GIBSON DUNN

November 4, 2019

ARTIFICIAL INTELLIGENCE AND AUTONOMOUS SYSTEMS LEGAL UPDATE (3Q19)

To Our Clients and Friends:

The third quarter of 2019 continued the public pushback on the unrestricted use of AI technologies, particularly, for the U.S., with regard to technologies used to create "deepfake" video and audio clips as well as the use of facial recognition technology in the public sector. Some of the actions this quarter were follow-on steps to matters we have discussed in prior quarterly alerts; others are new initiatives. Below we take a look at the current state of regulation efforts (both proposed and enacted) in the U.S. and EU, consider the rush to address deepfakes, and provide further updates on other movement in the U.S. and EU toward regulating the use of AI technologies during the past quarter.

Table of Contents

I. Key U.S. Legislative and Regulatory Developments

A. SEVERAL NEW AI BILLS PROPOSED IN CONGRESS

As the adoption of AI technology in the U.S. continues across a wide range of industries and the public sector, legislators are increasingly making efforts to regulate applicable data standards at federal level. On September 24, 2019, H.R. 4476, the "Financial Transparency Act of 2019" was reintroduced into Congress by Reps. Carolyn Maloney (D-NY) and Patrick McHenry (R-NC).[1] The bipartisan bill, which calls for the Treasury secretary to create uniform, machine-readable data standards for information reported to financial regulatory agencies,[2] has been referred to the Subcommittee on Commodity Exchanges, Energy, and Credit. By seeking to make information that is reported to financial regulatory agencies electronically searchable, the bill's supporters aim to "further enable the development of RegTech and Artificial Intelligence applications," "put the United States on a path towards building a comprehensive Standard Business Reporting program," and "harmonize and reduce the private sector's regulatory compliance burden, while enhancing transparency and accountability."[3]

Increasingly, algorithms are also being used at every stage of criminal proceedings, from gathering evidence to making sentencing and parole recommendations. H.R. 4368, the "Justice in Forensic Algorithms Act of 2019," was introduced in the House on September 17, 2019, would prohibit the use of trade secrets privileges to prevent defense access to the source code of proprietary algorithms used as evidence in criminal proceedings, and require that the Director of the National Institute of Standards and Technology ("NIST") establishes a program to provide for the creation and maintenance of standards for the development and use of computational forensic software ("Computational Forensic Algorithm Standards") to protect due process rights.[4] The standards would address underlying scientific principles and methods, an assessment of disparate impact on the basis of demographic features such as race or gender, requirements for testing and validating the software and for publicly available documentation, and requirements for reports that are provided to defendants by the prosecution documenting the use and results of computational forensic software in individual cases (e.g. source code).[5]

Legislators are also taking action to recognize the potentially vast implications of AI technology on employment and employees' rights. On September 11, 2019, Sen. Brown (D-OH) introduced S. 2468, the "Workers' Right to Training Act," which would require employers to provide training to employees whose jobs are in danger of being changed or replaced due to technology, and for other purposes.[6] "Technology" is defined in the bill as including "automation, artificial intelligence, robotics, personal computing, information technology, and e-commerce."[7]

B. INCREASED FOCUS ON COUNTERING DEEPFAKES

A new AI application called "deepfakes" is raising a set of challenging policy, technology, and legal issues. Deepfake technology is used to combine and superimpose existing images and videos onto source images or videos ─ creating new "synthetic" images or videos ─ by using a machine learning technique known as a generative adversarial network (GAN), a deep neural net architecture comprised of two nets, pitting one against the other (the "adversarial"). Since GANs can learn to mimic any distribution of data (images, music, speech, or text), the applications of deepfake technology are vast. Prompted by increased public concern over the potential impact of the technology on everything from cybersecurity to electoral manipulation, tentative federal bills intended to regulate deepfakes have emerged over the past several months, while state legislatures have already reacted by banning certain deepfake applications.[8]

