REPORT BY THE TECHNOLOGY, CYBER & PRIVACY COMMITTEE

RECOMMENDATIONS RESPECTFULLY SUBMITTED TO THE BIDEN-HARRIS ADMINISTRATION

The Technology, Cyber & Privacy Law Committee of the New York City Bar Association is honored to provide our recommendations relating to the subject matter of our Committee for the Biden-Harris Administration's consideration.

I. ALGORITHMIC ACCOUNTABILITY

We urge the new administration to explore and implement safeguards to ensure the continued leadership and development of artificial intelligence technologies in the United States. Such guidance can serve as a model for global norms of artificial intelligence development and use by governments and the private sector, with the goal of maintaining innovation, establishing public trust and maintaining public confidence in artificial intelligence systems and technologies.

The federal government, through Executive Order 13859, directed federal agencies to ensure that the United States maintains its competitive leadership position in artificial intelligence. Various agencies have taken steps to further such goals, including the National Institutes of Standards and Technology (NIST) in its work to develop technical standards for the development of artificial intelligence technologies. Additionally, the Federal Trade Commission has taken note of the ubiquitous use of artificial intelligence technologies in providing goods and services to consumers in the United States. Few areas are left untouched, as companies make use of new computing power and larger data sets to develop algorithms deployed in all major industries, such as automotive (autonomous driving), education (predictive analytics), banking (credit evaluation), housing (smart meters and facial recognition), healthcare (diagnoses), and human resources (hiring and retention), to name a few examples. Governments, too, utilize artificial intelligence technologies in the justice system (sentencing guidelines), law enforcement (facial recognition), and military (automated weapons).

The lack of a framework for the responsible development and use of artificial intelligence technologies has unsurprisingly led to countless examples of undesirable outcomes, whether it is failing to identify racial minorities in facial recognition software, curating a pool of less (rather than more) diverse employment candidates, or more benignly, deploying autonomous chat bots which were intended to be friendly companions but instead were trained by Internet users to act

profanely. It's easy to understand how the stakes are higher when governments make use of flawed algorithms, for example incorrectly calculating recidivism rates based on racial background. The results are particularly troubling because in almost no cases can the aggrieved party challenge, examine or audit the algorithm which was responsible for the undesirable result.

To guard against harmful discrimination in the use of artificial intelligence technologies, we urge the Biden Administration to develop a framework that takes into account several core principles for algorithmic transparency and accountability:

1. Education - developers, designers and other stakeholders should understand potential pitfalls of artificial intelligence and related technology design, thus guarding against reflecting and reifying existing biases through selection and use of varying models and data through the autonomous system.

2. Redress - adversely affected individuals should have clear and understandable opportunities to seek redress.

3. Explainability - algorithmic decisions and the data supporting them should be available to affected users in clear, non-technical terms.

4. Auditability - third parties should be reasonably able to independently verify models, algorithms, data, and decisions from autonomous analytic systems, including the provenance and handling of data used to train the system.

5. Accuracy and Fairness - algorithmic decisions should not create discriminatory or unjust impacts on vulnerable populations.

II. NATIONAL PRIVACY LEGISLATION

We urge the Administration to support the enactment of comprehensive federal privacy legislation that includes a uniform nationwide data breach notification, and is compatible with data protection and privacy laws in major global markets.

Privacy laws in the United States are disparate, sector-based and not easily reconciled with the laws of other jurisdictions. Navigating the complicated regulatory framework created by the various federal statutes and state laws is costly and time-consuming. The absence of a comprehensive federal privacy law makes it difficult for businesses to comply with the laws of each jurisdiction and can stymie economic development and efficient world trade, particularly as the world continues to grow increasingly dependent on technology, data and cross border commerce.

The lack of a cohesive legal framework governing data collection and protection practices of various entities, including telecommunications and internet services companies, retail merchants, marketing firms, data collectors and U.S. and State government agencies is reaching a breaking point. States are passing their own privacy legislation, started with the passage of the California Consumer Privacy Act (as amended by the California Privacy Rights Act) followed by the passage of the Virginia Consumer Data Protection Act, with privacy bills proposed or being

considered in other states, including Pennsylvania and North Carolina. While these state laws are based on common privacy principles, they are not harmonized in their definitions nor requirements. A national company with consumers in all 50 states will have a nearly insurmountable burden in navigating the disparate state laws.

