LAWYERS' COMMITTEE FOR CIVIL RIGHTS UNDER LAW

ONLINE CIVIL RIGHTS ACT

Highlights and Summary of Key Provisions

The following summary highlights important provisions in the Lawyers' Committee's model artificial intelligence bill. This model legislation was crafted to address the discriminatory outcomes, bias, and harm arising from algorithmic systems, which form the basis of artificial intelligence products and large language models. It seeks to both mitigate and prevent current, ongoing harms while also providing a broad, tech-neutral regulatory and governance regime to sufficiently address generative AI and further technological development in this space. The legislation was created through surveying and adopting concepts from major pieces of existing proposals on AI regulations (such as the Algorithmic Accountability Act, the Algorithmic Justice and Online Platform Transparency Act, California's Assembly Bill 331, DC's Stop Discrimination by Algorithms Act, and more) as well as modifying H.R. 8152, the American Data Privacy and Protection Act to fit the specific contexts of algorithmic systems. Currently, there is no comprehensive regulation of artificial intelligence, algorithmic systems, or federal privacy law governing the personal data these systems utilize. This model legislation seeks to change that status quo, providing significant civil rights and privacy protections and encouraging the safe and effective design and deployment of AI.

DISCRIMINATION, SEC. 101 - Developers of algorithmic systems and those who deploy algorithmic systems (henceforth referred to as "developers" and "deployers") may not offer, license, or use a covered algorithm in a manner that discriminates or otherwise makes unavailable services, including disparate impact, on the basis of race, color, religion, national origin, sex, disability, or other protected characteristics.

- Algorithmic discrimination is prohibited.
- Developers and deployers are permitted to use covered algorithms to check for and prevent discrimination, and to diversify applicant, participant, and customer pools.

HOW THIS SECTION IMPROVES THE STATUS QUO: Algorithmic systems collect and use data about who we are, resulting in intentional and unintentional discrimination and biased results. Already there is rampant discrimination by algorithms used in areas such as employment, financial services, healthcare, education, insurance, the criminal legal system, and housing. Without sufficient laws and enforcement resources, these harms will only grow worse as the technology evolves. The model legislation prohibits this discrimination and proactively protects civil rights.

PRE-DEPLOYMENT EVALUATIONS AND POST-DEPLOYMENT IMPACT ASSESSMENTS, SEC. 102 - Developers and deployers must evaluate and audit their products for discrimination, bias, and harm both before and after deploying or offering their products in interstate commerce.

- First, developers and deployers must conduct a short form evaluation checking whether it is plausible that the use of an algorithm may result in a covered harm under the act.
- If harm is plausible, they are required to engage an independent auditor to evaluate the algorithm's design, how it works, how the algorithm might produce harm or discriminatory outcomes, and how that harm can be mitigated.
- The evaluation will include a detailed review and description so that external researchers can evaluate how the covered algorithm functions, including its risks, uses, benefits, limitations, and other pertinent attributes.
- Deployers will then annually assess the algorithm as it is used, detailing any changes in its use or any harms it produces. Developers will review these, and both evaluations and assessments will be reported to the Federal Trade Commission and summarized on the websites of developers and deployers.

HOW THIS SECTION IMPROVES THE STATUS QUO: Because there is no comprehensive regulation of algorithmic systems, nor mandated human oversight, algorithms can produce a myriad of harms, including discrimination and bias, without being detected. This section ensures that algorithms are reviewed both in the design and deployment phases and ensures that there is a paper trail for enforcement of the act. It also encourages responsible innovation by building knowledge and best practices about how to prevent harm.

DUTY OF CARE, SEC. 201–204 requires that algorithmic systems are safe and effective.