In September 2018, Reps. Adam Schiff (D-Calif.), Stephanie Murphy (D-Fla.) and Carlos Curbelo (R-Fla.) sent a letter to the Director of National Intelligence to warn of potential risks relating to deepfakes.[9] The lawmakers cautioned that "[d]eep fakes have the potential to disrupt every facet of our society and trigger dangerous international and domestic consequences . . . . [a]s with any threat, our Intelligence Community must be prepared to combat deep fakes, be vigilant against them, and stand ready to protect our nation and the American people."[10] In the wake of a June 2019 hearing by the House Permanent Select Committee on Intelligence on the national security challenges of artificial intelligence, manipulated media, and deepfake technology, both the House and the Senate introduced legislation to regulate GANs. At present, however, the bills appear to do very little to restrict the use of deepfake technology, suggesting that Congress remains in "learning mode."

1. Federal level

On July 9, 2019, Sen. Rob Portman (R-OH) introduced the "Deepfake Report Act" (S. 2065), which would require the Department of Homeland Security to submit five annual reports to Congress on the state of the "digital content forgery" technology and evaluate available methods of detecting and mitigating threats.[11] The reports will include assessments of how the technology can be used to harm national security as well as potential counter measures. The bill defines digital content forgery as "the use of emerging technologies, including artificial intelligence and machine learning techniques, to fabricate or manipulate audio, visual, or text content with the intent to mislead." The bipartisan bill was passed in the Senate by unanimous consent on October 25 and is currently before the House Committee on Energy and Commerce, which is reviewing the same-named companion bill, H.R. 3600.[12]

In the House, H.R. 3230 ("Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act" or the "DEEPFAKES Act") was introduced by Rep. Clarke (D-NY-9) on June 12, 2019[13] It would require any "advanced technological false personation record" to be digitally watermarked. The watermark would be required to "clearly identifying such record as containing altered audio or visual elements." The bill has been referred to the Subcommittee on Crime, Terrorism, and Homeland Security.

On September 17, 2019, Rep. Anthony Gonzalez (R-OH) introduced the "Identifying Outputs of Generative Adversarial Networks Act" (H.R. 4355), which would direct both the National Science Foundation and NIST to support research on deepfakes to accelerate the development of technologies that could help improve their detection, to issue a joint report on research opportunities with the private sector, and to consider the feasibility of ongoing public and private sector engagement to develop voluntary standards for the outputs of GANs or comparable technologies.[14]

2. State level

At least three states, Virginia, Texas, and California, have already created laws banning the use of deepfake technology in certain applications: nonconsensual pornography[15] and electoral malfeasance.[16] These laws may signal state regulators' willingness to quickly regulate other controversial AI applications going forward.

C. MORE ACTIONS AGAINST FACIAL RECOGNITION SOFTWARE

1. Use in Law Enforcement

As we reported in our Artificial Intelligence and Autonomous Systems Legal Update (2Q19), biometric surveillance, or "facial recognition technology," has emerged as a lightning rod for public debate regarding the invasive nature of the technology and the risk of disparate impact. Until very recently, there were few if any laws or guidelines governing the use of facial recognition technology. However, amid increasing public concern about the technology operating in public spaces, 2019 has seen a string of efforts by various cities in the U.S to ban the use of facial recognition technology by law enforcement.[17] Oakland City Council recently passed an ordinance to ban its use by city police and other government departments, joining San Francisco, California and Somerville, Massachusetts who had already enacted similar bans.[18] Berkeley City Council also adopted a ban at a meeting in mid-October.[19] Cambridge, Massachusetts, also moved one step closer to prohibiting local government from using facial recognition. In December 2018, Cambridge City Council passed the "Surveillance Technology Ordinance," which requires the council's approval prior to the acquisition or deployment of certain surveillance tech, including facial recognition software. An amendment to the ordinance, which outright prohibits any use of facial recognition software, was forwarded by the council to the Public Safety Committee on July 30, 2019.[20]

At state level, in September 2019 California lawmakers passed legislation (A.B. 1215), barring police from installing facial recognition on body-worn cameras for the next three years.[21] The bill by Assemblyman Phil Ting (D-San Francisco), which was co-sponsored by the ACLU, was signed into law by Governor Newsom on October 8. Previously, the ACLU had run demonstrations using facial-recognition technology which falsely flagged 26 California lawmakers as matching arrest photos.[22]

