Pervasive Data Profiling, Moral equality and Civic Responsibility

Sylvie Delacroix

UCL Laws and UCL Computer Science

s.delacroix@ucl.ac.uk

Abstract

So far neither regulatory frameworks nor endeavours to develop bottom-up approaches to data protection have had much success in mitigating the moral hazard inherent in pervasive use of seemingly innocuous, "leaked data". This paper focuses on two aspects of those risks that are too rarely discussed. They relate to the possibility of civic responsibility (1) and moral equality (2).

(1) Ethical agency (and the responsibility it entails) presupposes the possibility of change: when our practices are wanting, someone needs to be able to stand up and question them. Change, in turn, presupposes the ability to break from habitual frames of thought. To what extent is the profile-based tailoring of the environmental architecture that shapes our choices and attitudes hampering the possibility of civic responsibility? The question at stake here is different from the better-known "right to be forgotten" issue: the latter focuses on the impact of recorded data on others' perception of oneself. This paper, by contrast, focuses on what may be called the "anchoring effect": the impact of recorded data on our ability to see the world -and, most importantly, our role in it- differently. The ability to acknowledge a discrepancy between one's present ethical stand and the person one seeks to be is essential to making sense of any notion of civic responsibility. The danger is that such discrepancy will simply cease to arise in an environment that has been systematically "optimized" in accordance to one's profile.

(2) The second section of this paper explores the extent to which ubiquitous, proactive computing gives rise to a very particular type of vulnerability, one that potentially threatens the moral equality of data-subjects. This vulnerability cannot be addressed by correcting epistemic imbalances. The current regulatory focus on information disclosure has obscured what mere disclosure cannot achieve: *empowering data-subjects to maintain and develop their sense of self*. This may sound overly ambitious. I argue that it is no more so than a commitment to retain a meaningful, practice-relevant concept of *civic* responsibility.

Imagine a seemingly ideal scenario, whereby policy-makers and software engineers have managed to collaborate in such a way as to seamlessly integrate both privacy concerns and transparency imperatives within the ongoing deployment of "smart" applications. The latter are designed to simplify or replace altogether our practical reasoning in both mundane (food choices, task prioritisation) and specialised contexts (professional applications):

"It's the end of a successful day for Ben: he's contributed to fine-tuning a `virtual GP app' which has today been approved for nationwide deployment: millions of patients will now be able to "consult" a virtual GP as and when needed, thus simultaneously increasing accessibility and cutting costs while delivering more reliable and accurate services. Ben is sitting in the tube taking him home –it's packed, but he's glad his commuting app recommended he leave his bike at work, as a large demonstration is taking place on his way home - something to do with euthanasia legislation. His "PA bot" interrupts his reading about it as a message comes in notifying Ben that he has not been selected for the job he applied for last week. Ben taps on the feedback button. In it he finds an ordered list of all the parameters taken into account. His PA is busy correlating those parameters to all the data that is likely to have been fed into the automated hiring system. His PA system flags up an anger management course which Ben recently attended in the context of his current job. Although his course registration itself was confidential, Ben had chosen to discuss this course, and the value of anger as a moral emotion, in one of his blogs (while Ben had de-activated his PA). Anticipating Ben's volatile emotional state, the PA bot starts Ben's favourite "gym playlist", which prompts Ben to leave the tube one stop earlier, for a detour via the gym (which means he will miss his kids' bedtime routine). The PA also messages several of Ben's friends who are scheduled to be around and silences several of his wife's increasingly irritated messages while planning for a bunch of flowers to be delivered to her in a couple of hours."

The above scenario is not science-fiction. True, we don't have virtual GPs yet –only video app consultations, with real GPs (if the instrumental logic that currently presides over fast growing professional automation has its way, it's only a matter of time). While travel optimisation apps are already with us, "PA bots" are on their way. All the applications deployed in the proposed scenario come with substantial privacy challenges.

Now let's imagine that, somehow, the infrastructure that is in place is robust enough to make sure that both the collection and processing of data (whether it is deemed "personal" or not) is transparent to all in its process, while its content remains rigorously opaque outside the applications it is meant for. Whether one considers the data collected (and relied on) during virtual GP consultations, or the data that enables Tom's PA to anticipate his desires or preferences, the assumption is that this data is both collected and processed in a transparent and accountable way. The algorithms that allow Tom's PA to infer future desires (and behaviour) from patterns identified in real time within his machine-readable behaviour are publicly accessible, as are those that preside over virtual GP consultations. Any form of data collection must be consented to, with adequate, individual guidance on both short and long-term implications. Imagine, in short, that the information asymmetry between data-controllers and data-subjects is successfully controlled and mitigated. Enlightened collaborative efforts between public policy makers and software engineers mean that a series of safeguards are constantly in the process of being built into the data processing algorithms, which are subject to regular checks and assessments (and can be audited by members of the public at any time).

As desirable as it may be, the above scenario is only apt to address (and remedy) one particular form of vulnerability: that which derives from *epistemic* inequality. Given the extent to which the deployment of smart technologies cannot but massively amplify the impact of pre-existing epistemic inequalities, it is both unsurprising and necessary that one should seek to address newly created knowledge asymmetries. If the latter were amplified tenfold by the advent of the script, they are probably magnified a thousand-fold by the advent of ubiquitous computing (Weiser, 1995). Yet the danger is to let this -laudable- concern for epistemic equality obscure other forms of equality, which are less visibly endangered by the deployment of smart technologies in our quotidian lives.

The second section of this paper explores the extent to which ubiquitous, proactive computing gives rise to a very particular type of vulnerability, one that potentially threatens the moral equality of data-subjects. This vulnerability cannot be addressed by correcting epistemic imbalances. The current regulatory focus on information disclosure has obscured what mere disclosure cannot achieve: *empowering data-subjects to maintain and develop their sense of self*. This may sound overly ambitious. I argue that it is no more so than a commitment to retain a meaningful, practice-relevant concept of *civic* responsibility.

Civic responsibility presupposes an ability to acknowledge a discrepancy between one's present ethical stand and the person one seeks to be. The danger is that such discrepancy

will simply cease to arise in an environment that has been systematically "optimized" in accordance to one's profile. The first section addresses the challenges raised by what I call the "anchoring effect": the impact of recorded data on our ability to see the world -and, most importantly, our role in it- differently.

1. Personalised profiling and Civic Responsibility

1.1. Inferring future attitudes from our machine-readable past: a self-fulfilling prophecy?

We have all learned to "profile" from a young age. Based on the past attitude or behavior of people with certain characteristics, we tend to expect people with those characteristics to behave in a certain way. Our expectations are often confounded: the "data sample" we base those expectations on are usually tiny, and most of us tend to be rather bad statisticians. That's not only because we are susceptible to all sorts of heuristic biases. We are also prone to getting mixed up and treating rumors and apprehensions as if they were behavioral facts.

Machines fare better. Increasingly sophisticated data collection technologies mean that machines can now "read" many aspects of the quotidian lives of a rapidly growing number of people. Combined with fast evolving data mining techniques, these large, expanding datasets allow for the discovery of statistically robust correlations between particular human traits, attitudes and behaviours. The tactical advantages -and considerable dangers- that stem from being able to leverage this newly generated knowledge for commercial or political purposes have been amply demonstrated this past year.

My concern is with a different kind of peril. It is harder to pinpoint as its effects are slower to manifest themselves, and when they do it will be much too late for any democracy to be worthy of the name. This peril stems from the nascent, but fast developing art of harvesting "live" personal data to personalize digital services in real time. Far from being confined to recorded online behavior (or commercial / lifestyle preferences), this "live" personal data will include physiological indicators of nascent emotions. Combined with increasingly sophisticated

profiles, the latter will enable smart applications to mold our perceived environment (and its offerings) to our anticipated desires and attitudes. This has dramatic consequences for ethical agency and the possibility of civic responsibility.

