



---

**The Journal of Robotics,  
Artificial Intelligence & Law**

---

Editor's Note: The Future  
Victoria Prussen Spears

Flying Cars: Are We Ready for Them?  
Elaine D. Solomon

**U.S. AI Regulation Guide: Legislative Overview and Practical Considerations**  
Yoon Chae

Artificial Intelligence in Healthcare: Can Regulation Catch Up with Innovation?  
Alaap B. Shah

New York and New Jersey Make an Early Effort to Regulate Artificial Intelligence  
Marc S. Martin, Charlyn L. Ho, and Michael A. Sherling

Artificial Intelligence and the Fair Housing Act: Algorithms Under Attack?  
William T. Gordon, Katherine Kirkpatrick, and Katherine Mueller

Angel Investing Lessons: The First Mover Disadvantage  
Paul A. Jones

The Convertible Debt Valuation Cap: The Trigger Financing Investor Perspective  
Paul A. Jones

Big News for Small Mobility: Germany Opens Up to E-Scooters  
Andreas Grünwald, Christoph Nüßing, and Theresa Oehm

Everything Is Not *Terminator*: AI Issues Raised by the California Consumer Privacy Act  
John Frank Weaver

- 5 Editor’s Note: The Future**  
Victoria Prussen Spears
- 9 Flying Cars: Are We Ready for Them?**  
Elaine D. Solomon
- 17 U.S. AI Regulation Guide: Legislative Overview and Practical Considerations**  
Yoon Chae
- 41 Artificial Intelligence in Healthcare: Can Regulation Catch Up with Innovation?**  
Alaap B. Shah
- 47 New York and New Jersey Make an Early Effort to Regulate Artificial Intelligence**  
Marc S. Martin, Charlyn L. Ho, and Michael A. Sherling
- 53 Artificial Intelligence and the Fair Housing Act: Algorithms Under Attack?**  
William T. Gordon, Katherine Kirkpatrick, and Katherine Mueller
- 57 Angel Investing Lessons: The First Mover Disadvantage**  
Paul A. Jones
- 63 The Convertible Debt Valuation Cap: The Trigger Financing Investor Perspective**  
Paul A. Jones
- 69 Big News for Small Mobility: Germany Opens Up to E-Scooters**  
Andreas Grünwald, Christoph Nüßing, and Theresa Oehm
- 73 Everything Is Not *Terminator*: AI Issues Raised by the California Consumer Privacy Act**  
John Frank Weaver

**EDITOR-IN-CHIEF**

**Steven A. Meyerowitz**

*President, Meyerowitz Communications Inc.*

**EDITOR**

**Victoria Prussen Spears**

*Senior Vice President, Meyerowitz Communications Inc.*

**BOARD OF EDITORS**

**Miranda Cole**

*Partner, Covington & Burling LLP*

**Kathryn DeBord**

*Partner & Chief Innovation Officer, Bryan Cave LLP*

**Melody Drummond Hansen**

*Partner, O'Melveny & Myers LLP*

**Paul B. Keller**

*Partner, Norton Rose Fulbright US LLP*

**Garry G. Mathiason**

*Shareholder, Littler Mendelson P.C.*

**Elaine D. Solomon**

*Partner, Blank Rome LLP*

**Linda J. Thayer**

*Partner, Finnegan, Henderson, Farabow, Garrett & Dunner LLP*

**Mercedes K. Tunstall**

*Partner, Pillsbury Winthrop Shaw Pittman LLP*

**Edward J. Walters**

*Chief Executive Officer, Fastcase Inc.*

**John Frank Weaver**

*Attorney, McLane Middleton, Professional Association*

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at \$495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2020 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at [support@fastcase.com](mailto:support@fastcase.com).

Publishing Staff

Publisher: Morgan Morrisette Wright

Journal Designer: Sharon D. Ray

Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Copyright © 2020 Full Court Press, an imprint of Fastcase, Inc.

All Rights Reserved.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004

<https://www.fastcase.com/>

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

## Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc.,  
26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@  
meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

### QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please call:

Morgan Morrisette Wright, Publisher, Full Court Press at mwright@fastcase.com  
or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service  
Available 8am–8pm Eastern Time  
866.773.2782 (phone)  
support@fastcase.com (email)

Sales  
202.999.4777 (phone)  
sales@fastcase.com (email)  
ISSN 2575-5633 (print)  
ISSN 2575-5617 (online)

# U.S. AI Regulation Guide: Legislative Overview and Practical Considerations

Yoon Chae\*





*This article discusses the state of U.S. regulation of artificial intelligence (“AI”), covering legislative instruments directed to algorithmic accountability, the use of facial recognition technology and associated data, and promoting “transparency” when using AI, as well as pending federal bills on general governance or research issues for AI, among other things. The author also discusses practical considerations when using AI for businesses and in-house counsel.*

---

Regulation of artificial intelligence (“AI”) is still in its infancy, perhaps with the exception of autonomous vehicles, which have seen the most legislative activities worldwide.<sup>1</sup> Many countries have just issued their national plans, guidelines, or codes—which often highlight essential principles for developing ethical AI—without having passed much substantive law; notable examples include the European Parliament’s resolution on Civil Law Rules on Robotics (February 2017), the European Union’s Ethics Guidelines for Trustworthy AI (April 2019), and OECD’s Council Recommendation on Artificial Intelligence (May 2019).<sup>2</sup> The time may now be ripe, according to certain experts, to tackle the associated challenges in transitioning from these general principles to actual legislation in order to provide the necessary regulatory frameworks that safeguard those principles.<sup>3</sup>

Much of the recent development in filling the legal void that exists for AI governance is surprisingly coming from the United States, which, with the exception of three AI reports issued by the Obama administration,<sup>4</sup> has been relatively inactive with AI regulation until last year. In 2015–2016, for example, the 114th Congress saw only two bills containing the term “artificial intelligence,” which increased to 42 bills with the 115th Congress (2017–2018) and to 51 bills for the current, 116th, Congress, as of early November 2019. Similar trends are observed at the state and city levels as well. California, for instance, had 0 bills on “artificial intelligence” two

legislative sessions ago (2015–2016), five bills during the last term (2017–2018), and 13 bills for the current legislature (2019–2020). Other than regulatory instruments on autonomous vehicles<sup>5</sup>—which are beyond the scope of this article—most of the lawmaking on AI, automated systems, and their underlying technologies have been in the following areas:

 Policy	 Algorithmic Accountability	 Facial Recognition Technology	 Transparency
<p>★[Fed] Maintaining Am. Leadership in AI (Feb. 2019)</p> <p>-----</p> <p>[Fed] H.R. Res. 153 (Feb. 2019)</p> <p>-----</p> <p>[Fed / NIST] US Leadership in AI (Aug. 2019)</p> <p>-----</p> <p>★[Cal] Res. on 23 Asilomar AI Principles (Sep. 2018)</p>	<p>[Fed] Algorithmic Accountability Act (Apr. 2019)</p> <p>-----</p> <p>[N.J.] New Jersey Algorithmic Accountability Act (May 2019)</p> <p>-----</p> <p>[Cal] AI: Reporting (Feb. 2019)</p> <p>-----</p> <p>[Wash] Guidelines for Gov't Procurement and Use of Auto. Decision Systems (Jan. 2019)</p> <p>-----</p> <p>★ NYC (Jan 2018)</p>	<p>[Fed] Commercial Facial Recognition Privacy Act (Mar. 2019)</p> <p>-----</p> <p>[Fed] FACE Protection Act (July 2019)</p> <p>-----</p> <p>[Fed] No Biometric Barriers to Housing Act (July 2019)</p> <p>-----</p> <p>[Cal] Body Camera Account. Act (Feb. 2019)</p> <p>-----</p> <p>[Cal] Privacy: facial recog. tech. (Feb. 2019)</p> <p>-----</p> <p>[Mass] An Act establishing a moratorium on face recognition (Jan. 2019)</p> <p>-----</p> <p>[NY] Prohibits Use of Facial Recog. Sys. (May 2019)</p> <p>-----</p> <p>★ SF, Somerville, Oakland (June, July 2019)</p>	<p>★[Cal] B.O.T Act – SB 1001 (effect. July 2019)</p> <p>-----</p> <p>[Cal] Anti-Eavesdropping Act (Assemb. May 2019)</p> <p>-----</p> <p>★[Ill] AI Video Interview Act – H.B. 2557 (eff. Jan. 2020)</p>
<p><b>Other</b></p> <p>[Fed] FUTURE of AI Act (Dec. 2017)    [Fed] AI JOBS Act (Jan. 2019)    [Fed] GrAITR Act (Apr. 2019)    [Fed] AI in Government Act (May 2019)    [Fed] AI Initiative Act (May 2019)</p>			

The first area is what this article labels as “policy,” and it includes documents like executive orders, resolutions, and plans that reflect the U.S. government’s policies on AI regulation. The second category covers legislative instruments directed to algorithmic accountability, likely reflecting the governments’ response to recently publicized concerns of algorithmic bias and discrimination. The third is on the rapidly growing body of law that governs the use of facial recognition technology and associated data. The fourth area is labeled as “transparency,” and it includes those that are primarily directed to promoting transparency when it comes to the use of AI in different contexts. The last category is designated as “other,” and comprises pending federal bills on general governance or research issues for AI, among other things.<sup>6</sup>

## Policy

---

### The Executive Order and the NIST Plan

President Trump issued the Executive Order on Maintaining American Leadership in Artificial Intelligence (No. 13,859) on February 11, 2019.<sup>7</sup> The Order explains that the federal government plays an important role in facilitating AI research and development (“R&D”) and in promoting trust, training people for a changing workforce, and protecting national interests, security, and values.<sup>8</sup> It launched the “American AI Initiative,” guided by five principles:

- (1) Driving technological breakthroughs;
- (2) Driving the development of appropriate technical standards;
- (3) Training workers with the skills to develop and apply AI technologies;
- (4) Protecting American values, including civil liberties and privacy, and fostering public trust and confidence in AI technologies; and
- (5) Protecting U.S. technological advantage in AI, while promoting an international environment that supports innovation.<sup>9</sup>

The Order requires all executive departments and agencies that develop or deploy AI, among other things, to adhere to six strategic objectives that generally align with the five principles listed above.<sup>10</sup> An objective that is particularly worth noting is the one directed to ensuring that “technical standards minimize vulnerability to attacks from malicious actors and reflect Federal priorities for innovation, public trust, and public confidence in systems that use AI technologies” and highlighting the need to “develop international standards to promote and protect those priorities.”<sup>11</sup> The Order tasks the National Institute of Standards and Technology (“NIST”) of the U.S. Department of Commerce to create a plan for federal engagement in the development of technical standards to support reliable, robust, and trustworthy AI systems.<sup>12</sup>

In response, in August 2019, NIST issued its Plan for Federal Engagement in Developing Technical Standards.<sup>13</sup> It identifies nine areas of technical AI standards that are available or being developed, among which “[s]tandardization of AI safety, risk management, and



some aspects of trustworthiness such as explainability or security, are in their formative stages and especially would benefit from research to provide a strong technical basis for development.”<sup>14</sup> The Plan also identifies three areas of “non-technical” AI standards that inform policy decisions, such as “societal and ethical considerations,” “governance,” and “privacy.”<sup>15</sup>

The Executive Order and the release of the NIST Plan may be indications that federal governance of AI under the Trump administration favors or values a standards-driven approach,<sup>16</sup> and they are significant in that they mark the federal government’s first major efforts in providing clarity and guidance to agencies that are looking to adopt AI.<sup>17</sup> NIST also has plans for more guidance in the near future, with plans to seek public comment on recommendations on confronting adversarial machine learning, as well as to seek public feedback on upcoming standards for explainable AI, which can further inform businesses on how to address those issues.<sup>18</sup>

### House Resolution 153

Shortly after the Executive Order, the House of Representatives introduced House Resolution 153 on Supporting the Development of Guidelines for Ethical Development of Artificial Intelligence on February 27, 2019. The Resolution seeks to strike a balance between promoting AI’s “potential to enhance wellbeing, foster economic growth, and improve care and services for many people” with the need for its “safe, responsible, and democratic development.”<sup>19</sup> It provides ten aims for achieving that balance, including “[t]ransparency and explainability,” “[i]nformation privacy and the protection of one’s personal data,” “[a]ccountability and oversight for all automated decisionmaking,” “[a]ccess and fairness regarding technological services and benefits,” and “[s]afety, security, and control of AI systems now and in the future,” among other things.<sup>20</sup> Although the Resolution has not yet been adopted, it highlights some of the same principles that are emphasized by other governments and international organizations for developing ethical and trustworthy AI.

### California’s Assembly Concurrent Resolution 215

Several months prior to the federal House Resolution 153, California unanimously adopted Assembly Concurrent Resolution

215 on September 7, 2018.<sup>21</sup> The Resolution expresses legislative support for using the 23 Asilomar AI Principles as the “guiding values for the development of artificial intelligence and of related public policy.”<sup>22</sup> The Principles were developed in conjunction with a 2017 conference in Asilomar, California, where experts from various disciplines met to establish the core principles for managing responsible development of AI.<sup>23</sup> As of November 12, 2019, the Principles have been signed and endorsed by 5,030 of the world’s leading AI researchers and leaders in government, industry, and academia, including Stephen Hawking and Elon Musk.<sup>24</sup>

The Resolution identifies the need for developing AI in a manner that “ensures security, reliability, and consonance with human values,” and looks to the Principles for guidance, which are categorized into “research issues,” “ethics and values,” and “longer-term issues” that are designed to promote safe and beneficial development of AI.<sup>25</sup> The Principles listed under ethics and values include safety, failure transparency, judicial transparency, responsibility, value alignment, human values, personal privacy, liberty and privacy, and human control, among other themes.<sup>26</sup> Since the adoption of ACR 215, California has been significantly more legislative active on governing AI.