2. Other Uses

On July 25, 2019, Reps Yvette Clark (D-NY), Ayanna Pressley (D-Mass.) and Rashida Tlaib (D-Mich.) introduced the "No Biometric Barriers to Housing Act." If passed, the bill would prohibit facial recognition in public housing units that receive Department of Housing and Urban Development ("HUD") funding. It would also require HUD to submit a report on facial recognition and its impacts on public housing units and tenants.[23] New York City Council is also considering proposed legislation that would prevent landlords from mandating that tenants use facial recognition, biometric scanning, or other "smart" key technology to enter their apartment buildings or their individual unit.[24]

For businesses working on or considering the use of facial recognition technologies, the recent developments emphasize the increased scrutiny that such technologies are receiving. It is important for companies operating in these technologies to understand the legal and regulatory landscape before launching products, and to seek to minimize risks in high liability areas.[25]

D. ILLINOIS AI VIDEO INTERVIEW ACT GOES INTO EFFECT

Amid the acceleration in the spread of AI and automated decision-making in the public and private sector, many U.S. and multinational companies have begun to use AI to streamline and introduce objectivity into their hiring process,[26] using AI-powered interview platforms ─ equipped with abilities such as sentiment analysis, facial recognition, video analytics, neural language processing, machine learning and speech recognition ─ that are capable of screening candidates against various parameters to assess competencies, experience and personality on the basis of hundreds of thousands of data points, and rank them against other candidates based on an "employability" score.[27] The lack of transparency resulting from the use of proprietary algorithms to hire and reject candidates has led to some regulatory pushback. As we reported in our Artificial Intelligence and Autonomous Systems Legal Update (2Q19), in May 2019 the Illinois legislature unanimously passed H.B. 2557 (the "Artificial Intelligence Video Interview Act"), which governs the use of AI by employers when hiring candidates.[28] State Rep. Jaime Andrade Jr. (D), who co-sponsored the bill, noted that spoken accents or cultural differences could end up improperly warping the results, and that people who declined to sit for the assessment could be unfairly punished by not being considered for the job.[29] On August 9, 2019, Governor J.B. Pritzker signed the Act into law, effective January 1, 2020. Under the Act, an employer using videotaped interviews when filling a position in Illinois may use AI to analyze the interview footage only if the employer:

- Gives **notice** to the applicant that the videotaped interview may be analyzed using AI for purposes of evaluating the applicant's fitness for the position. (A Senate floor amendment removed from the bill a requirement for written notice.)
- Provides the applicant with an **explanation** of how the AI works and what characteristics it uses to evaluate applicants, and
- Obtains **consent** from the applicant to use AI for an analysis of the video interview.
- Keeps video recordings **confidential** by sharing the videos only with persons whose expertise or technology is needed to evaluate the applicant, and **destroying** both the video and all copies within 30 days after an applicant requests such destruction.

Illinois employers using such software will need to carefully consider how they are addressing the risk of AI-driven bias in their current operations and whether hiring practices fall under the scope of the new law, which does not define "artificial intelligence," what level of "explanation" is required, or whether it applies to employers seeking to fill a position in Illinois regardless of where the interview takes place. Nor is there provision in the Act for a private right of action or specific remedies. While the Illinois Act currently remains the only such law to date in the U.S., companies using automated technology in recruitment should expect that the increasing use of AI technology in recruitment is likely to lead to further regulatory proposals in due course. As previously noted,[30] a major challenge for companies subject to such laws will be explaining to regulators how their AI assessments work and how the criteria are ultimately used in any decision-making processes.

II. Developments in the EU

A. FOCUS ON COMPREHENSIVE AI REGULATION

AI remains a top priority for policymakers in the EU. The new president of the European Commission, Ursula von der Leyen, recently unveiled her policy agenda for the next five years. As part of her proposal to create "a Europe fit for the digital age" she promised to put forward legislation "for a coordinated European approach on the human and ethical implications of AI" in the first 100 days (meaning we can expect a draft by March 2020).[31] A key challenge for the new president will be to grow investment, data, and talent required to develop AI and accelerate its adoption, and creating an innovation-friendly regulatory environment across the EU, which has thus far adopted a "regulate-first" strategy.