- An algorithm is safe if it is evaluated by a pre-deployment evaluation and impact assessments, reasonable steps are taken to prevent it from causing harm, its use would not violate the Act, and its use is not unfair or deceptive.
- An algorithm is effective if it functions as expected, intended, and publicly advertised.
- Developers and deployers are also prohibited from engaging in deceptive marketing, off-label uses, and abnormally dangerous activities.
- To meet these obligations, the act addresses contractual obligations between developers and deployers and requires that both establish governance programs.
- The act also prohibits retaliation, protects whistleblowers, and establishes a right to appeal decisions made by algorithms or the ability to opt for a human alternative to a covered algorithm in specific circumstances.

HOW THIS SECTION IMPROVES THE STATUS QUO: Consumers should be able to trust that algorithmic systems are safe and effective. But, many algorithmic systems currently on the market have significant inaccuracies, biases, or simply fail to perform as expected or advertised. These sections ensure that companies must take adequate steps to protect consumers and make sure that their products work, or else they may be subject to enforcement actions and liability.

DATA SECURITY, SEC. 301–303 requires companies to maintain robust data security and restricts the collection and use of personal data.

- Deployers and Developers are prohibited from collecting, processing, or transferring an individual's data except for what is reasonably necessary and proportionate to provide or maintain the specific product or service requested by the individual to whom the data pertains.
- Developers may only use an individual's personal data to train a covered algorithm if they obtain affirmative express consent.
- There are some limited exceptions for security processes, maintenance, debugging, delivery of products or services, authenticating users, transferring assets in the context of a merger, preventing fraud and harassment, running diagnostics, conducting research, effecting product recalls, and complying with other laws.
- The act also requires that companies provide individuals with the right to access, correct, or delete any personal data used to develop or deploy an algorithmic system.

HOW THIS SECTION IMPROVES THE STATUS QUO: Data protection is necessary to protect individuals and prevent data misuse or breaches, as well as to ensure information is used to train AI responsibly. These sections are built on the idea that the best way to protect private data is to not collect unnecessary data in the first place. Currently, we have a notice and consent framework, meaning companies create long, dense privacy policies which are required to use a service and give them permission to make virtually any use of data they choose. Companies therefore collect, use and share vast amounts of personal data when developing or deploying algorithmic systems, leading to security risks, discriminatory practices, predatory advertising, and fraud based on personal information.

TRANSPARENCY AND EXPLAINABILITY, SEC. 401–404 requires that companies notify individuals about whether and how an algorithmic system affects their rights.

- Companies are required to publish long-form disclosures that include information about pre-deployment evaluations, impact assessments, and a detailed description of data practices. This enables research and accountability.
- Companies are also required to provide individuals with an easy-to-understand short-form notice about its use of a covered algorithm, so that individuals know that an algorithm is being used, and why.
- In certain high-risk circumstances, companies are required to provide individuals with a means to request an explanation about how they are affected by an algorithmic system.

- Deployers are also required to label any AI-generated content used in a commercial setting, making it clear to consumers when content is created or modified by AI.

HOW THIS SECTION IMPROVES THE STATUS QUO: Although algorithmic systems are used throughout the economy, most people have no knowledge about when or how they are impacted by these systems. Without this awareness, individuals cannot make informed decisions about how they interact with AI and are unable to seek redress when harm occurs. These sections ensure that individuals can access the information they need to know about when and how AI affects their rights and opportunities.

ENFORCEMENT, SEC. 501–504 - The FTC, State Officials, and individuals will be able to enforce the bill's provisions through different means.

- The FTC is empowered to enforce the act and promulgate regulations.
- State authorities will be able to bring and join civil actions against those suspected of violating the act.
- Individuals will have a private right of action to bring civil actions against those suspected of violating the act.
- The act clarifies that a person who offers or uses generative AI—like AI chatbots or image generators—does not receive Section 230 immunity for the AI-generated content.

HOW THIS SECTION IMPROVES THE STATUS QUO: Multiple enforcement mechanisms ensure compliance with the Act and improve on the limited options available to protect against algorithmic discrimination now. The FTC will have enhanced authority. State Attorneys General and other authorities will be able to enforce on behalf of their citizens while still allowing individuals to protect their rights themselves by bringing legal action. These measures help ensure that individuals who are harmed have recourse.