## Algorithmic Accountability

---

### Algorithmic Accountability Act

Senate and House bills for the Algorithmic Accountability Act (S. 1108, H.R. 2231) were introduced in Congress on April 10, 2019,<sup>27</sup> likely in response to recently publicized reports on the risks of AI’s biased outcomes. In the words of one of the sponsors, Senator Wyden, the intention behind the bill was to require “companies to regularly evaluate their tools for accuracy, fairness, bias, and discrimination.”<sup>28</sup>

If the bill were to get enacted, it would require covered entities to conduct “impact assessments” on their “high-risk” automated decision systems in order to evaluate the impacts of the system’s design process and training data on “*accuracy, fairness, bias, discrimination, privacy, and security.*”<sup>29</sup> The Act also provides that the impact assessments should be performed “with external third parties, including independent auditors and independent technology experts” when “reasonably” possible.<sup>30</sup> Businesses would then be

required to “reasonably address” any identified issues in a “timely manner.”<sup>31</sup>

“Automated decision system” is defined broadly as “any computational process, including one derived from *machine learning*, statistics, or other data processing or *artificial intelligence techniques*, that makes a decision or facilitates human decision making, that impacts consumers.”<sup>32</sup> Covered entities would include companies that:

- (1) Make \$50 million or more per year;
- (2) Hold data for over one million consumers or consumer devices; or
- (3) Act as data brokers that buy and sell personal information.<sup>33</sup>

The Algorithmic Accountability Act expressly provides that it would *not* preempt any state law,<sup>34</sup> which means that businesses would need to remain vigilant on keeping up with any state law development on similar subject matter. The bill also does *not* provide for a private right of action, nor extraterritorial jurisdiction.<sup>35</sup> Instead, it would be enforced by the Federal Trade Commission (“FTC”) under Section 5 of the Federal Trade Commission Act on deceptive and unfair acts and practices, or via civil suits brought by the affected state’s attorney general.<sup>36</sup>

Although the bill’s future is uncertain, it is significant in that it is the first federal legislative effort to regulate AI across industries,<sup>37</sup> with broad proposed protections that mirror the General Data Protection Regulation (“GDPR”) in several ways.<sup>38</sup> The bill is also significant in that it may be a harbinger of the laws to come,<sup>39</sup> and in fact, some of this movement is already gaining momentum at the state and city levels.

## New Jersey’s Algorithmic Accountability Act

Just a month after the federal Algorithmic Accountability Act was introduced, New Jersey introduced a similar bill, A.B. 5430, titled “New Jersey Algorithmic Accountability Act,” on May 20, 2019.<sup>40</sup> Like the federal counterpart, the bill requires covered entities to conduct impact assessments on “high-risk” automated decisions systems and information systems.<sup>41</sup>

“Automated decision system impact assessment” requires an evaluation of the system’s development process, including the

design and training data, for impacts on “accuracy, fairness, bias, discrimination, privacy, and security,” and must include “a detailed description of the best practices used to minimize the risks” and a “cost-benefit analysis,” among other things.<sup>42</sup> The bill also requires the covered entities to work with *independent third parties*, record any *bias* or threat to the security of consumer’s personally identifiable information discovered through the impact assessments, and provide any other information that is required by the Director of the Division of Consumer Affairs in the Department of Law and Public Safety.<sup>43</sup>

The bill is significant in that it mirrors the federal Algorithmic Accountability Act, with a broad scope and large potential impact on businesses.

## Other States’ and Cities’ Regulation of AI Bias

Although New Jersey appears to be the only state so far to have introduced legislation mirroring the federal Algorithmic Accountability Act, there is also a growing trend toward other state and city governments considering laws that regulate algorithmic bias in the context of AI procurement and use by government entities.<sup>44</sup> In early 2018, for example, New York City enacted the first algorithm accountability law—“A Local Law in relation to automated decision systems used by agencies” (Int. No. 1696-2017)—in the United States.<sup>45</sup> In January 2019, Washington State introduced bills, S.B. 5527 and H.B. 1655, with GDPR-like prohibitions against algorithmic discriminations, although likewise limited to government’s procurement and use.<sup>46</sup> In February 2019, California introduced a bill, S.B. 444, where businesses that rely on AI for delivery of a product to a public entity would be required to make certain disclosures to the public entity regarding “the steps that it has taken to reduce the bias inherent in the artificial intelligence system.”<sup>47</sup>

## Facial Recognition Technology

---

### Commercial Facial Recognition Privacy Act

The Commercial Facial Recognition Privacy Act (S. 847) was introduced on March 14, 2019,<sup>48</sup> to strengthen consumer protections and increase transparency, and in the words of one of the

sponsors, Senator Blunt, to make sure “that people are given the information and [] the control over how their data is shared” when it comes to facial recognition.<sup>49</sup>

If enacted, the bill would generally prohibit covered entities from using “facial recognition technology to collect facial recognition data” of end users without providing *notice* and obtaining their *consent*.<sup>50</sup> “Covered entities” is broadly defined and would include any non-governmental entity that “collects, stores, or processes facial recognition data.”<sup>51</sup> This definition would therefore seemingly include entities like app operators that collect facial data, businesses that use the technology on their premises, and outside vendors that process such data for the original data collectors.<sup>52</sup> Facial recognition data is tied to personal information (i.e., “unique personal identification of a specific individual”), but may also include pseudonymized information (i.e., where “a unique, persistent identifier” is assigned).<sup>53</sup>

Covered entities would also be prohibited from using the technology to *discriminate* against the consumers, from *repurposing* the facial data, or from *sharing* such data with third parties without obtaining further consent from the end users.<sup>54</sup> The covered entities would also not be allowed to condition service of the technology on the consumer’s consent to waive privacy rights when the use of facial recognition technology is not necessary for that service.<sup>55</sup> In an effort to provide more oversight, the bill also requires the covered entities to conduct *meaningful human review* before making any final decision based on the output of the technology if it can result in a reasonably foreseeable harm or be “highly offensive” to a reasonable end user.<sup>56</sup> If the technology is made “available as an online service,” then the covered entity would additionally be required to make available an API to enable at least one third party to conduct reasonable independent tests for accuracy and bias.<sup>57</sup>

The bill, however, contains some notable exceptions. For example, the bill exempts “security applications” that use the technology for “loss prevention” or “to detect or prevent criminal activity.”<sup>58</sup> The bill also exempts products or services “designed for personal file management or photo or video sorting or storage if the facial recognition technology is not used for unique personal identification of a specific individual,” involves “identification of public figures for journalistic media created for public interest,” “involves identification of public figures in copyrighted material,” or is used in an emergency.<sup>59</sup>

The law would *not* preempt state laws, except to the extent such regulations are “inconsistent” with the provisions of the bill.<sup>60</sup> If passed, the act would thus likely not preempt stricter state laws, such as Illinois’s Biometric Information Privacy Act (“BIPA”) or other state biometric information privacy laws in Texas and Washington.<sup>61</sup> The bill does *not* provide for a private right of action, and would instead be enforced by the FTC or via civil suits brought by the affected state’s attorney general.<sup>62</sup>

This bill is worth monitoring as it makes its way through Congress given that it is a bipartisan bill<sup>63</sup> with a narrow scope that has received early conceptual support from several technology companies.<sup>64</sup> Again, like the Algorithmic Accountability Act, the bill mirrors certain aspects of the GDPR, such as the differentiation between processors and controllers.<sup>65</sup> Numerous commentators believe that this bill signals the types of impending laws on facial recognition technology. In fact, in 2019, lawmakers in at least 10 states have introduced bills to ban or delay the use of facial recognition technology by government agencies or businesses.<sup>66</sup>

## Other Federal Bills on Facial Recognition Technology

Since the introduction of the Commercial Facial Recognition Privacy Act, Congress has seen an increasing number of bills on facial recognition technology. For example, H.R. 3875 was introduced on July 22, 2019, to “prohibit Federal funding from being used for the purchase or use of facial recognition technology.”<sup>67</sup>