Based on public comments by those likely to be involved in the creation of proposed AI regulation, we anticipate that the EU legislation will (1) address government funding of research, workplace training and the availability of public data, (2) not seek to significantly re-write exiting legal frameworks, but largely try to fit within the GDPR, the Directive on Copyright in the Digital Single Market, and the ePrivacy regulation, (3) require, like some U.S. states – notably California – that any chatbot or virtual assistant interacting with individuals will need to disclose that it is not a human, and create enhanced requirements for transparency as to the use of data and the bases for decisions or recommendations to avoid unintended bias or disparate impact, (4) require and potentially allocate accountability for failures or problems caused by machines, and (5) require GDPR-style impact assessments to ensure AI systems do not perpetuate discrimination or violate fundamental rights.[32]

B. UK FOCUS ON AI

A report from the UK Government's Business, Energy and Industrial Strategy Committee published in September 2019 has investigated the state of automation in the UK.[33] The Automation and the Future of Work report highlights how the UK's slow adoption of automation is being hampered by a lack of action from the UK Government, with entire regions of the country at risk of being left behind by G7 competitors. In 2015, the UK had 10 robots for every million hours worked, compared with 131 in the US, 133 in Germany and 167 in Japan. By 2017, the UK represented just 0.6% of industrial robotics shipments. The report argues that unless concerted efforts are made to manage the transition to the so-called Fourth Industrialization, UK businesses will miss a pivotal opportunity for economic growth.

The report urges the UK Government to establish a robot and AI strategy by 2020, which is a step towards building confidence amongst businesses, industries and universities. The report urges that the strategy be created by bringing together employers, workers, academia, and automation developers to collaboratively design the best strategic approach to "promote and manage the transition to a more automated world of work."

Echoing many of the sentiments seen in the U.S (as noted above), in addition to issuance of the automation report, the House of Commons' Science and Technology Committee has also called for a suspension of the use of automatic facial recognition technology until regulations have been put in place.[34]

III. Autonomous Vehicles: A New Hope For Federal Regulation

Federal regulation of autonomous vehicles ("AVs") has so far faltered in the new Congress. However, more recently federal lawmakers have demonstrated renewed interest in a comprehensive AV bill aimed at speeding up the adoption of autonomous vehicles and deploying a regulatory framework. In July 2019, the House Energy and Commerce Committee and Senate Commerce Committee sought stakeholder input from the self-driving car industry in order to draft a bipartisan and bicameral AV bill, prompting stakeholders to provide feedback to the committees on a variety of issues involving autonomous vehicles, including cybersecurity, privacy, disability access, and testing expansion.[35]

Meanwhile, the National Highway Traffic Safety Administration ("NHTSA") continues to take tentative steps to plug the regulatory gap. As we noted in our Artificial Intelligence and Autonomous Systems Legal Update (2Q19), the NHTSA earlier this year sought comments on petitions from industry stakeholders regarding exemptions from the Federal Motor Vehicle Safety Standards ("FMVSSs") in connection with automated vehicles and the Federal Motor Carrier Safety Regulations (regulations governing commercial vehicles, e.g. trucks), which may be a barrier to deploying Automated Driving System-Dedicated Vehicles ("ADS-DVs"). Additionally, on September 18, 2019, the Department of Transportation ("DOT") announced $60 million in federal grant funding to eight projects that test the safe integration of automated driving systems on roads.

On October 16, 2019, the UK Law Commission published a second public consultation[36] on a proposed regulatory framework for Highly Automated Road Passenger Services ("HARPS") ─ vehicles that operate without a driver (or "user-in-charge").[37] The current consultation seeks stakeholders' views on whether HARPS operators should be subject to a national licensing scheme, and on the conditions that they should meet to obtain a license. The consultation also considers private ownership of passenger-only vehicles, accessibility for older and disabled people, how to control congestion on public roads, and how regulation can help self-driving vehicles integrate with public transport. Comments may be submitted to the law Commission before January 16, 2020, with the final report and final recommendations due in 2021. We encourage our clients to contact us if they would like further information or assistance in developing and submitting comments.

