Testimony of Julia Stoyanovich before the New York City Council Committee on Technology regarding Automated Processing of Data *Int. 1696-2017*

October 16, 2018

Good afternoon!

My name is Julia Stoyanovich, I am a resident of New York City (District 7). I hold a Ph.D. in Computer Science from Columbia University. I am an Assistant Professor of Computer Science at Drexel University in Philadelphia, and an affiliated faculty at the Center for Information Technology Policy at Princeton University. In my research and teaching, I focus on data management and data science topics, including algorithmic ethics: fairness, accountability and transparency. I am also the founder of the *Data, Responsibly* consortium.

My statement is based on conversations with Ellen P. Goodman (Professor of Law at Rutgers University) and Bill Howe (Associate Professor at the Information School at the University of Washington).

I would like to commend Councilman Vacca on sponsoring an ambitious bill on algorithmic transparency. Transparency of algorithms that are used in the public sector refers to making explicit the design and policy choices these algorithms embed. Transparency of digital governance is essential because it enables accountability to the public, facilitates public debate about policy, and helps move our democracy forward.

However, it is my belief that the bill under discussion requires significant improvement to achieve its intended goal. In my statement, I will focus on three critical shortcomings of the bill, namely that:

1. algorithmic transparency cannot be achieved without data transparency;
2. results received by the user by interacting with the system must be made interpretable;
3. enacting transparency will require significant technological effort on the part of the agencies, for which more time will be necessary than is currently provisioned.

I now briefly discuss each of these points in turn, and conclude with a set of recommendations.

My first point relates to the first part of the proposed amendment: “publish on such agency’s website the source code of such system.” While making source code publicly available is a significant step towards transparency (as long as the posted code is readable, well-documented and complete), **meaningful transparency of algorithmic processes cannot be achieved without transparency of data.**

In the case of predictive analytics, data is used to customize algorithm behavior - this is called “training.’’ The same algorithm may exhibit radically different behavior -- make

different predictions; make a different number of mistakes, and even different kinds of mistakes -- when trained on two different datasets. In other words, without access to training data, we cannot know how a predictive analytics method will actually behave. Algorithms of this kind are used, for example, in predictive policing software.

Other decision-making algorithms, including, for example, scoring methods like the VI-SPDAT, which is used to prioritize homeless individuals for receiving services, and matchmaking methods such as those used by the Department of Education to assign children to spots in public schools, do not explicitly attempt to predict future behavior based on past behavior. Yet, these algorithms also rely on data in important ways: they are designed and validated using data.

What do we mean by data transparency? One immediate interpretation of this term is -- making the training and validation datasets publicly available. However, while data should be made open whenever possible, much of it is sensitive and cannot be shared directly. That is, data transparency is in tension with the privacy of individuals who are included in the dataset.

An alternative interpretation of data transparency is as follows: In addition to releasing training and validation datasets whenever possible, agencies shall make publicly available information about the data collection and pre-processing methodology, in terms of assumptions, inclusion criteria, known sources of bias, and data quality. Agencies shall make publicly available summaries of statistical properties of the datasets, while using state-of-the-art methods to preserve the privacy of individuals. When appropriate, privacy-preserving synthetic datasets can be released in lieu of real datasets, if real datasets are sensitive and cannot be released to the public.

My second point relates to part 2 of the proposed bill: “permit a user to (i) submit data into such system for self-testing and (ii) receive the results of having such data processed by such system.’’ **To facilitate transparency, the result of the self-test program should be interpretable, insightful and actionable.** For example, suppose that software is used to score and rank individuals for access to a service. If a user enters her data and receives the result -- a score of 42 -- this will not explain to the user why she was scored in this way, how she compares to others, and what she can do to potentially improve her outcome.

Establishing appropriate result presentation methodology that supports interpretability will require a deep understanding of the technical and policy context on the part of the agency. As part of the result, data that pertains to other individuals, or a summary of such data, may need to be released to the user, for example, to explain which users, or groups of users, receive a higher score, or a better outcome. This functionality requires data transparency mechanisms discussed above.

Further, when a user receives a result, she must be able to challenge it by submitting a request for additional explanation, or correction, to the agency.

Finally, in addition to allowing individual users to interrogate the system, it is important to establish an auditor role in support of systematic verification. An auditor may be granted access to more data than what the general public is allowed to see, and will have a

sufficient level of technical expertise to test software for properties like robustness, correctness and non-discrimination with respect to legally protected groups.

My third point is brief, and relates to paragraph 2 of the amendment "this local law takes effect 120 days after it becomes law." Enacting this amendment will require significant technological effort on the part of the agencies. It will require careful planning, financial resources and time. As an illustration of two recent public actions of a similar nature: the French Digital Republic Act came into effect on October 7, 2016, following a year-long process, while the EU General Data Protection Regulation (GDPR) was adopted on April 27, 2016 and will become enforceable on May 25, 2018, more than two years later.

In summary, I recommend:

1. that data transparency be considered in this amendment as an integral part of algorithmic transparency;
2. that users be provided interpretable self-testing results, and have an option to request additional explanation or correction; and
3. that a realistic plan for enactment of the amendment be put in place, with a longer timeline.

Thank you for your attention!

Julia Stoyanovich
stoyanovich@drexel.edu
www.dataresponsibly.com