1.2. Civic Responsibility and the possibility of moral change in an "onlife world"

To make sense of ethical agency (and its concomitant responsibility) in a low-tech, "offline" world is hard enough. One of the key challenges for moral philosophy is indeed to explain what conditions our ability to take a moral stand against the usual or socially accepted. We now have ample empirical evidence suggesting that our ethical sensitivity (our ability to see how the world could be made better) is enabled by the habits of thought and action that we've acquired in the process of growing up. If ethical judgment is thoroughly culturally conditioned, where does anybody find the momentum necessary to standing back and questioning potentially abhorrent practices?

The above question takes a dramatic turn -since acquired habits of evaluation are even more likely to "stick"- when raised in the context of a hypothetical "ambient intelligence environment", which is best described by (Hildebrandt & Koops, 2010):

> "Ambient Intelligence is based on proactive computing meant to adapt your environment to your preferences before you become aware of them. It organises your life at a subliminal level by seamlessly catering to your needs and desires and thus providing you with personalised opportunities based on a calculated anticipation of what you would have preferred had you known what the smart environment 'knows'".

While the real-time, calculated adaptation of our environment on the basis of what our profile suggests would best fit our upcoming preferences may be appealing in its comforting efficiency, it is also morally hazardous. Why? Because all will agree that, at some point or another, our ability to stand back and question commonly accepted practices requires some kind of trigger. The dawning awareness of an irresolvable discrepancy between the person one seeks to be and socially conditioned habits of evaluation requires precisely the kind of "friction" which any seamless, profile-based optimisation of our environment is unlikely to tolerate.

1.3. "Counter profiling" confrontations?

In keeping with the current focus on epistemic vulnerability when it comes to data protection and the implication of profiling practices, many emphasize the need to equip each data subject with an understanding of how her behavior may be interpreted by "ambient" algorithms. Along this line, (Hildebrandt & Koops, 2010) for instance call for:

> "autonomic profiling […] to be designed in such a way that it affords reasonably accurate anticipations of how a person is being and will be profiled. These anticipations must be as smooth, seamless, and subliminal as the smart environment itself, thus requiring novel types of human machine-interfaces that warn a person how her behaviour may be interpreted by the smart infrastructure".

This paper emphasizes the need to see beyond epistemic vulnerability, and take into account the impact of profiling practices upon the possibility of civic responsibility. Alerting the data subject to the profiling implications of her behavior is important, but it is unlikely to foster the openness to being called into question often required for the processes leading to moral change: "engineered encounters" with significantly different others, on the other hand, might. Designed so as to confront us with markedly different worldviews or lifestyles, such engineered encounters would leverage the knowledge inherent in profiling practices but reverse their purpose. For when it comes to awakening us from deeply entrenched habits, "mere" words are no match for the kind of encounter described in radical terms by Levinas[1] when he refers to the "face of the Other" summoning each and every one of us. These encounters may be engineered through seemingly "random" encounters or they may be fabricated all the way through: fully immersive virtual environments are starting to be used for ethics training precisely because of their ability to mobilise "primitive", emotional responses that do not necessarily come live in the nitty-gritty of our personal or professional lives.

2. Proactive computing and moral equality

It is relatively easy to see how existing knowledge asymmetries may be exacerbated in an environment that relies on systematic, personalised profiling to optimise our environment to our upcoming preferences. To claim that, beyond epistemic inequality, it is our commitment to *moral* equality that is most problematically imperilled by these emerging, "smart enviornments" may sound far-fetched.

2.1. When epistemic inequality morphs into moral inequality

> "What infringes our privacy is that emotional states, which are mostly unconscious, may be picked up by our environment before we become aware of them. 'They' may thus 'read' our emotions before we have a chance to develop our own reflection and response to our own emotional state. This is decisive, because researchers like Damasio have shown a crucial the difference between feelings and emotions. Feelings emerge when humans become aware of their emotions. Feelings allow for and thrive on conscious attention to and reflection on one's emotional responses. They enable us to develop a personality that is not entirely intuitive, not completely dependent on whatever emotion overwhelms us. Feelings integrate awareness, deliberation and interior monologue on our emotional habits. They thus enable us to grow and mature into the kind of person we want to be." (Hildebrandt, 2015)