On July 25, 2019, the Facial, Analysis, Comparison, and Evaluation (“FACE”) Protection Act of 2019 (H.R. 4021) was introduced to prohibit a federal agency from applying “facial recognition technology to any photo identification issued by a State or the Federal Government or any other photograph otherwise in the possession of a State or the Federal Government unless the agency has obtained a Federal court order determining that there is probable cause for the application of such technology.”<sup>68</sup>

On the same day, another bill on the No Biometric Barriers to Housing Act of 2019 (H.R. 4008) was introduced to “prohibit the use of biometric recognition technology in certain federally assisted dwelling units.”<sup>69</sup> If enacted, it would also require the Secretary of Housing and Urban Development (“HUD”) to submit a report describing “the impact of such technology on the residents

of such covered federally assisted rental dwelling units” and the potential impacts on vulnerable communities of additional usage of such technology in covered federally assisted rental dwelling units, including impacts on “resident privacy, civil rights, and fair housing,” among other required details.<sup>70</sup> These trends may indicate the federal government’s increasing willingness to regulate the use of facial recognition technology.

## State and City Regulation of Facial Recognition Technology

There has been a wave of state and local laws and bills on the procurement and use of facial recognition technology. For example, California introduced a bill, A.B. 1215, on February 21, 2019, which would prohibit law enforcement agencies and officials from using any “biometric surveillance system,” including facial recognition technology, in connection with an officer camera or data collected by the camera.<sup>71</sup> On the same day, another bill, A.B. 1281, was introduced in California, which would require California businesses that use facial recognition technology to disclose such usage on a physical sign that is “clear and conspicuous at the entrance of every location that uses facial recognition technology.”<sup>72</sup>

Senate Bill 1385 was introduced in Massachusetts on January 22, 2019, to establish a moratorium on the use of face recognition systems by state and local law enforcement, and Senate Bill 5687 was introduced in New York on May 13, 2019, to propose a temporary stop to the use of facial recognition technology in public schools.<sup>73</sup> Similarly, companion bills, S.B. 5528 and H.B. 1654, were introduced in Washington in January 2019, concerning the procurement and use of facial recognition technology by government entities and privacy rights relating to facial recognition technology.<sup>74</sup>

As for cities, San Francisco and Oakland, California, and Somerville, Massachusetts, passed ordinances this summer to ban the use of facial recognition software by the police and other government agencies.<sup>75</sup>

On a related note, there has also been a resurgence of biometric privacy bills being introduced in state legislatures. Although the Illinois Biometric Information Privacy Act and Texas’s law on the Capture or Use of Biometric Identifier have been around since 2008 and 2009,<sup>76</sup> other states have recently started enacting or introducing privacy laws on biometric identifiers, such as

Washington's enactment of the bill on Biometric Identifiers in July 2017,<sup>77</sup> California's enactment of the California Consumer Privacy Act ("CCPA") in June 2018 (to become effective in January 2020),<sup>78</sup> and Massachusetts's introduction of a bill, S. 120, on An Act relative to consumer data privacy in January 2019,<sup>79</sup> among others.

The legislative trends on facial recognition technology and associated data, combined with the resurgence of biometric privacy laws, likely highlight the governments' increasing attention to the use of biometric and facial data.

## Transparency

---

### California's Bolstering Online Transparency Act

Moving on to laws directed to improving transparency, California's Bolstering Online Transparency ("B.O.T.") Act (S.B. 1001) came into effect this July after being enacted last year.<sup>80</sup> The law is the first of its kind,<sup>81</sup> and it prohibits the use of "a bot to communicate or interact with another person in California online, with the intent to mislead the other person about its artificial identity" for *commercial* or *political* purposes.<sup>82</sup> The law defines a "bot" as "an automated online account where all or substantially all of the actions or posts of that account are not the result of a person."<sup>83</sup>

There is a safe harbor exemption, however, if the bot first discloses its identity in a "clear, conspicuous, and reasonably designed" manner.<sup>84</sup> Further, the B.O.T. Act applies only to bot communications deployed via public-facing internet websites, web applications, and digital applications, including social networks or publications,<sup>85</sup> and it expressly provides that *no* duty is imposed on "service providers of online platforms."<sup>86</sup> The statute does not specify the method of enforcement, but given that it is a part of California's Unfair Competition Law, it would likely be enforced by the state attorney general via fines of up to \$2,500 per violation.<sup>87</sup>

The bill also went through significant amendments, which, according to the Electronic Frontier Foundation ("EFF"), were the results of its involvement.<sup>88</sup> The bill's initial definition of a "bot," for example, covered most or all bots, but was amended to focus on bots used for a commercial or political purpose, and the bill's earlier requirement that platforms create a notice and takedown system for suspected bots was also removed as a result of the amendments.<sup>89</sup>



## California's Anti-Eavesdropping Act

California's Anti-Eavesdropping Act (A.B. 1395) recently passed the Assembly and is now pending in the State Senate.<sup>90</sup> If enacted, it would prohibit manufacturers of smart speakers from installing devices "without prominently informing" the user.<sup>91</sup> It would also prohibit any recording or transcription that "qualifies as personal information or is not deidentified" from being used for advertising purposes, shared or sold to third parties, or retained without the user's affirmative consent.<sup>92</sup> Under the bill, a manufacturer would "only be liable for functionality provided at the time of the original sale of a connected television or smart speaker device and shall not be liable for functionality provided by applications that the user chooses to use in the cloud or are downloaded and installed by a user."<sup>93</sup>

## Illinois's Artificial Intelligence Video Interview Act

Illinois's Artificial Intelligence Video Interview Act (H.B. 2557) was signed on August 9, 2019, and will become effective in January 2020.<sup>94</sup> It governs an employer's ability to use AI analysis on video interviews by requiring the employer to:

- (1) Notify each applicant before the interview that AI may be used to analyze the video interview;
- (2) Provide the applicant with information on how the AI works; and
- (3) Obtain consent from the applicant to be evaluated by the AI program before the interview.<sup>95</sup>

The Act also limits sharing of the videos—only "with persons whose expertise or technology is necessary in order to evaluate an applicant's fitness for a position"—and requires deletion of an applicant's interview(s) within 30 days after receipt of any request from the applicant.<sup>96</sup> The Act does not include provisions on a private right of action.<sup>97</sup>

The Act is significant in that it is the first U.S. law to specifically regulate artificial intelligence as an evaluation tool on applicant videos.<sup>98</sup>

## Other Federal Bills on AI

---

There are several other pending federal bills on AI, the earliest being S. 2217 and H.R. 4625 on the FUTURE of Artificial Intelligence Act of 2017, introduced on December 12, 2017.<sup>99</sup> Although never passed, it would have required the Department of Commerce to establish a new committee to advise on topics related to the development and implementation of AI.<sup>100</sup>

