Interview with Isabelle Moeller:

Ubiquitous and Positive Biometrics

Abstract:

In this interview with Isabelle Moeller questions surrounding the responsible use and development of biometric apps are explored. The use of biometrics - originally to digitally represent and authenticate an identifiable characteristic of a product or a person - have become so wide spread that they are capable of facilitating ever greater continuous surveillance of the what, how, when and where of life. The more biometrical data of a user is collected, the more the integrity of the underlying e-identity is open to fraud and being invisibly compromised. Ethical reflection is long overdue but a prerequisite of minimizing risk to the autonomy of the human person as well as to the integrity of his digital persona.

Interviewee:

Isabella Moeller, MA

- Chief Executive, The Biometrics Institute, London and Sydney.
  Email: manager@biometricsinstitute.org
- The Biometrics Institute - founded in 2001 - is an **independent** and **impartial international** membership organisation. It is a unique forum that brings together the whole of the biometrics industry – users, suppliers and researchers – while giving users more power in setting the direction of this not-for-profit membership organisation through double the voting rights and a majority on the Board of Directors.

Introduction

For philosophers and social scientists, the exercise of power presents many challenges. The exercise of of arbitrary power especially raises concerns both about the purpose of arbitrariness as well as that of accountability. Ethics in implicit. The automated exchange of data and information by robots and strings of code without human intervention begs questions about arbitrariness and power. It also appears to objectify the human, incrementally removing human agency and potentially liberty and autonomy. The internet of Everything requires use to reconsider the scope of resulting challenges to our contemporary understanding of what it is to be human and what, when, how and whether the automated code embedded in everyday life is ethically aware or informed.

The challenges society faces go way beyond constitutional and legal issues: they demand an interrogation of the fundamental tension between the use and abuse of power for ethical and unethical ends by both knowing humans and human-coded machines invisibly qualifying human free choice and shaping the range of human choice. This tension was and remains at the heart of everything and every policy area. The question is what the development of digital life, digital traces and onward use of digitised information that is readily linked to an individual person – as in the case of biometrics – tells us about the nature of digital society and what it means to be a human in a society increasingly adapting to machines mediating our sense of beingness. This begins in babyhood and may have profound implications for our sense of self, autonomy, liberty and responsibility. Interaction with machines is not value-free. Nor is it confined to considerations about invisible ubiquitous tracking and surveillance, and the associated erosion of privacy and notion of informed consent. The digital world begs the question : has the transformative potential of automated data linkage in what is sometimes called an information society been realised, corrupted or (ab)used for (un)ethical ends?

The digi-power dilemma arises not simply from the existence of and accessibility to so much digitised information but from the invisibility of three things: (1) a recognisable and identifiable 'face' to show who is using information over which individuals have lost control, and (2) the invisibility of the fate of that information as it is (ab)used in full or in part by whoever accesses it for known and unknown purposes, often distinct from the purpose for which the information was first provided by, or *accumulated about,* the individual, and (3) most critically, the unknowability for individuals and society about the ultimate locus of both the information slices and whichever machine, contains them temporarily or as permanently as say processing and storage of an e-document trace allow.

Central to the question of identifying who or what is using information is the issue of responsibility and accountability for its use, handling and processing. That is a core principle of legal redress. It is key to concepts of transparency and public accountability in all domains. A lack of recognisability and identifiability of who or what is using information reveals a paradox. On the one hand, the individual must constantly assert and prove their claim to be the authentic owner of a digitized 'identity'. On the other, the human relies on a string of code to validate that claim, usually by linking it automatically and invisibly to some other bit of code. For the human, what is visible is rarely the code but instead some coded representation of an element of himself : a biometric token that trades in probability matching. The tools developed to get and use biometric information skew our understanding of the acceptable limits of public and increasingly privatised or semi-privatised and commercialised intrusion into the private sphere.

During the past decade, the term biometrics has been re-fashioned to conflate the original notion of an algorithm to digitally represent and authenticate an identifiable characteristic of a product or a person with practices that exploit both that identification mechanism and which rely on societal prioritisation of 'security and safety' in order to make such intrusion seem normal; render it so invisible to the individual and society as to encourage them not to think about it; and so facilitate ever greater continuous surveillance of the what, how, when and where of life.

Governments used to monitoring behaviour, see in 'biometrics' and research into biometrics, a short-cut to removing uncertainty by exploiting monitoring techniques to make the unpredictable predictable. Small scale biometric experiments, as in the case of automatic border controls, e-passports, e-visas and e-civil documents, e-banking, e-health have been trialled and presented as convenience gains to citizens and administrative cost-saving gains to governments and commercial ventures alike. However, the accompanying rationale for ever greater surveillance and monitoring by means of linking-up the smaller scale trials is out of step with technological innovation. Technology's capacity to scale-up sometimes lags behind practices which in other contexts would have been deemed politically questionable and unacceptable. However, the opportunities for invisible tracking and linkage attract those who prioritise speed (and convenience) over careful consideration of the purpose behind them, much less the legitimacy or proportionality of such a purpose. The lure of doing something because it is technically possible to do so has held sway over other considerations.

