rule of Law in Cyberspace?” Inaugural Lecture, Nijmegen, Radboud University. https://works.bepress.com/mireille_hildebrandt/48/

Kosinski, Michal, David Stillwell, and Thore Graepel. 2012. “Private Traits and Attributes are Predictable from Digital Records of Human Behaviour.” Proceedings of the National Academy of Sciences USA 110: 5802–5.

Fritsch, Lothar. 2008. “Profiling and Location-Based Services.” In Profiling the European Citizen, edited by Mireille Hildebrandt and Serge Gutwirth, 147-68. Dordrecht: Springer.

Kaminski, Margot. 2018. “The Right to Explanation, Explained.” University of Colorado Legal Studies Research Paper No: 18-24.

Madge, Robert. 2017. “Five loopholes in the GDPR” My Data Journal, August 27, 2017. https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b.

O’Neil, Cathy. 2016. Weapons of Math Destruction; How big data increases inequality and threatens democracy. New York: Crown.

Schreurs, Wim, Mireille Hildebrandt, Els Kindt, and Michaël Vanfleteren. 2008. “*Cogitas, Ergo Sum.* The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector.” In Profiling the European Citizen: Cross-disciplinary Perspectives, edited by Mireille Hildebrandt and Serge Gutwirth, 241-64. Dordrecht: Springer.

Selbst, Andrew and Julia Powles, 2017. “Meaningful Information and the Right to Explanation.” International Data Privacy Law 7(4): 233-42.

Veale, Michael, and Lilian Edwards. 2018. “Clarity, Surprises, and Further Questions to in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling” Computer Law & Security Review, 34(2):398-404.

Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. 2017. “Why a Right to Explanation of Automated Decision-Making Does not Exist in the General Data Protection Regulation.” International Data Privacy Law 7(2): 76-99.

WP29. 2016. Guidelines on the right to data portability, Article 29 Data Protection Working Party. 242. Brussels.

Yannopoulos, Angelos, Vassiliki Andronikou, and Theodora Varvarigou. 2008. “Behavioural Biometric Profiling and Ambient Intelligence.” In Profiling the European Citizen: Cross-disciplinary Perspectives, edited by Mireille Hildebrandt and Serge Gutwirth, 89-110. Dordrecht: Springer.

Zarsky, Tal. 2003. “Mine Your Own Business! Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion.” Yale Journal of Law and Technology 5(1): 1-5.