Further, H.R. 2202 on the Growing Artificial Intelligence Through Research (“GrAITR”) Act, introduced on April 10, 2019, and S. 1558 on the Artificial Intelligence Initiative Act (“AI-IA”), introduced on May 21, 2019, are primarily directed to establishing a coordinated federal initiative to accelerate research and development on AI.<sup>101</sup> Several components of the proposed initiative are directed to eliminating AI *bias*. For example, the bills provide that the president shall establish a National AI Research and Development Initiative, where the responsibilities would include strengthening research and development with respect to AI by “identifying and minimizing inappropriate bias in data sets algorithms, and other aspects of artificial intelligence.”<sup>102</sup> The bills also seek to “establish and implement a research and education program on” AI and AI engineering, where the program would need to “continue to support interdisciplinary research” on “algorithm accountability,” “minimization of inappropriate bias in training data sets or algorithmic feature selection,” and “societal and ethical implications” of AI, among other things.<sup>103</sup>

Related bills, H.R. 2575 and S. 1363, on the AI in Government Act were re-introduced on May 8, 2019, and are generally directed to establishing an AI Center of Excellence.<sup>104</sup> The Act also discusses AI bias in some detail—for example, responsibilities of the AI Center of Excellence would include studying “economic, policy, legal, and ethical challenges and implications related to the use of artificial intelligence by the Federal Government” and establishing “best practices for identifying, assessing, and mitigating any bias on the basis of any classification protected under Federal non-discrimination laws or other negative unintended consequence stemming from the use of artificial intelligence systems.”<sup>105</sup>

Many believe that these federal bills reflect the government’s heightened awareness of the risks associated with AI bias.

## Practical Considerations for Businesses and In-House Counsel

---

### Internal Governance Structures and Measures

It would be helpful for businesses to establish and continually improve on its internal governance structures and measures to promote robust oversight of AI.<sup>106</sup> Having such infrastructure reflect the key principles highlighted in the various regulatory instruments, such as transparency, fairness (no bias/discrimination), human oversight, accountability, and safety, among other things, will likely facilitate consistency and compliance with future laws on AI.

For their internal governance structures, businesses may consider establishing clear roles and responsibilities for the ethical deployment of AI and having sound risk management and internal controls.<sup>107</sup> Such governance structures may also benefit from careful consideration of the “susceptibility of data” and assessment of whether using such data would promote fairness for the consumers.<sup>108</sup> Further, from a broader organizational perspective, helping develop and establish diverse, multidisciplinary teams to build and oversee such internal measures can provide an additional layer of protection against potential biases that can permeate algorithms and datasets.<sup>109</sup>

It would also be useful to provide sufficient training on the various risks of AI and its underlying technologies, such as the risks of inherent algorithmic bias or of discrimination stemming from the use of facial recognition technology. Such training should be provided not just for the legal or policy members, but also to the engineers, coders, and product managers that are engaged in AI development and data processing, so as to promote the culture of fair and unbiased AI. Well-documented training processes and internal guidelines can also provide more transparency to regulators.

### External Resources

In addition to employing any internally developed measures, strategically considered use of effective external resources may help safeguard against some of the risks that can arise from the use of

AI, as well as bring objectivity and transparency to the businesses' AI deployment.

When it comes to algorithmic bias, for example, businesses can consider employing AI tools that generate metrics for evaluating whether there are unintended biases in algorithmic models. They can also consider using external open source AI frameworks, such as IBM's AI Fairness 360, which implements bias metrics and mitigation algorithms,<sup>110</sup> or employing DARPA's Explainable Artificial Intelligence ("XAI") program that provides a toolkit library for developing future explainable AI systems.<sup>111</sup> To minimize potential discrimination from the use of facial recognition technology, businesses can consider using third-party data repositories, such as Canadian Institute for Advanced Research's CIFAR-10, that contain images commonly used to train machine learning and computer vision algorithms.<sup>112</sup>

It is also important for organizations to ensure data quality in the form of "the accuracy of the dataset," "completeness of the dataset," "veracity of the dataset," "relevance of the dataset and the context for data collection," and integrity of the dataset, among other factors.<sup>113</sup> It is also advisable to consider using different datasets for "training, testing, and validation" of an AI model and to periodically review and update the pertinent datasets.<sup>114</sup>

Keeping up with guidelines and best practices being developed by governments, international and non-profit organizations, and private entities can also help inform businesses on implementing their own governance structures and measures. For example, Canada's Algorithmic Impact Assessment questionnaire or AI Now Institute's Algorithmic Accountability Policy Toolkit, which are designed to help assess and mitigate the risks associated with automated decision systems, may be useful resources.<sup>115</sup> The Partnership on AI to Benefit People and Society, which was established to study and formulate best practices on AI technologies, among other things, may provide useful resources for businesses as well.<sup>116</sup>

Such practices may also help satisfy the Algorithmic Accountability Act's and the New Jersey Algorithmic Accountability Act's respective provisions requiring that impact assessments evaluate the relative benefits and costs of the system in light of its purpose, where relevant factors include "data minimization practices."<sup>117</sup> Establishing best practices involving the use of such external tools and datasets can also help satisfy the New Jersey Algorithmic Accountability Act's requirement that covered entities provide "a

detailed description of the best practices used to minimize the risk of the automated decision system” that impacts “accuracy, fairness, bias, discrimination, privacy, and security,” among other things.<sup>118</sup>

## Technical Standards

Using certain AI technical standards as benchmarks and staying up-to-date on their development can help inform businesses on the direction of AI development and safeguard them against future laws. For instance, the ISO (International Organization for Standardization) and the IEC (International Electrotechnical Commission) are developing numerous standards on Artificial Intelligence, including standards on “Overview of trustworthiness in Artificial Intelligence.”<sup>119</sup> IEEE is also developing AI standards under its P7000 series, such as P7001 on “Transparency of Autonomous Systems” and P7010 on “Wellbeing Metrics Standard for Ethical Artificial Intelligence and Autonomous Systems,” which could be helpful for businesses to consider when striving to design trustworthy and transparent AI systems.<sup>120</sup>

For laws on algorithmic accountability (against bias), such as the Algorithmic Accountability Act, reviewing ISO/IEC’s technical standard being developed on “Bias in AI systems and AI aided decision making” and IEEE’s P7003 on “Algorithmic Bias Considerations” could be informative.<sup>121</sup> For laws on facial recognition technology, it could be useful to stay up-to-date on ISO’s standard, JTC 1 SC 37, on Biometrics and IEEE’s P7013 on “Inclusion and Application Standards for Automated Facial Analysis Technology.”<sup>122</sup> For laws directed to promoting transparency, such as California’s B.O.T. Act, some of the relevant technical standards that are being developed include IEEE’s P7008, which governs ethically driven methodologies for autonomous systems that make overt or hidden suggestions or manipulations for influencing the behavior or emotions of a user.<sup>123</sup>

## Evaluation & Audit Systems

Implementing an evaluation or audit system for regularly checking the input data and the generated results, then having appropriate feedback channels for further improvements, can provide more transparency and oversight, while reducing some of AI’s inherent

risks.<sup>124</sup> Organizations can also consider periodically conducting risk impact assessments in order to “continually identify and review risks relevant to their technology solutions, mitigate those risks, and maintain a response plan should mitigation fail.”<sup>125</sup> This would also likely assist the businesses in satisfying the provisions of the algorithmic accountability laws that require covered entities to conduct impact assessments on their automated decision systems. And having third-party algorithm audits can provide even a greater level of transparency and explainability to the public and regulators.

