# Thies Gehrmann Ph.D    Letter of Motivation

Dear Committee,

I am applying to your vacancy within the DIGIFED project on trust in government decision making and machine learning. I am a bioinformatician and I have worked on and with machine learning and statistical models for the prediction and interpretation of biological effects in fungal, plant, and human systems. My latest research focuses on the genetic and environmental effects on longevity and healthy ageing in humans. Therefore, my research expertise is less on governance through technology, but on the methods by which these predictions are being made, and the possibilities these technologies provide. The position your group has announced is very interesting to me as it provides an opportunity to pose questions that quickly arise when one looks up beyond the research niche to the broader social implications of the technologies we develop and use. In this text, I have omitted references for my statements. If you wish me to provide them, please do not hesitate to contact me.

The desire for mass surveillance of populations, by local and foreign companies or governments, has been repeatedly demonstrated by the development of encryption backdoors in telecommunications infrastructure, the proliferation of social media, loyalty programs, online trackers, the cash-free economy, mobile wallets, the extensive use of sensors and wearables, cameras in public spaces, and the sharing of data between private and public entities. These large datasets are collected to tailor personalized advertising, to detect banking and social service fraud, to predict creditworthiness, crime, recidivism and urban waste production, to determine risk factors for disease and insurance claims, and more. While these aims sound appealing, they carry with them the danger of being abused, incorrectly investigated, or worse, incorrectly applied to inform social and governance policy. Further, the aims of these programmes risk to exacerbate, rather than ameliorate pre-existing social inequalities.

The collection and exploitation of data in public and private spaces has become a source of concern for many. Fearing that these concerns may lead to market regulations, Data Science companies invested strongly in the discourse surrounding the limitations and solutions to these concerns, in part through the funding of research into Ethical AI. While government institutions and research institutes (such as universities) are subject to ethical reviews and approval that restrict data collection and processing, private companies are not subject to such invasive restrictions on their activities. In partnership with companies, government institutions may be able to tap into data collected in the private domain, without the agreement of the individuals whose data is being used. Through such collaboration, the distinction between private and public collection of data is obscured. Further, it is likely that private enterprises will be contracted to implement specific government projects, be they for law enforcement, military, medical, or social tasks. Therefore, an analysis of trust of machine learning in governance, cannot be separated from trust of machine learning in the private space, though they may be separate in the eyes of the citizen.

Anecdotally, I am often surprised by the blasé attitude, common among not only the lay-public, but also many data science researchers towards the mass collection of data, arguing that people should have nothing to hide, and the perception that, with further research consequences can be avoided. This strategy is mirrored in many aspects of society, such as climate change, in which the promised technological developments of the future provide a Carte Blanche to consume and pollute today. This comparison goes further in that, just as your act of polluting the earth does not only affect you, so does your data characterize not only you, but also of those around you. Your interactions reveal information not only on you, but also on those with whom you communicate and the genetic material you provide to a testing facility reveal data not only on you, but on your whole extended family.

These observations, on the continued collection and exchange of data by governments and private parties through mass surveillance, their continued exploitation for antisocial tasks or private interests, the impossibility to opt-out, and the misleading information provided on the dangers and risks of these technologies, it is clear why trust in the uses of these technologies are up for debate. Why would somebody trust a public entity or a government in these tasks? I anticipate that these this question will have deeply personal answers, connected tightly to their knowledge, their values and risk assessment.

A framework in which I believe it would be very interesting to examine this trust or distrust is that

of bounded rationality. In this model, we claim that all decisions are rational, but that rationality can be limited, or bounded, by the lack of information, the personal value system, psychological limitations, and other factors. These limitations are expressed in a utility function, which may differ between people. For example, salary loans and cigarettes, will be highly rational decisions when the utility function is dominated by severe financial need or addiction. The same thing can happen when the downsides of personal data collection are overshadowed by immediate personal benefit, or if the costs associated with them are obscured. The challenge will be to reconstruct the utility functions - how are risks evaluated, and what values do they have? - that people use to make their decision to trust or distrust the use of machine learning by government or private entities.

I therefore think that the project will contain several components. First, to identify the (positive and negative) outcomes of the use of machine learning by government (and private entities). Second, to determine what people estimate the likelihoods and costs associated with these outcomes are. Third, to identify the confounding factors that motivate people to calculate the risk as they do; What are their values, beliefs, and preferences that may cause them to value certain outcomes more desirable than others, and what do they use to calculate the likelihood of different abuses? Finally, to understand how these different factors are used to make a decision on whether to trust or distrust the government and private exploitation of data.

My background is perhaps not what you are looking for; I am not a political scientist, sociologist or a psychologist. During my career so far, each stage has provided a methodological challenge. My Masters degree was in machine learning, my Doctorate focused on the development of novel computational methods for the exploitation of RNA-Sequencing data, and my postdoctoral positions have gone from comparative genomics methodologies, to population genetics and investigations of population heterogeneity. I am ready for another methodological challenge. I hope that this letter convinces you that I am aware of the discourse surrounding this topic, interested in understanding these complexity of the subject, and willing to learn and perhaps develop novel methodologies within sociology.

I hope that I may have the opportunity to discuss the ideas in this letter further with you.

Kind regards,

-Thies Gehrmann