Transatlantic Forum – 3.23.2022 Minutes
Topic – (Un)knowing the Human in Biometric Surveillance: Thoughts on Uncertainty, Ignorance, and Rights
Speaker: Dr. Matthias Wienroth, Senior Fellow in Social Studies of Crime and Policing, University of Northumbria
Discussant: Dr. Marie-Michelle Strah, CIHR Visiting Scholar and Adjunct Professor of International Crime and Justice, John Jay College of Criminal Justice
Rapporteur: Joseph Shiovitz

Presentation by Dr. Matthias Wienroth

Dr. Wienroth opens his presentation by introducing the concept of unknowing as a starting point for the development of biometric human rights. Then he presents the following structure of his talk:

1. Context
2. Human rights as processes of value (valuing)
3. Surveillance as mode of ordering
4. Biometrics
5. The biometric body as (un)known object
6. Towards biometric human rights?

He notes that surveillance is embedded in our daily lives, including how we make decisions and how decisions are made about us, and he highlights our active participation in the surveillance culture as a significant component, meaning that we participate by sharing our data. One purpose for surveillance is to shape behaviors, but not necessarily according to any moral program.

Dr. Wienroth references the concept of 'datafication' as the massive collection of personal data unbound to any specific purposes, whereby the subjects are often unaware that data is being collected about them, how that data is then analyzed, or for what purposes it will be used. Increasingly, data is being aggregated, which emphasizes group and categorical data, and therefore diffuses the boundaries between various uses. Human rights typically concern individuals, but such data aggregation raises issues for groups.

Core rights for biometric surveillance concern privacy, equality, access to benefits, justice, and bodily integrity. Dr. Wienroth raises the issue of transparency, questioning who will get a voice in discussing such rights in the context of biometric surveillance.

Dr. Wienroth describes surveillance as a mode of ordering by describing its most important role as managing people through the monitoring of their movements and behaviors. Common forms include CCTV, identity documents, fingerprints, voice and facial recognition, and things like credit scores. The data collected from such technologies constitute risk assessments, and, he argues, new types of identities and social sorting. For example, travelers are categorized as safe, risky, or illegal. This form of social sorting dictates who has access to certain spaces or services.

Next, Dr. Wienroth introduces the concept of 'data doubles', which enable algorithms to make automated decisions about social sorting. Surveillance mechanisms collect metadata, which

inform how categories of characteristics are generated and contribute to the de-individualization of decision-making, thus re-making human individuals as data images whose significance depends only upon prioritized forms of data. Data is standardized and prioritized for the sake of generating a risk score. Standardized characteristics and risk scores matter more than the individual.

Dr. Wienroth presents examples of data use by police organizations. Police often argue the benefits of such data collection for managing crime, while others argue it is illegal and against human rights to retain DNA profiles in a database.

Biometrics allow for the measurement of unique and comparable physical traits to enable secure identification. Categories of 'belonging' are built according to frequencies of genetic information. Behavioral biometrics also play a role by developing what could be considered 'normal' ways of behaving that would render contrasting behaviors 'risky' by comparison. This poses a problem for people with mobility issues, for example. Dr. Wienroth provides additional examples to highlight the diffuse boundaries of where personal data might end up – created for one purpose but later used for an entirely different purpose, while the process remains largely unknown by the subject/individual.

Dr. Wienroth draws attention to the concept of 'digital epidermalization', taken from Simone Brown's book Dark Matter, meaning the rendering of body characteristics and performances into digitized code to be stored on searchable databases. He warns that certain body forms will become normative as a result of this practice, which leads to bias and discrimination.

He argues that the use of biometric features for security purposes renders the body as both a datafied object and a security-referent object. Both transform collected personal data into aggregated categories for decision-making about individuals.

He then refers to his conception of unknowing, stating the biometric surveillance has a dualistic nature, both knowing and unknowing. Examples of what can be known includes measurements, categories and statistics. However, unknowing includes both ignorance and strategic ignorance, the latter referring to what we don't want to know. Unknowing becomes relevant for human rights when considering that human rights provide guidance for ethical behavior in an uncertain world. Biometric surveillance contains an inherent bias dictating that increased collection and retention of data are goods in themselves.

Dr. Wienroth gives an example of Black Uber drivers being denied access to the software because the facial recognition software failed to match the person to their profile.