To the extent feasible, providing general information on whether and how an AI product is used by the organization can inspire trust and transparency, which may help comply with legislations focused on transparency, as well as contribute to building greater confidence in and acceptance by the end users of the AI products.<sup>126</sup>

## Notes

---

\* Yoon Chae is an associate in Baker McKenzie’s Dallas office, where he advises on IP and technology matters. He also served as the firm’s first fellow at the World Economic Forum’s Centre for the Fourth Industrial Revolution, where he researched diverse policy issues arising from AI. This article reflects his personal views and not the positions of the firm. He may be reached at [yoona.chae@bakermckenzie.com](mailto:yoona.chae@bakermckenzie.com).

1. See THE LAW LIBRARY OF CONG., REGULATION OF ARTIFICIAL INTELLIGENCE IN SELECTED JURISDICTIONS 1 (2019).

2. Other examples include South Korea’s Mid- to Long-Term Master Plan in Preparation for the Intelligent Information Society (December 2016), the United Kingdom’s National Robotics and Autonomous Systems Strategy (January 2017) and AI in the UK: ready, willing and able? report (April 2018), Canada’s Pan-Canadian Artificial Intelligence Strategy (March 2017), France’s National Artificial Intelligence Research Strategy (March 2017) and National Strategy for AI (March 2019), China’s National AI Strategy (July 2017), United Arab Emirates’ Strategy for Artificial Intelligence (October 2017), Germany’s National Strategy for AI (November 2018), Singapore’s Proposed Model Artificial Intelligence Governance Framework (January 2019), and Japan’s AI Strategies 2019 (June 2019), among many others. Non-governmental organizations have also been active in issuing guidelines and frameworks on ethical development of AI. See, e.g., IEEE, ETHICALLY ALIGNED DESIGN (2017); MICROSOFT, THE FUTURE COMPUTED (2018).

3. Mina Hanna, *We Don’t Need More Guidelines or Frameworks on Ethical AI Use. It’s Time for Regulatory Action*, BRINK NEWS (July 25, 2019), <https://www.brinknews.com/we-dont-need-more-guidelines-or-frameworks>

-on-ethical-ai-use-its-time-for-regulatory-action; cf. WORLD ECON. FORUM, AI GOVERNANCE—A HOLISTIC APPROACH TO IMPLEMENT ETHICS INTO AI 9 (2019) (discussing disadvantages of legislation as regulatory instrument for AI).

4. EXEC. OFFICE OF THE PRESIDENT, ARTIFICIAL INTELLIGENCE, AUTOMATION, AND THE ECONOMY 8 (2016); EXEC. OFFICE OF THE PRESIDENT NAT'L SCI. & TECH. COUNCIL COMM. ON TECH., PREPARING FOR THE FUTURE OF ARTIFICIAL INTELLIGENCE (2016); NETWORKING & INFO. TECH. RESEARCH & DEV. SUBCOMM., EXEC. OFFICE OF THE PRESIDENT NAT'L SCI. AND TECH. COUNCIL, THE NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH AND DEVELOPMENT STRATEGIC PLAN (2016).

5. This article does not cover trends in autonomous driving legislation, which merit preparation of a separate article. It also does not cover the Filter Bubble Transparency Act due to timing of the article's submission.

6. The chart is not provided as an exhaustive list of laws and bills under the different categories, but is meant to merely provide a substantive sampling of the different legislative instruments. A red star on the chart indicates that the bill has been enacted.

7. Exec. Order No. 13,859, 3 C.F.R. 3967 [hereinafter "Executive Order"].

8. Executive Order, *supra* note 7, at § 1.

9. *Id.*

10. *AI Policy—United States*, FUTURE OF LIFE, <https://futureoflife.org/ai-policy-united-states/> (last visited Sept. 23, 2019).

11. Executive Order, *supra* note 7, at § 2. The other five objectives are: (a) promote sustained investment in AI R&D; (b) enhance access to high-quality and fully traceable Federal data, models, and computing resources to increase the value of such resources for AI R&D, "while maintaining safety, security, privacy, and confidentiality protections consistent with applicable laws and policies;" (c) reduce barriers to the use of AI technologies while protecting American technology, economic and national security, civil liberties, privacy, and values; (d) train the next generation of AI researchers and users; and (e) develop and implement an action plan, in accordance with the National Security Presidential Memorandum of February 11, 2019. *Id.*

12. *Id.* at § 6(d).

13. NAT'L INST. OF STANDARDS & TECH., U.S. LEADERSHIP IN AI: A PLAN FOR FEDERAL ENGAGEMENT IN DEVELOPING TECHNICAL STANDARDS AND RELATED TOOLS (2019) [hereinafter "NIST Plan"].

14. *Id.* at 12.

15. *Id.*

16. See Brian Higgins, *Government Plans to Issue Technical Standards for Artificial Intelligence Technologies*, ARTIFICIAL INTELLIGENCE TECHNOLOGY AND THE LAW (Feb. 20, 2019), <http://aitechnologylaw.com/2019/02/government-plans-to-issue-technical-standards-governing-artificial-intelligence-technologies/> ("[F]ederal governance of AI under the Trump Administration

will favor a policy and standards governance approach over a more onerous command-and-control-type regulatory agency rulemaking approach leading to regulations (which the Trump administration often refers to as “barriers”).

17. Jory Heckman, *NIST Sets AI Ground Rules for Agencies Without “Stifling Innovation,”* FEDERAL NEWS NETWORK (Aug. 22, 2019, 5:58 PM), <https://federalnewsnetwork.com/artificial-intelligence/2019/08/nist-sets-ai-ground-rules-for-agencies-without-getting-over-prescriptive>.

18. *Id.*

19. H.R. Res. 153, 116th Cong. (2019). For an overview of the recent developments in AI, see Kay Firth-Butterfield & Yoon Chae, *Artificial Intelligence Collides with Patent Law*, WORLD ECONOMIC FORUM (2018), [http://www3.weforum.org/docs/WEF\\_48540\\_WP\\_End\\_of\\_Innovation\\_Protecting\\_Patent\\_Law.pdf](http://www3.weforum.org/docs/WEF_48540_WP_End_of_Innovation_Protecting_Patent_Law.pdf).

20. *Id.*

21. Assemb. Con. Res. 215, 2018 Reg. Sess. (Cal. 2018) (enacted).

22. *Id.*

23. *Asilomar AI Principles*, FUTURE OF LIFE INSTITUTE, <https://futureoflife.org/ai-principles> (last visited Nov. 12, 2019).

24. *Id.*

25. Yoon Chae, *Recent Trends in California’s AI Regulation Efforts*, LAW360 (July 11, 2019), <https://www.law360.com/articles/1176167/recent-trends-in-california-s-ai-regulation-efforts>.

26. *Asilomar AI Principles*, *supra* note 23.

27. Algorithmic Accountability Act of 2019, S. 1108, H.R. 2231, 116th Cong. (2019); *see also* Yoon Chae, *supra* note 25.

28. Sneha Revanur, *In a Historic Step Toward Safer AI, Democratic Lawmakers Propose Algorithmic Accountability Act*, MEDIUM (Apr. 20, 2019), <https://medium.com/@sneharevanur/in-a-historic-step-toward-safer-ai-democratic-lawmakers-propose-algorithmic-accountability-act-86c44ef5326d>.

29. Algorithmic Accountability Act of 2019, *supra* note 27, at § 2(2) and 3(b) (emphases added). The bill would also require the covered entities to conduct data protection impact assessments on their “high-risk information systems.” *See id.* at § 2(6) and 3(b).