Only more recently have privacy impact assessments become normalized. Even if desirable and necessary, by themselves they are not sufficient. Interoperability is still the holy grail, even if still compromised by significant technical problems. Even so, generating, acquiring, managing, possessing, accessing, splicing, sharing and selling ever more data information proceeds apace, accelerating so far beyond the capacity of data protection authorities and legislatures to protect personal data sufficiently and guard against individual and collective harm. Thus, the 'do no harm' principle of ethical codes is transgressed. The 'right to forget' is laudable but electronic trails remain somewhere that may be unknowable and those trails may become corrupted over-time leaving legacy traces that in turn are unreliable but may nevertheless be (ab)used. How much certainty can or should we attach to technical 'proofs' of the authenticity claim to own an identity, including one's personal identity? Can we develop an innovative identity ecosystem using novel technical capabilities to address more effectively the challenges posed by wrong identity, identity fraud and associated types of cyber and other forms of organized crime?

For industry, biometrics provides at least part of an affirmative answer: probability matching of a token to a person or commodity is enhanced under certain circumstances. But biometrics are not infallible. Yet they are increasingly key to how an algorithm links it automatically to other information and data, or uses it to 'make' automatic decisions about the fate of its subject – the human, a commodity, an animal, plant or mineral. This can of course be very useful. It can also be a double-edged sword. Direct and immediate human analysis is removed from real-time automatic machine decisionmaking in ways that may harm a person or at the very minimum inconvenience him.

The power of an algorithm is misunderstood and exaggerated. Assumptions made when fashioning algorithms and deductions made when employing them need to be better understood. The preconceptions and biases of who or whatever does either must be made explicit. Neither are value free. Neither are neutral. Neither are infallible. Both are likely to have potentially dangerous consequences when used or combined with other data and information or used for purposes which were not envisaged, or not the original purpose. Both human and automated machine analysis can be fallible.

One of the more intriguing challenges posed by artificial intelligence relates to how machine/robot – human interaction and human use of the machine may change the way in which the human relates to his environment. This is not just about 'out-sourcing' memories to the cloud and storing information, such as biometrics, on a mobile device. It is about the potential impact of the robot on human-to-human relationships and interaction. This has been typically described as a master-slave relationship, where the human is master and the robot a tool. This might be an appropriate analogy in a factory assembly line. But, it is questionable in the case of any automated sifting of information designed to match a pre-determined 'profile' with another one in a mass of information, as in the most obvious case of border controls and the use of biometrics to access services.

If, as a society, we are better to understand the impact of something that is rapidly becoming more widely used as a means to authenticating identity claims, it is important to be clear about purpose and about who or what is generating 'information' or 'decisions' (new algorithms derived from the first set of assumptions). What are the underlying assumptions and biases that inform how an algorithm is framed and then used both in real-time and 24/7 by both humans and other automated robots? Wherein lies the allure of biometrics?

Biometric apps are imperfect. Biometric attributes change over time: eg finger prints and voice prints degrade with age: for example, the former are less reliable after the age of 45. However, the idea of using a biometric from birth is gaining advocates. The child's toy that responds automatically to its voice relies on processing that voice biometric and linking it to other strands of information. Alll can be re-used and re-purposed without reflecting on proportionality and purpose. Instead, priority has been attached to the question of how a person's claimed e-identity be made both secure and private. Creating an appropriate balance in the digital single market between privacy and security remains a core challenge and opportunity in developing and managing e-identity. Ensuring privacy and security for our digital persona has to be considered at all stages in the definition and design of any technological project. The more personal data about a user is collected, the more the integrity of the underlying e-identity is open to fraud and being invisibly compromised. E-identity is vulnerable. In that case, asking how to minimize associated risks should, but does not always, begin with reflection on the purpose(s) for which it is created and used. Purpose minimization is often incompatible with the wider commercial goals of interoperability. How, when, who, what and for how long algorithmic information empowers and disempowers needs to be better understood. Ethical reflection is long overdue but a prerequisite of minimizing risk to the autonomy of the human person as well as to the integrity of his digital persona.

In the following interview with Isabelle Moeller, CEO, Biometrics Institute (founded in 2001), Sydney and London, questions surrounding the responsible use and development of biometric apps are explored.

Ubiquitous and Positive Biometrics

Editors: *Why biometrics?*

Isabelle Moeller: Biometrics are everywhere. They are portrayed as the secure and convenient solution to 'proving' identity claims for all manner of transactions from accessing a mobile phone or bank account to paying for goods and services, and crossing international borders, notably at airports. Biometrics have become more widely deployed in all manner of apps, artificial intelligence, banking, travel, domestic robots, children's toys and used as the preferred means for authenticating children registering for school and paying for lunches, for example. This raises profound ethical questions about the nature of society that is being created. These questions dovetail with those around privacy, data protection and consent.

Editors: *why is interest in using biometrics rising?*

Isabelle Moeller : For consumers and industry alike, the asserted convenience and time gains seem persuasive enough to commend the more widespread use of biometrics to 'prove' an asserted claim - you are who you say you are – upon which entitlement to proceed with a transaction depends.

Editors: *Would you say that biometrics are just associated with 'Big Brother'?*

Isabelle Moeller: Not anymore. People who have passports and come across automated physical border management systems are usually familiar with wider uses of biometrics, such as payments. But how much society willingly accepts them varies from country to country.

Editors: *Countries and jurisdictions differ in how acceptable they find biometric identifiers in different contexts. What is the role of the Biometrics Institute in addressing the challenge? How can we try and move towards a consensus internationally about ethical use?*

Isabelle Moeller: It is vital to have a space where ideas can be challenged and an independent voice can emerge. The Biometrics Institute is the **independent** and **impartial international** not-for-profit membership organisation that offers a unique forum that brings together the whole of the biometrics industry – users, suppliers and researchers. It gives users more power in setting the direction of the organisation through double the voting rights and a majority on the Board of Directors. The mission of the Biometrics Institute is to promote the responsible use of biometrics as an independent and impartial international forum for biometric users and other interested parties.

Editors: *How does the Biometrics Institute begin to examine the social impact of biometrics?*

Isabelle Moeller: The Biometrics Institute created a Special Interest Group in January 2017 to help map out the environment. Organisations currently engaged include **DHS USA, UNODC, DIA New Zealand, Amber Alert, NCMEC and other**s. We are still scoping the focus. Social impact can be broken down on a policy specific basis like crime prevention or take a more holistic view to the role of biometrics in respect of social enablement (a basic human right).

Editors: *The two examples you give are not necessarily mutually exclusive are they?*

Isabelle Moeller: No indeed. If one looks at first world challenges like preventing child exploitation and child trafficking, it is tempting to legislate against such practices. Biometric identifiers may be used as a tool by those seeking to investigate, prosecute and prevent such crimes. Biometrics may be a means to help authenticate a child's claimed identity, for example, in natural disasters or war zones, in establishing origin and links in cases of migration, trafficking and modern slavery. But taking a wider view, legislation is not enough. Children are vulnerable in terms of their identity because in part they have to rely on adults providing one for them. These adults may be the perpetrators of crimes involving children. Can biometrics help to protect the child, for example, where modern slavery and cross border trafficking are concerned?

Editors: *so how do we confront the challenges posed by using biometrics to effect change for the good of society?*

Isabelle Moeller: The Biometrics Institute consults its members to define the focus area and assess what can be done to make a change. Do we need guidelines, a statement on research priorities, more of the think piece work to create debate, sponsoring an industry 'competition ' to encourage development of solutions, approaches to multilateral organisations/governments to encourage development of policy?

Editors: *If you begin with the issue of children's rights…*

Isabelle Moeller: having an identity is surely a human right for children. So for us the starting point might be to ask what stops the provision of such an identity. What are the barriers to solving this?

Editors: *presumably there is a lot of interest in how children's identity is authenticated online?*

Isabelle Moeller: Certainly, and also in preventing and resolving child exploitation online. Biometrics have a place in helping to pinpoint the criminals. A further question arises as to how biometrics can be exploited to prevent and resolve missing children and trafficking; create internet safety; combat exploitation of vulnerable people, including children, and illiterate people.

Editors: *Do you see biometrics as a means of enabling the excluded to become more included in society?*

Isabelle Moeller: yes. For example, biometric payment methods could be a safe way for illiterate people to make transactions, or make payments. What is it that inhibits this as a focus? How can biometrics have an ethical impact for sectors of society that are vulnerable and excluded?

Editors: *What is stopping this from being solved?*

Isabelle Moeller: Biometrics are a tool, part of a solution. We need to ask appropriate questions and then come up with some answers that reflect our values. We need to work together across sometimes competing sectors, industries, business models, governments and policy interests to focus on the needs of society in the 21st century and give voice to critical reflection that may challenge long-held assumptions and encourage innovation. If biometrics is an appropriate tool, how can we better use it?

Editors: *Thank you.*