A. Uniform Data Breach Notification Requirements

States already have state specific notification requirements in event of a data breach. A company that uses, transmits or stores certain personal information must do a variety of things when that company has a breach: assess the situation, contain the harm/breach, notify authorities and, depending on the type and extent of information concerned, notify the affected individuals. A breach or incident is generally defined as unauthorized access to an individual's personal information or the possibility of such access.

The precise definition of the personal information, who needs to be notified, within what time-frame and other measures are all determined by individual state laws. Conducting a state-by-state assessment is costly and burdensome to the affected entity and can have a detrimental impact on the affected individuals.

B. Compatibility with Data Protection Laws in Major Markets

Lack of a cohesive federal privacy framework also impacts trans-Atlantic commerce, with economic consequences for any US company that markets or conducts business abroad, particularly in the EU. The European Union's General Data Protection Regulation ("GDPR") became effective in May 2018, and has a far reach. Under the GDPR, cross border transfer of data to jurisdictions where the national laws are not deemed to provide adequate level of data protection is generally prohibited, unless one of the specific mechanisms are put in place by the company. The current patchwork of privacy laws in the US are not deemed to provide 'adequate level of data protection', thus requiring companies that need to move data across jurisdictions for conducting their business to put in place mechanisms which can be cumbersome and costly.

III. CYBERSECURITY AND CYBER OPERATIONS: ESTABLISHING NORMS

We urge the new administration to continue the United States governmental efforts to advance worldwide cybersecurity and develop global norms of cyber operations that observe obligations under international laws and conventions.

The increasing number of brazen cyber operations involving malicious use of Information Communication Technology capabilities (ICTs), by State and non-State actors, pose a great threat to critical infrastructure that provides services to the public, supports the functioning of economic activity, and increasingly permeates all facets of our lives. To this end, we urge you to work with private sector stakeholders as well as governmental experts to build trust and security in cyberspace and consensus among States on norms of responsible behavior in cyber operations.

Private sector stakeholders include private providers of networks and internet functionality, financial institutions, hardware manufacturers, software providers, and other developers and providers of ITCs. These various stakeholders around the globe have extensive experience in

dealing with cyberattacks and often bear the brunt of attacks by State and/or criminal actors, and many have signed on to The Cybersecurity Tech Accord. As the speed of change in cyberspace—including cyberwarfare, cyberespionage and cybercrime— vastly outstrips the speed of most governmental institutions to identify and counter such threats, it is important that cyber norms be developed in coordination with those who have firsthand and varied experience in this realm.

A number of international forums and academic groups have been convened and continue to look at the application of existing international laws and conventions to cyber operations and cyberwarfare, identify gaps and formulate recommendations on norms, e.g., UN Group of Governmental Experts, Global Commission on the Stability of Cyberspace. Continued and enhanced participation by representatives from the US Government in these efforts would greatly advance the development and shaping of much needed global norms.

A. Consequences for Cybercrimes, Cyberattacks

Among areas in need of further development are norms concerning prosecution of those engaging in cybercrimes, including norms around cooperation, exchange of information and assistance among States, law enforcement and the private sector. Such norms might be addressed globally by trusted institutions that transcend any particular government or private interests. A global trusted institution model would maximize efficiencies and ensure that government agencies, private enterprise and other stakeholders have access to relevant information in a timely and efficient manner.

We recognize that a significant challenge with respect to cybercrimes is that some participants in a global forum might also be responsible, directly or indirectly, for the very cyber activities that the forum is intended to combat. We urge further study of the risk factors that might escalate a cyber skirmish into a war in the physical world, and the development of norms on acceptable responses and invocation of countermeasures as permissible under international law.

B. Cybersecurity as Part of Physical Infrastructure

We applaud the Administration's spending proposal on infrastructure upgrades, and urge continued focus and funding specifically aimed at cybersecurity infrastructure in all infrastructure plans. Physical infrastructure is increasingly dependent on technology and, therefore, on the security of those technological functions. Strengthening U.S. cybersecurity infrastructure is critical to maintaining all aspects of our lives increasingly dependent on technology, including transit and many facets of transportation, drinking water, waste management, schools, energy, commerce and communication.

Technology, Cyber & Privacy Law Committee
Sylvia Khatcherian, Chair

May 2021

Contact
Mary Margulis-Ohnuma, Policy Counsel | 212.382.6767 | mmargulis-ohnuma@nycbar.org
Elizabeth Kocienda, Director of Advocacy | 212.382.4788 | ekocienda@nycbar.org