30. *Id.* at § 3(b)(1)(C).

31. *Id.* at § 3(b)(1)(D).

32. *Id.* at § 2(1) (emphases added). “High risk” automated decision systems would include those that: (1) pose a significant risk to the privacy or security of personal information of consumers, or of resulting in or contributing to inaccurate, unfair, biased, or discriminatory decisions affecting consumers; (2) make or facilitate human decision-making based on systematic and extensive evaluations of consumers (including attempts to analyze/predict sensitive aspects of their lives) and alter legal rights of consumers or otherwise affect consumers; (3) involve the personal information of consumers



regarding race, religion, health, gender, gender identity, criminal convictions or arrests, and other factors; (4) monitor public places; and (5) meet any other criteria established by the FTC. *Id.* at § 2(7).

33. *Id.* at § 2(5).

34. *Id.* at § 4 (“Nothing in this Act may be construed to preempt any State law.”).

35. Byungkwon Lim et al., *A Glimpse into the Potential Future of AI Regulation*, LAW360 (Apr. 10, 2019), <https://www.law360.com/articles/1158677/a-glimpse-into-the-potential-future-of-ai-regulation>.

36. See Algorithmic Accountability Act of 2019, *supra* note 27, at § 3(d)-(e); Byungkwon Lim, *supra* note 35.

37. See Byungkwon Lim, *supra* note 35; Emily J. Tail et al., *Proposed Algorithmic Accountability Act Targets Bias in Artificial Intelligence*, JD SUPRA (June 27, 2019), <https://www.jdsupra.com/legalnews/proposed-algorithmic-accountability-act-70186> (“The Act is the first federal legislative effort to regulate AI systems across industries in the United States, and it reflects a growing and legitimate concern regarding the lawful and ethical implementation of AI.”).

38. See Byungkwon Lim, *supra* note 35.

39. Jennifer Betts, *Keeping an Eye on Artificial Intelligence Regulation and Legislation*, OGLETREE, DEAKINS, NASH, SMOAK & STEWART, P.C. (June 17, 2019).

40. New Jersey Algorithmic Accountability Act, A.B. 5430, 218th Leg., 2019 Reg. Sess. (N.J. 2019).

41. *Id.* at § 3.

42. *Id.* at § 2.

43. See Charlyn Ho et al., *New York and New Jersey Make an Early Effort to Regulate Artificial Intelligence*, JD SUPRA (July 15, 2019), <https://www.jdsupra.com/legalnews/new-york-and-new-jersey-make-an-early-73507>.

44. Ben Kelly & Yoon Chae, *Insight: AI Regulations Aim at Eliminating Bias*, BLOOMBERG LAW (May 31, 2019, 4:01 AM), <https://news.bloomberglaw.com/tech-and-telecom-law/insight-ai-regulations-aim-at-eliminating-bias>.

45. A Local Law in relation to automated decision systems used by agencies, Int. No. 1696-2017 (N.Y.C. 2018); see also Ben Kelly & Yoon Chae, *supra* note 44.

46. S.B. 5527, H.B. 1655, 66th Leg., 2019 Reg. Sess. (Wash. 2019); see also Yoon Chae, *supra* note 25.

47. S.B. 444, 2019 Reg. Sess. (Cal. 2019); see also Yoon Chae, *supra* note 25.

48. Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019).

49. Makena Kelly, *New Facial Recognition Bill Would Require Consent Before Companies Could Share Data*, THE VERGE (Mar. 14, 2019, 5:40 PM EDT), <https://www.theverge.com/2019/3/14/18266249/facial-recognition-bill-data-share-consent-senate-commercial-facial-recognition-privacy-act>.

50. Commercial Facial Recognition Privacy Act, *supra* note 48, at § 3(a)(1).

51. *Id.* at § 2(3).

52. See Jeffrey Neuburger & Daryn Grossman, *Bipartisan Facial Recognition Privacy Bill Introduced in Congress*, PROSKAUER (Mar. 26, 2019).

53. “[F]acial recognition data” is defined as “any unique attribute or feature of the face of an end user that is used by facial recognition technology to assign a unique, persistent identifier or for the unique personal identification of a specific individual.” Commercial Facial Recognition Privacy Act, *supra* note 48, at § 2(6). Likewise, “facial recognition technology” is defined as a technology that analyzes facial features in still or video images and “is used to assign a unique, persistent identifier;” or “is used for the unique personal identification of a specific individual.” *Id.* at § 2(5).

54. *Id.* at § 3(a)(2)-(4).

55. *Id.* at § 3(b)(3).

56. *Id.* at § 3(c)(1)-(2).

57. *Id.* at § 3(d).

58. *Id.* at § 3(e)(2) and § 2(9).

59. *Id.* at § 3(e)(1)(A).

60. *Id.* at § 6.

61. *Id.* at § 6-7.

62. *Id.* at § 4.

63. The bill was introduced by Senator Roy Blunt (R-MO) and co-sponsored by Senator Brian Schatz (D-HI).

64. See Jeffrey Neuburger & Daryn Grossman, *supra* note 52.

65. See Commercial Facial Recognition Privacy Act, *supra* note 48, at § 2(2)-(3).

66. Teresa Wiltz, *Facial Recognition Software Prompts Privacy, Racism Concerns in Cities and States*, GOVERNMENT TECHNOLOGY (Aug. 13, 2019), <https://www.govtech.com/products/Facial-Recognition-Software-Prompts-Privacy-Racism-Concerns-in-Cities-and-States.html>.

67. H.R. 3875, 116th Cong. (2019).

68. FACE Protection Act of 2019, H.R. 4021, 116th Cong. (2019).

69. No Biometric Barriers to Housing Act of 2019, H.R. 4008, 116th Cong. (2019).

70. See *id.* at § 3.

71. Yoon Chae, *supra* note 25.

72. *Id.*

73. An Act Establishing a Moratorium on Face Recognition and Other Remote Biometric Surveillance Systems, S. 1385, 191st Leg. (Mass. 2019); S. 5687, A.B. 7790, 2019 Reg. Sess. (N.Y. 2019).

74. S.B. 5528, H.B. 1654, 66th Leg., 2019 Reg. Sess. (Wash. 2019).

75. See Ben Kelly & Yoon Chae, *supra* note 44; Katie Lannan, *Somerville Bans Government Use of Facial Recognition Tech*, WBUR (June 28, 2019),

<https://www.wbur.org/bostonmix/2019/06/28/somerville-bans-government-use-of-facial-recognition-tech>. For further discussion of state and local regulatory development on facial recognition technology, see GIBSON DUNN, ARTIFICIAL INTELLIGENCE AND AUTONOMOUS SYSTEMS LEGAL UPDATE (2Q19) 5-6, July 23, 2019.

76. See Illinois Biometric Information Privacy Act, 740 ILCS 14/1; Tex. Bus. & Com. Code § 503.001.

77. Wash. Rev. Code § 19.375 *et seq.*

78. CCPA will be codified at Cal. Civ. Code § 1798.100 to 1798.198.

79. An Act relative to consumer data privacy, S. 120, 191st Leg. (Mass. 2019).

80. Cal. Bus. & Prof. Code § 17940 *et seq.*

81. See Noam Cohen, *Will California's New Bot Law Strengthen Democracy?*, NEW YORKER (July 2, 2019), <https://www.newyorker.com/tech/annals-of-technology/will-californias-new-bot-law-strengthen-democracy>; Jamie Williams & Jeremy Gillula, *Victory! Dangerous Elements Removed from California's Bot-Labeling Bill*, ELECTRONIC FRONTIER FOUNDATION (Oct. 5, 2018), <https://www.eff.org/deeplinks/2018/10/victory-dangerous-elements-removed-californias-bot-labeling-bill>.

82. See Cal. Bus. & Prof. Code § 17941(a) (“It shall be unlawful for any person to use a bot to communicate or interact with another person in California online, with the intent to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication in order to incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election. A person using a bot shall not be liable under this section if the person discloses that it is a bot.”).

83. *Id.* at § 17940(a).

84. *Id.* at § 17941(a)-(b).

85. *Id.* at § 17941(b)-(c); see also Harry Valetk & Brian Hengesbaugh, *California Now Has a New Bot Disclosure Law—Will Other States Follow Suit?*, B:INFORM (July 26, 2019), <http://www.bakerinform.com/home/2019/7/26/california-now-has-a-new-bot-disclosure-law>.

86. Cal. Bus. & Prof. Code § 17942(c) (“This chapter does not impose a duty on service providers of online platforms, including, but not limited to, Web hosting and Internet service providers.”).

87. See Harry Valetk & Brian Hengesbaugh, *supra* note 85 (“Violating the B.O.T. Act’s disclosure requirements could constitute a violation of California’s Unfair Competition Act (Cal. Code BPC § 17206), which includes a civil penalty of up to USD 2,500 for each violation. Accordingly, each ‘like,’ ‘share,’ or ‘re-tweet’ performed by a bot without a proper disclosure could result in a USD 2,500 penalty”).

88. See Jamie Williams & Jeremy Gillula, *supra* note 81.

89. See *id.*

90. Anti-Eavesdropping Act, A.B. 1395, 2019 Reg. Sess. (Cal. 2019), status available at [https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill\\_id=201920200AB1395](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1395) (last amended in Senate on June 26, 2019).

91. *Id.* at § 3 (proposing amendment of Cal. Bus. & Prof. Code § 22948.20(a)).

92. *Id.* at § 3 (proposing amendment of Cal. Bus. & Prof. Code § 22948.20(b)(1)-(3)).

93. *Id.* at § 3 (proposing amendment of Cal. Bus. & Prof. Code § 22948.20(d)).

94. Artificial Intelligence Video Interview Act, H.B. 2557, 101st Gen. Assemb., 2019 Reg. Sess., Public Act 101-0260 (Ill. 2019).

95. *Id.* at § 5(1)-(3).

96. *Id.* at § 10 and 15.

97. Theodore F. Claypoole & Dominic Dhil Panakal, *Illinois Law Regulates Use of AI in Video Interviews*, THE NATIONAL LAW REVIEW (Aug. 15, 2019), <https://www.natlawreview.com/article/illinois-law-regulates-use-ai-video-interviews>; see also Justin Steffen & Heather Renée Adams, *Hiring ex Machina: Preparing for Illinois's Artificial Intelligence Video Interview Act*, LEGALTECH NEWS (Sept. 23, 2019, 7:00 AM), <https://www.law.com/legaltech/news/2019/09/23/hiring-ex-machina-preparing-for-illinois-artificial-intelligence-video-interview-act> (providing that the Act is silent on “whether job candidates have a private right of action for violations of the Act”).

98. Theodore F. Claypoole & Dominic Dhil Panakal, *supra* note 97.

99. FUTURE of Artificial Intelligence Act of 2017, S. 2217, H.R. 4625, 115th Congress (2017).

100. Ben Kelly & Yoon Chae, *supra* note 44.

101. See GrAITR Act of 2019, H.R. 2202, 116th Congress (2019); AI-IA, S. 1558, 116th Congress (2019).

102. GrAITR Act of 2019, *supra* note 101, at § 101(6)(F); AI-IA, *supra* note 101, at § 101(6)(F).

103. GrAITR Act of 2019, *supra* note 101, at § 301(b); AI-IA, *supra* note 101, at § 301(b).

104. AI in Government Act of 2019, S. 1363, H.R. 2575, 116th Congress (2019).

105. *Id.* at § 3(b)(5) and 4(a)(3).

106. PERSONAL DATA PROT. COMM'N SINGAPORE, A PROPOSED MODEL ARTIFICIAL INTELLIGENCE GOVERNANCE FRAMEWORK 3.3 (2019).

107. *Id.* at 3.4.1-2.

108. WORLD ECON. FORUM, DRAFT GUIDELINES FOR AI PROCUREMENT 12 (2019).

109. See *id.* at 13.

110. *AI Fairness 360*, IBM DEVELOPER (Nov. 14, 2018), <https://developer.ibm.com/open/projects/ai-fairness-360>; see also NIST Plan, *supra* note 13, at App. III (AI-Related Tools).

111. Matt Turek, *Explainable Artificial Intelligence*, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, <https://www.darpa.mil/program/explainable-artificial-intelligence> (last visited Sept. 25, 2019); *see also* NIST Plan, *supra* note 13, at App. III.

112. *See id.*

113. *See* PERSONAL DATA PROT. COMM’N SINGAPORE, *supra* note 106, at 3.16(b).

114. *Id.* at 3.16(d)-(e).

115. *Algorithmic Impact Assessment (AIA)*, GOVERNMENT OF CANADA, <https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/responsible-use-ai/algorithmic-impact-assessment.html> (last visited Sept. 25, 2019); *Algorithmic Accountability Policy Toolkit*, AI NOW INSTITUTE (Oct. 2018), <https://ainowinstitute.org/aap-toolkit.pdf>; *see also* PERSONAL DATA PROT. COMM’N SINGAPORE, *supra* note 106; WORLD ECON. FORUM, DRAFT GUIDELINES FOR AI PROCUREMENT, *supra* note 108; IEEE, ETHICALLY ALIGNED DESIGN, *supra* note 3.

116. *See* PARTNERSHIP ON AI, <https://www.partnershiponai.org> (last visited Sept. 25, 2019).

117. Algorithmic Accountability Act, *supra* note 27, at § 2(2)(B)(i).

118. New Jersey Algorithmic Accountability Act, *supra* note 40, at § 2.

119. NIST Plan, *supra* note 13, at App. II (AI Standards).

120. NIST Plan, *supra* note 13, at App. II; *see also* IEEE P7000<sup>TM</sup> Projects, OPEN COMMUNITY FOR ETHICS IN AUTONOMOUS AND INTELLIGENT SYSTEMS, <https://ethicsstandards.org/p7000> (last visited Sept. 24, 2019).

121. *See* NIST Plan, *supra* note 13, at App. II; IEEE P7000<sup>TM</sup> Projects, *supra* note 120.

122. *Id.*

123. *Id.*

124. For example, monitoring and reviewing the AI models that have been deployed “with a view to taking remediation measures where needed” may be considered. *See* PERSONAL DATA PROT. COMM’N SINGAPORE, *supra* note 106, at 3.4.1(c)(ii).

125. PERSONAL DATA PROT. COMM’N SINGAPORE, *supra* note 106, at 3.9.

126. *See id.* at 3.27–29.