IV. Data Privacy

While not strictly focused on artificial intelligence technologies, a number of state and federal developments in the area of data privacy are noteworthy, given the central importance of access to large quantities of data (often including personal and private data) to the successful development and operation of many AI systems.

First, in California, a series of amendments to the California Consumer Privacy Act ("CCPA") were signed into effect by the Governor in early October.[38] Some of these amendments may prove significant to certain businesses; such as A.B. 25, which provides a one-year carve-out of the personal information of employees from personal information that would otherwise fall under the requirements of the CCPA. Similarly, A.B. 1355 creates a one-year carve-out of certain personal information that is collected as part of purely business-to-business communications, which may also help alleviate concerns about how to handle personal information necessarily acquired in a business context. In addition to the amendments, the California Attorney General's Office released a series of proposed regulations for implementing the requirements of the CCPA, and initiated a period in which they will solicit public comments before making any final changes putting the regulations into force and effect.[39] The proposed regulations generally set out guidance for how businesses should implement the notice provisions of the CCPA, procedural steps for implementing consumer rights provisions and data collection requirements, as well as provide some clarification of the CCPA's non-discrimination provisions.

Second, in Nevada, the 2019 amendments to Nevada's existing on-line privacy law went into effect on October 1, 2019.[40] These amendments add data privacy provisions giving consumers the ability to opt-out of the sale of their covered information, although with fewer requirements than set out in the CCPA. Similarly, the Nevada law takes a narrower view of "sale" than does the CCPA, and only applies to the collection of covered information by commercial internet website and on-line services.

Finally, in July, California Senator Dianne Feinstein introduced the Voter Privacy Act of 2019, which is currently before the Senate Committee on Rules and Administration.[41] As introduced, the Act will give voters certain rights with regard to their personal data collected in connection with voter information. In particular, the Act provides notice rights, rights of access, deletion rights, and rights to prohibit transfer or targeting through use of the data. The stated purpose of the Act is to put an end to the manipulation and misdirection of voters through the use of their personal data, and the Act would be monitored by the Federal Election Commission. Obviously, for companies collecting voter information as part of the data processed by AI systems, the Act could add a number of significant compliance requirements should it ultimately pass.

---

[1] H.R.4476, 116th Congress (U.S. House of Representatives).

[2] *Id*. (Including the Securities and Exchange Commission, Commodity Futures Trading Commission, Federal Deposit Insurance Corp., Federal Reserve, Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, the National Credit Union Association and the Federal Housing Finance Agency.).

[3] *Id*.

[4] H.R.4368, 116th Congress (U.S. House of Representatives).

[5] Press Release, *Rep. Takano Introduces the Justice in Forensic Algorithms Act to Protect Defendants' Due Process Rights in the Criminal Justice System* (Sep. 17, 2019), *available at* https://takano.house.gov/newsroom/press-releases/rep-takano-introduces-the-justice-in-forensic-algorithms-act-to-protect-defendants-due-process-rights-in-the-criminal-justice-system.

[6] S. 2468, 116th Congress (U.S. Senate).

[7] *Id*.

[8] AB 730, AB 602 (California); SB 751 (Texas); HB 2678 (Virginia); HR 3230, 116th Congress (U.S. House of Representatives); S 2065, 116th Congress (U.S. Senate).

[9] Letter from Adam Schiff, U.S. Representative, Stephanie Murphy, U.S. Representative & Carlos Curbelo, U.S. Representative to Hon. Daniel R. Coats, Dir. of Nat'l Intelligence (Sept. 13, 2018).

[10] *Id*.

[11] S. 2065, 116th Congress (U.S. Senate).

[12] H.R. 3600, 116th Congress (U.S. House of Representatives).

[13] H.R. 3230, 116th Congress (U.S. House of Representatives).

[14] H.R. 4355, 116th Congress (U.S. House of Representatives).