In his closing remarks, Dr. Wienroth states that the problem of unreflected unknowing is a creeping naturalization of data categories and data doubles as facts of individuation. Data is collected without an individual's awareness, specific knowledge types are prioritized over others, and data aggregation standardizes categories that lead to bias and discrimination in decision-making. The individual is pitted against an abstract whole. He claims the eventual result will be the erosion of human rights because they won't be applicable to categories or data doubles.

Two essential issues must be considered to think about human rights in the context of datafication and the culture of surveillance:

1. Human rights must be understood as a process of valuing (ethical deliberation).
2. We must think about the production of knowledge about the human and the creation of risk profiles as new forms of identity.

Response by Dr. Marie-Michelle Strah (discussant)

Dr. Strah refers to human rights as a product of the post-WWII era and a reflection of the state of technology and knowledge in 1948, which presupposes a concept of citizenship as a physical person with inalienable rights. But the era did not address the concept of data doubles or the era of surveillance capitalism (a reference to work by Shoshana Zuboff). Data doubles have transformed the question of 'how do we know' into 'how do we own'.

The concept of protecting the individual from state encroachment has shifted to protecting against corporate encroachment in the new era of surveillance capitalism. Corporate actors have "productized" data collection and resold them back to criminal justice agencies as tools of predictive policing. Data doubles are also used in micro-targeting by terrorist groups and in political disinformation campaigns.

The push for more technology and more data is driven by Silicon Valley, where computer scientists often have different concepts of "knowing" than lawyers, social scientists and others. Dr. Strah supports her arguments with the example of Timnit Gebru being fired from Google for her work on bias and racism in artificial intelligence. Her epistemological lit review was considered non-standard by Google. Many other researchers are being prevented from doing their work.

All 193 member states of UNESCO unanimously approved a resolution on AI and ethics.

Along with the corporatization of data doubles, we are seeing the resurgence of pseudo-sciences like phrenology. Scientists are becoming corporate criminologists and commodifying this knowledge.

Dr. Strah uses the example of San Francisco Police using DNA data from sexual assault victims to underscore the issue of gender and the diffuse boundaries of data usage. The DNA was provided to solve sexual assault cases, but the police were using it to solve other cases (and without the victims' consent).

Discussion

Question: While using public transportation at night, I observed erratic behavior from a mentally ill person, prompting a reflection of whether I felt safer knowing there was surveillance, as if it would deter any crime. My answer was no. Also, I felt uncomfortable knowing I was on-screen and somewhere another person was observing my personal characteristics, and I ask who would really need the information?

Answer (presenter): We are talking about protection against state and commercial actors. We must consider that we share data voluntarily, but we also don't know what kind of data we share. Can we even have human rights for regular sharing of large amounts of data?

Responding to the discussant, the question of what is normal is a really complex and difficult one. 'Norming' excludes people from the commons, particularly people with disabilities or mental health issues, and others. How can we overcome this exclusion of people from the commons? I don't have an answer. We do need to work across expertise. We need to work with developers of biometric technologies, as well as those who are subject to them. How biometrics affects people. My experience is that the developers do not understand the experience of biometric surveillance.

Ownership of data, regarding the NYPD case. Police want to retain data. Some people say it is unethical to use data from victims to investigate crimes. I agree it is unethical if they are not asked, on the basis of informed consent. In the UK, a lot of voluntary data can be retained on police databases. And there's no real mechanism for volunteers to get their data off there. But in the case of victims, they are not volunteers. The victimization through state agencies has led to the crisis of legitimacy in state policing.

Going back to the issue of surveillance, most CCTV cannot hear, it can only see. The information is therefore limited. It's also operated at a distance. There is a record, but will it help to prevent an attack? So, data is being taken. Is it preventative, or only useful after the fact? Who is the beneficiary of the data being collected? Some have characterized CCTV as open-air prisons. But, if you're not protected by CCTV, is it fair?

Question: You mentioned the example of a Black Uber driver who could not be recognized to access the Uber technology. How should we think about this? Do we improve the technology so recognition is more 'inclusive'? At the same time, you are warning against the dangers of having our data collected. It's kind of damned if you do, damned if you don't. What are the short and long-term implications? When "access" becomes dependent on our data being collected, will we need to surrender it in order to stay involved?

