Verbal Testimony - Dr. Sara Jordan, Future of Privacy Forum
H.263 (automated decision systems) & H.410 (artificial intelligence commission)
House Energy & Technology Committee Hearing: Status of AI Policy Throughout the Country and Internationally
April 28, 2021 (9:00am ET)

Thank you Mr. Chair, I am Dr. Sara Jordan, Senior Counsel at the Future of Privacy Forum, focused on Artificial Intelligence and Ethics.FPF is a non-profit dedicated to supporting consumer privacy leadership and scholarship. Our mission is to advance principled data practices in support of emerging technologies.

First, I'd like to take the opportunity to commend the sponsors for your continued attention towards artificial intelligence, an important issue of significant concern for privacy, data protection, and civil rights.

Vermont is not alone in considering this issue. Automated decision systems legislation is also being considered in California, Colorado, New Jersey, Washington State, and Maryland. In addition, the Federal Trade Commission has decades of experience enforcing the FTC Act, the Fair Credit Reporting Act, and the Equal Credit Opportunities Act in the context of automated decision making. Overseas, the European Commission recently unveiled an extensive proposal to regulate AI.

Given this broader context, today, I would like to offer some general observations and recommendations about regulation in this area, which I hope will be helpful as you consider how to move forward with AI policy. As a general matter, it's crucial that any measures adopted serve to increase transparency and accountability without overburdening vendors or creating compliance barriers for new technology.

As we see it, there are at least four key areas of opportunity for legislators across the US to clarify and improve the technical and conceptual expectations incorporated into current automated decision system legislation: (1) Clearly define the automated decision-making systems of concern; (2) Attend to the needs of the audience; (3) Ensure an appropriate timeline for complete compliance; and (4) Include appropriate provisions to mitigate unintended consequences.

1. **Clearly define the automated decision-making systems of concern**

Automated decision systems are part of the fabric of our lives, whether used to reroute internet traffic due to unexpected surges in data flows, or used in situations that materially impact a person, such as when they are used to grade students' tests or diagnose health conditions. It will be important for regulation to focus on areas which present a heightened risk of harm to a natural person, and to avoid over-broad or vague definitions of ADS. Appropriately defining what is considered to be an ADS is an important step for implementable regulation. Clarifying which ADS influence decision-making in an adverse, discriminatory, or harmful way is also imperative. Particularly for regulations that invoke a tiered method for ranking which systems will need to go through different forms (e.g., self vs third party) of review or different levels of scrutiny, it is essential that the legislation define ADS in ways appreciable by system engineers, the public, and legislators.

A key component to be clarified in legislative efforts to define automated decision systems is the definition of “automated decisionmaking” that accounts for the wide range of tools used to create the outputs of automated systems. In particular, legislators should be cautious to define automated decision systems with respect to techniques used to manipulate data to arrive at a decision, whether that is through use of statistical modeling, artificial intelligence or machine learning that produces a score, classification, recommendation, or other simplified output, to support or replace human decisionmaking.

As part of our efforts to educate policymakers like you about the various types of AI and machine learning that make up the “automation” in many, but not all, automated decision systems, we build an infographic, “The Spectrum of Artificial Intelligence” that shows the many forms of AI that are used in decision systems deployed by governments and private firms today. We have shared this infographic with you as part of the testimony we submitted and I am happy to take questions about this.

Many automated decision systems rely on methods of data analysis that do not fit visions of extraordinarily complex, inexplicable, artificial intelligence as created by the “AI hype cycle”. In most cases, explicable forms of artificial intelligence are used rather than more opaque, neural-network based machine learning. Rules-based or symbolic AI, which knits together logical “if-then” statements to determine whether a combination of data points meets a decision threshold, is able to be explained in ordinary language. Knowledge engineering, which creates network map pathways between documents and their components to help us understand tax codes, can be explained by computer scientists in much the same way that social network analysis can be explained by social scientists. Natural language processing systems that help customers navigate websites through interfaces such as chatbots may be powered by extremely large language models, but many are not. Instead, commonplace natural language processing techniques, such as dictionary-based search or question-answer wizards, are behind many of the systems used by unemployment offices and vaccine-finders. Machine learning, which is used to build recommender systems that help customers find products that fit their preferences, often leans on regression techniques readily understood by economists. Even image processing performed by neural networks can be explained through use of saliency maps. The primary challenge for legislators striving to understand the techniques of automated interpretation of data, such as through AI, is to grasp the landscape and vocabulary. We hope that the infographic and associated white paper will help you accomplish these goals. We also hope that these tools will help you to better explain automated decision systems to the audience of other Vermont legislators and your constituents.

2. Attend to the needs of the audience

Automated systems are pervasive, affecting individuals, groups, offices, and organizations. What each of these members of the audience to ADS need is comprehensible information that allows them to understand when automated systems make decisions that affect them, to understand how their data is used in these systems, and to appreciate how they might take action to protect themselves and others from any adverse effects the use of ADS introduces into their lives. Effective legislation will need to address the information needs of the multiple audiences of users and subjects of ADS when considering the variou types of oversight tools that could be used, such as disclosure requirements, registries, and impact assessments governing automated decision systems.

In January of 2021, the National Institutes of Standards and Technology (NIST) offered guidance on explainability in artificial intelligence that might help states as they craft the criteria for impact assessments which will be useful for the multiple audiences to automated systems using artificial intelligence and similar technology. The NIST guidelines suggest four principles for explanation: (1) Systems [should] offer accompanying evidence or reason(s) for all outputs; (2) Systems [should] provide explanations that are understandable to individual users; (3) The explanation [given should] correctly reflects the system's process for generating the output; and (4) The system [should] only operates under conditions for which it was designed or when the system reaches a sufficient confidence in its output (p.2). These principles might be met through any number of mechanisms within an impact assessment framework, but constitute a baseline for the components that ADS or AI impact assessment tools will need to encompass to meet their intended regulatory goals.

3. Ensure appropriate timeline for compliance

Proposed legislation, presently considered in Vermont and elsewhere, suggest wide ranges of tools and timelines for implementation of oversight of automated decision systems. Some bills assume that ADS in current use have been appropriately documented, characterized, versioned, and catalogued in a location easily accessible by persons accountable for submitting impact assessment evidence. However, the complexity of the systems themselves and the lack of prior requirements for tracking automated systems in contracts or procurement decisions means that some organizations may not readily have access to technical information on all systems in use.

Government offices and vendors to governments may not be aware that the systems they use every day to improve throughput, efficiency, and effective program monitoring fall under the definitions of automated decision systems as proposed. Governmental organizations in particular may not realize that they are using algorithmic systems provided as part of a package of services provided by a vendor. Also, governmental offices suffer from siloed procurement and development strategies and may have built or purchased overlapping ADS to serve specific, sometimes narrow, needs. Ensuring that ADS legislation is robust to the somewhat messy reality of documenting ADS in use by governments or private businesses, including identifying dependencies between automated systems, will require legislators to build in supportive mechanisms such provisions of time, or expert personnel.

4. Include appropriate provisions to mitigate unintended consequences

Many proposed bills envision a new or expanded oversight office with the responsibility to design and review organizations compliance with legislators' expectations. Creating or expanding these offices will present states with many challenges, including identifying and attracting appropriately qualified personnel. The personnel needed for these offices must be able to meaningfully interpret algorithmic impact assessments, they will need to do so in an environment of high sensitivity, publicity, and technological change. As observed in many state and federal bills calling for STEM and AI workforce development, the talent pipeline is limited and legislatures should address the challenges of attracting qualified personnel as a key component of these bills.

Finally, protecting the public from adverse decisions by automated decision systems may, perversely, raise privacy and security risks. Bills requiring handovers of training, test or

validation data, or to make public the source code for systems, may inadvertently open opportunities for data breaches, exfiltration of intellectual property (IP), or even attacks on the algorithmic system which could either identify individuals or cause the systems to behave in unintended, harmful, ways. As state bills progress, deep collaboration with privacy engineers, data protection, cybersecurity, and IP lawyers will be needed to ensure that these assessments do not introduce unforeseen risks.

We would encourage lawmakers and agencies to continue to solicit the input of the business and technical community.

We've sent resources to the Committee as well - and I'd be happy to discuss any aspect further. Thank you for your time and attention.

Sincerely,
Dr. Sara R. Jordan
Senior Policy Counsel, Artificial Intelligence and Ethics
Future of Privacy Forum
sjordan@fpf.org

Attached:

- FPF "Spectrum of Artificial Intelligence" Infographic
- FPF "Spectrum of Artificial Intelligence" Whitepaper
- FPF "10 Questions on AI Risk"
- FPF "Distilling the Harms of Automated Decision Systems"