[15] California (A.B. 602) and Virginia (H.B. 2678) have banned the application of pornographic deepfakes. Virginia, in enacting the first piece of legislation to directly address deepfakes, banned "dissemination or sale of certain images of another person, that "another person" includes a person whose image was used in creating, adapting, or modifying a videographic or still image with the intent to depict an actual person and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic." California created a private right of action against a person who either "(1) creates and intentionally discloses sexually explicit material if the person knows or reasonably should have known the depicted individual did not consent to its creation or disclosure or (2) who intentionally discloses sexually explicit material that the person did not create if the person knows the depicted individual did not consent to its creation."

[16] California (A.B. 730) and Texas (S.B. 751) have banned deepfakes designed to influence elections. In Texas, it is now a crime to "with intent to injure a candidate or influence the result of an election: (1) creates a deep fake video; and (2) cause[] the deep fake video to be published or distributed within 30 days of an election." Texas defines a "deep fake" broadly as "a video, created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality." California has banned anyone, within 60 days of an election of a candidate, from "distributing with actual malice materially deceptive audio or visual media of the candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate, unless the media includes a disclosure stating that the media has been manipulated." The California law defines the prohibited activity more narrowly, it must "falsely appear to a reasonable person to be authentic" and "cause a reasonable person to have a fundamentally different understanding or impression of the expressive content of the image or audio or video recording than that person would have if the person were hearing or seeing the unaltered, original version of the image or audio or video recording."

[17] For further detail, *see* our Artificial Intelligence and Autonomous Systems Legal Update (2Q19).

[18] Sarah Ravani, *Oakland bans use of facial recognition technology, citing bias concerns* (Jul. 17, 2019), *available at* https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php; *see also*, Cade Metz, *Facial Recognition Tech Is Growing Stronger, Thanks to Your Face* (Jul. 13, 2019), *available at* https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html.

[19] Levi Sumagaysay, *Berkeley bans facial recognition* (Oct. 16, 2019), *available at* https://www.mercurynews.com/2019/10/16/berkeley-bans-facial-recognition/.

[20] *See* Jack Karp, *Facial Recognition Software Sparks Transparency Battle*, Law360 (Nov. 3, 2019), *available at* https://www.law360.com/access-to-justice/articles/1215786/facial-recognition-software-sparks-transparency-battle; Declan J. Knieriem, *City Council Introduces Facial Recognition Ban Bill at Summer Meeting* (Aug. 2, 2019), available at https://www.thecrimson.com/article/2019/8/2/council-may-ban-facial-recognition/.

[21] A.B. 1215 2019–2020 Reg. Sess. (Cal. 2019); *see also* Anita Chabria, *California could soon ban facial recognition technology on police body cameras* (Sep. 12, 2019), *available at* https://www.latimes.com/california/story/2019-09-12/facial-recognition-police-body-cameras-california-legislation.

[22] Monica Melton, *Amazon Rekognition Falsely Matches 26 Lawmakers To Mugshots As California Bill To Block Moves Forward* (Aug. 13, 2019), available at https://www.forbes.com/sites/monicamelton/2019/08/13/amazon-rekognition-falsely-matches-26-lawmakers-to-mugshots-as-california-bill-to-block-moves-forward/.

[23] *See* H.R. 4008, 116th Congress (House of Representatives), currently pending before the House Committee on Financial Services.

[24] Brad Lander, *New City Council legislation would protect tenants from facial recognition & "smart" key surveillance*, NYC Council (Oct. 7, 2019), *available at* https://council.nyc.gov/brad-lander/2019/10/07/new-city-council-legislation-would-protect-tenants-from-facial-recognition-smart-key-surveillance/.

[25] For more on the importance of monitoring regulatory and technology developments in this space, *see* Fontenot, Gaedt-Sheckter, *Implications of AI on Board Oversight* (Oct. 2019) available at https://www.gibsondunn.com/wp-content/uploads/2019/10/Fontenot-Gaedt-Sheckter-Implications-of-AI-on-Board-Oversight-Corporate-Board-Member-10-23-2019.pdf.

[26] Robert Booth, *Unilever saves on recruiters by using AI to assess job interviews*, The Guardian (Oct. 25, 2019), *available at* https://www.theguardian.com/technology/2019/oct/25/unilever-saves-on-recruiters-by-using-ai-to-assess-job-interviews.