Answer (presenter): That is workplace biometric surveillance. You need to submit to be able to work. I don't think that is right. You could just have a code you need to type in. There should not be this requirement. To make it worse, if the system does not auto recognize you, it gets pinged onto a person. Then, not even a person could make the connection. Clearly there is an issue around race-based recognition in human beings as well, not just in a system. Here, I don't think the requirement is justified. To the other part of the question, there are dangers, but we cannot escape having our data collected in many cases. Mortgages are based on risk profile. We need to become more aware of where data goes and where we are sharing data, but also need to recognize we don't have control over our data. This is the uncertainty created in us as data subjects. This should have an impact on legislation. There should be questions around how can we embed the kind of valuing in regulative tools. That's more for lawyers and legal scholars.

Answer (discussant): The Uber case speaks to the challenges in experience (UX) design. A lot of human-computer interaction is not just about culling a database, there is a whole element of

design that often gets neglected. The Uber case is an example. Also, a lot of companies are unwilling to invest in UX design. It can be expensive and raise the cost of the project, and slows down bringing things forward, which is the ethos of Silicon Valley. It requires upfront investment.
Having a more informed public, not just data literacy, but also info and media literacy, is critical to rebalancing the damned if you do or don't ecosystem. More data is not necessarily good. The idea that collecting so much data will make it easier for police is always mentioned as justification, but effectively it takes police longer to sort through unsolicited data. So it's not necessarily accelerating or improving these procedures. We should interrogate this assumption of more data being more efficient or necessarily good. The time and expense is much more.

Question: Will the discussion regarding the usage of data someone once gave willingly ultimately lead to a new question of defendants' rights? I.e. shouldn't the question be: Do I have a right of my data to remain silent? Won't the discussion ultimately turn toward the question of legally or illegally obtained evidence, as Matthias just implied? The police will probably say that it should be able to use any means they can get to solve a potential crime anyway. So how do we discern then, which kind of data which I gave willingly can be used against me (ex. fingerprints) and which can't? Will there maybe be a general disclaimer before any sort of data is used telling me that this data might be used against me at some point in the future if I commit a crime?

Answer (presenter): There is a limit for how long CJ data can be retained in many places. Usually, the longest period is for those convicted, much less for others. The issue is rogue police officers using data without telling anyone they're using it, which falls back to retention periods and who has access. There are problems with unregulated data. How can you control it? In the US, you can sue the police force. I feel that not very much can be done around data that ends up on databases unless there is legislation around retention periods. I don't think police will agree to limitations that are not legally prescribed. The question of 'should we catch killers or make people uncomfortable with data collection' is an unethical question because it is completely hypothetical.

Question: I was fascinated with how much you have been influenced by Donald Rumsfeld. It seems we are being compartmentalized into different spaces of varying degrees of unknowingness. We may be in a space we are targeted for our spending patterns, or credit card companies if we are credit worthy. Other spaces can be trickier, like if we socialize with certain people then we become security threats. All these spaces are varying degrees of things we don't know that we don't know, but that we should know. It seems to me that an entry point to addressing this issue in the era of increasing normalization of surveillance is the reconceptualization of the right to know. If we don't have a credible understanding, it will be difficult to address these challenges. Can you elaborate on the point you raised about attending to the epistemology of biometric surveillance technologies, as we are thinking about the role of human rights, and how should we reconceptualize the right to know so we can address the epistemology of biometric surveillance?

Answer (presenter): Donald Rumsfeld is an excellent strategic ignorance manipulator. He identifies information that should be ignored. This links to your question. A right to know depends on the context in which you want to apply this right. I'm not the person to tell you about

the legal context. I'm interested in how decisions are made about how and what we need to know. We need to understand what values come into play around what knowledge is considered to be central in order to make decisions about people, and what knowledge isn't, and how this knowledge should be interpreted and should be applied. Customer profiles bring together a lot of very diverse data. Shopping habits will have an impact on credit score, and the ability to take out a loan. I am in favor of saying any commercial information about which categories you belong to should be made visible to you. You don't necessarily know what to do with the knowledge, but at least you'll know what elements are used for a commercial player to make decisions about you. Especially important for data doubles. We need to know what knowledge is coming together about us, not even individually. But what categories are being drawn from to categorize us. What concentric circles do we belong to? My inquiry is about what types of knowledge are relevant to make decisions about other people. Consider the case of access to a country... border control. We speculate about what decisions are made about whether it's a legal traveler, risky traveler, etc... but we don't really know everything. State actors may say it is good that people don't know, or else people may try to evade these factors. Some data collection is important. Think about health data and learning about treatments. I'm saying, in a commercial context, we need to know categories. In a criminal justice context, I don't think we will ever find out because it might be considered as prescribing a crime script and what to avoid.