In the above quote, that which ultimately "enable[s] us to grow and mature into the kind of person we want to be" is understood as falling under the umbrella of (widely defined) privacy concerns. This characterisation may well obscure the distinctiveness of what is at stake, which cannot be addressed by remedying epistemic imbalances, for in that scenario epistemic inequality effectively morphs into moral inequality. How so? Sangiovanni brilliantly articulates the conceptual link between the exploitation of another's vulnerability and moral (in)equality via the notion of social cruelty. What makes it wrong to treat others as inferiors *in a way that violates our equal status*[2] is not some mysterious "value-bestowing capacity possessed to an equal extent by each one of us" (such as dignity) but rather a rejection of social cruelty. The latter is

---

[1] "The relation with the Other, or Conversation, is […] an ethical relation; but inasmuch as it is welcomed this conversation is a teaching. Teaching is not reducible to maieutics; it comes from the exterior and brings me more than I contain. In its non-violent transitivity the very epiphany of the face is produced." (Levinas, 1969, p. 51)

[2] Clearly it is not the case that all forms of treating others as inferiors are wrong: social relationships are structured by all sorts of hierarchies that make it acceptable, or even expected, for someone to treat another as inferior. Some cases of treating another as inferior are wrong "merely" because they are unfair. Others are wrong in a more fundamental way. Sangiovanni argues that, instead of traditional (whether Christian or Kantian) references to dignity, a rejection of social cruelty does a better job at explaining our commitment to moral equality.

defined as "the unauthorized, harmful and wrongful use of another's vulnerability to attack or obliterate their capacity to develop and maintain an integral sense of self" (Sangiovanni, 2017, p. 76).

2.2. Personalised profiling and opacity respect

Whether it be through stigmatisation or instrumentalisation, the seamless adaptation of our environment on the basis of our past, machine-readable behaviour provides fertile ground for inferiorising treatment that is wrong not because it violates some norm of fairness but rather because it threatens our unique ability to develop and maintain a sense of self. The latter is in part dependent upon the possibility of preserving a gap between the self that we present to the world and the self that we conceal. Maintaining such opacity is key to all sorts of role-based social practices. It is also what protects us against various forms of social cruelty: "the most systematic forms of social cruelty aim at breaking our sense of ourselves as self-presenting" (Sangiovanni, 2017, p. 83). The latter sense requires at least partial control over what is "inner" and what is "outer". In the "ambient intelligence" environment described earlier, such control is at best illusory.

One may seek to address the above concerns by engineering ways of actively seeking genuine and ongoing consent to pervasive, personalised profiling. One may argue that there is no fundamental, qualitative difference between such profiling practices and the way some of us are happy to relinquish some of our personal data in order to reap the benefits of time-saving (or entertaining) applications. If this line of argument is correct, and if the vulnerabilities at stake are indeed of the same kind, then the current regulatory focus on epistemic imbalances (whether it be through imposing transparency or explanatory constraints) is right: what matters is to find ways of actualising "genuine" and "ongoing" consent. Yet if, beyond the all too visible epistemic inequalities, it is our very ability to maintain and develop a sense of self that is called into question by the proactive computing described earlier, then the regulatory fixation with epistemic imbalances is wholly inadequate. In that case it is high time engineers and policy-makers start to grapple with what it means to be committed to *moral* equality.

Acknowledgements

References

Hildebrandt, M. (2015). *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology*: Elgar.

Hildebrandt, M., & Koops, B.-J. (2010). The Challenges of Ambient Law and Legal Protection in the Profiling Era. *The Modern Law Review, 73*(3), 428-460. doi:10.1111/j.1468-2230.2010.00806.x

Levinas, E. (1969). *Totality and infinity: an essay on exteriority* (A. Lingis, Trans.): Duquesne University Press.

Sangiovanni, A. (2017). *Humanity without Dignity: Moral equality, respect and human rights*. Cambridge, MA: Havard University Press.

Weiser, M. (1995). The computer for the 21st century. *Scientific American, 272*(3), 78-89.