[27] Drew Harwell, *A face-scanning algorithm increasingly decides whether you deserve the job*, Washington Post (Oct. 25, 2019), *available at* https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

[28] H.B. 2557, 2019-2020 Reg. Sess. (Ill. 2019) (101st Gen. Assembly), *available at* http://www.ilga.gov/legislation/101/HB/PDF/10100HB2557lv.pdf.

[29] Drew Harwell, *A face-scanning algorithm increasingly decides whether you deserve the job*, Washington Post (Oct. 25, 2019), *available at* https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

[30] For further detail, *see* our Artificial Intelligence and Autonomous Systems Legal Update (2Q19).

[31] Ursula von der Leyen, *A Union that strives for more: My agenda for Europe*, *available at* https://www.europarl.europa.eu/resources/library/media/20190716RES57231/20190716RES57231.pdf/. Note that the von der Leyen commission was slated to begin on November 1, but due to problems with filling three of the commissioners' seats, it is likely to be delayed at least a month (thus pushing back the 100-day deadline).

[32] *See further*, H. Mark Lyon, *Gearing up for the EU's next regulatory push: AI*, Daily Journal (Oct. 11, 2019).

[33] U.K. House of Commons, Business, Energy and Industrial Strategy Committee, *Automation and the future of work* (Sep. 18, 2019), *available at*https://publications.parliament.uk/pa/cm201719/cmselect/cmbeis/1093/1093.pdf.

[34] Leo Kelion, *MPs call for halt to police's use of live facial recognition* (Jul 18, 2019), *available at* https://www.bbc.com/news/technology-49030595.

[35] Makena Kelly, *Congress wants the self-driving car industry's help to draft a new AV bill*, The Verge (Jul. 31, 2019), *available at* https://www.theverge.com/2019/7/31/20748582/congress-self-driving-cars-bill-energy-commerce-senate-regulation.

[36] The first public consultation in this review was launched in November 2018, focusing on safety assurance and legal liability, *available at* https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/11/6.5066_LC_AV-Consultation-Paper-5-November_061118_WEB-1.pdf.

[37] U.K. Law Commission, *Automated Vehicles, available at* https://consult.justice.gov.uk/law-commission/automated-vehicles-harps/.

[38] For more information, see our prior client alert, *California Consumer Privacy Act: 2019 Final Amendments Signed, available at* https://www.gibsondunn.com/california-consumer-privacy-act-2019-final-amendments-signed/.

[39] Again, for more information on the proposed regulations for CCPA, please see our prior client alert, *California Consumer Privacy Act Update: Regulatory Update, available at* https://www.gibsondunn.com/california-consumer-privacy-act-update-regulatory-update/.

[40] *See* Nevada S.B. 220, 80th Legislature.

[41] *See* S. 2398, 116th Congress (Senate).

■ ■ ■ ■ ■

The following Gibson Dunn lawyers prepared this client update: H. Mark Lyon, Frances A. Waldmann, Tony Bedel, Panayiota Burquier, and Arjun Rangarajan.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, any member of the firm's Artificial Intelligence and Automated Systems Group, or the following authors:

H. Mark Lyon - Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Frances A. Waldmann - Los Angeles (+1 213-229-7914,fwaldmann@gibsondunn.com)

Please also feel free to contact any of the following practice group members:

Artificial Intelligence and Automated Systems Group:

H. Mark Lyon - Chair, Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
J. Alan Bannister - New York (+1 212-351-2310, abannister@gibsondunn.com)
Lisa A. Fontenot - Palo Alto (+1 650-849-5327, lfontenot@gibsondunn.com)
David H. Kennedy - Palo Alto (+1 650-849-5304, dkennedy@gibsondunn.com)
Ari Lanin - Los Angeles (+1 310-552-8581, alanin@gibsondunn.com)
Robson Lee - Singapore (+65 6507 3684, rlee@gibsondunn.com)
Carrie M. LeRoy - Palo Alto (+1 650-849-5337, cleroy@gibsondunn.com)
Alexander H. Southwell - New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33 180, mwalther@gibsondunn.com)

Attorney Advertising: The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice.