<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Article</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOREWORD</td>
<td></td>
<td>Balancing Public Health and Individual Privacy</td>
</tr>
<tr>
<td>SPECIAL NOTE</td>
<td></td>
<td>Why Knowledge Sharing is the Only Way Forward</td>
</tr>
<tr>
<td>JANUARY 2019</td>
<td></td>
<td>EU Proposes New Rules for Open Data</td>
</tr>
<tr>
<td>FEBRUARY 2019</td>
<td></td>
<td>Pentagon Releases its AI Strategy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ESA Nod to More Funds for Copernicus Program</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Saudi Arabia Releases its Cloud First Policy</td>
</tr>
<tr>
<td>MARCH 2019</td>
<td></td>
<td>Canada Releases New Space Strategy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UAE Approves New Space Strategy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UKSA Comes Out with Post-Brexit Prospects</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Singapore Proposes Taskforce for AI Growth</td>
</tr>
<tr>
<td>APRIL 2019</td>
<td></td>
<td>Singapore Ups Investment in Digital Innovation</td>
</tr>
<tr>
<td>MAY 2019</td>
<td></td>
<td>Angola Gives Nod to National Space Strategy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Malaysia Decides to Build Its First AI Park</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UK Plans to Boost Security of IoT Devices</td>
</tr>
<tr>
<td>JUNE 2019</td>
<td></td>
<td>G20 Forms Guiding Principles for AI Use</td>
</tr>
<tr>
<td></td>
<td></td>
<td>India Rolls Out its Data Protection Bill</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New York Implements the Shield Act</td>
</tr>
<tr>
<td>AUGUST 2019</td>
<td></td>
<td>Brazil Sets Up National Data Protection Agency</td>
</tr>
<tr>
<td>NOVEMBER 2019</td>
<td></td>
<td>FCC Enforces New Rules for Vertical Location</td>
</tr>
<tr>
<td>DECEMBER 2019</td>
<td></td>
<td>FAA Proposes Remote ID for Drones</td>
</tr>
<tr>
<td>JANUARY 2020</td>
<td></td>
<td>US Curbs Geospatial Imagery Software Export</td>
</tr>
<tr>
<td></td>
<td></td>
<td>California Enforces Consumer Privacy Act</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NIST Releases Framework for Ethical Data Use</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Crucial Space Bill Delivered to Congress</td>
</tr>
<tr>
<td>FEBRUARY 2020</td>
<td></td>
<td>European Commission Proposes AI Regulations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>South Korea Plans to Tighten Drone Laws</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Singapore Plans to Boost Cybersecurity</td>
</tr>
<tr>
<td>MARCH 2020</td>
<td></td>
<td>Bill to Create Data Protection Agency in US</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US Releases Strategy for 5G Security</td>
</tr>
<tr>
<td>COVID-19 EFFECT</td>
<td></td>
<td>China Uses Surveillance Tech to Contain Cases</td>
</tr>
<tr>
<td>MARCH 2020</td>
<td></td>
<td>EU Relaxes Privacy Rules to Manage Outbreak</td>
</tr>
<tr>
<td>APRIL 2020</td>
<td></td>
<td>UK to Use Personal Data to Combat Virus</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US Looks to Use Phone Data to Fight Pandemic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nations Use Surveillance to Limit Spread of Virus</td>
</tr>
</tbody>
</table>
Balancing Public Health and Individual Privacy

My goodness, as we look at today, last month, and last year, would you have ever expected that the global situation would have changed so much? The daily, weekly and monthly impacts that we are experiencing due to the global Coronavirus pandemic are staggering – a situation that was barely identified as we entered 2020. And yet, in a relatively short amount of time, the geospatial community has responded like it does after every natural disaster – with applications and tools for preparedness, response, recovery and mitigation.

Ironically, many of these applications are resulting in increased focus and attention on the sometimes-delicate balance between protecting public health and protecting personal privacy. The Coronavirus-related posts in this Annual Summary of Policy Watch will show what some countries are doing in this regard, e.g. China, Hong Kong, Israel, Singapore and South Korea are using data to track movement and/or purchases of individuals; in Italy, mobility flows, individual mobility and contact patterns have been used to make a first estimate of intervention effectiveness; in Austria and Germany, the network operators/telecom companies have passed along anonymized data to the government; in The Netherlands, coronavirus has been added to the Public Health Act; in Europe, even though the General Data Protection Regulation (GDPR) allows relaxing some prior-consent requirements under “public-interest” circumstances, the European Data Protection Board has emphasized the need to anonymize or obtain prior consent to help manage the outbreak; and in the U.K. and U.S., discussions with the telecom and/or technology giants and health officials are occurring to determine how best to map the virus, noting that specific concerns have been raised by Congress (in the U.S.) to ensure the protection of personal privacy.

As one person mentioned recently on a WGIC telecon, the WGIC Policy Report 2020-01 titled, Geospatial Information and Privacy: Policy Perspectives and Imperatives for the Geospatial Industry could not have been more timely. While much of our attention is appropriately focused on the global pandemic, please take some time to review the other highlights contained herein. During this past year, there have been numerous and substantial policy advances globally. Included among them are: Artificial Intelligence (AI) efforts in Europe, Malaysia, Singapore, the U.S., and at the G20 level; further efforts to regulate drones and unmanned aerial vehicles (UAVs) in South Korea and the U.S.; new or strengthened space strategies in Angola, Canada, Europe, the U.A.E., U.K. and the U.S.; and additional privacy and/or data protection regulations or legislation in Brazil, India, and the U.S. (nationally, and in California and New York State).

In closing, this is a good time to reflect upon the role that the global geospatial community plays in protecting both public health and personal privacy. While, as indicated above, this is sometimes a delicate balance, I am confident that the professionals in this field can responsibly strike that balance. As always, we are open to your feedback, and most importantly, stay healthy.

Barbara J. Ryan
Why Knowledge Sharing is the Only Way Forward

We live in a highly interconnected and digitalized world, where almost every major decision, legislation and policy by a big economy has a ripple effect across geographies and markets. In this scenario, the geospatial industry, which has been growing exponentially in the last few years, has a very important role to play in building and strengthening knowledge economies, and ensuring sustainable development for all. So, any major policy decision in the geospatial ecosystem — by government or private players — impacts not only the industry, but also affects the global economy and society.

That is why, it is imperative to dig deeper into major policies/decisions and observe new and recurring trends that may go on to shape the future. When it comes to emerging technologies like 5G, Artificial Intelligence and IoT, most government regulations aim to spearhead fast deployment, reduce bottlenecks, incentivize R&D and make products more scalable. These policies and guidelines are instrumental in the formation of similar laws in other parts of the world, thereby encouraging knowledge sharing.

Once there is consensus among the decision-makers on key issues such as ensuring data privacy and ethical use of AI, the next step is standardization of protocols, which benefits both enterprises as well as consumers. Knowledge dissemination coupled with thorough and progressive policies ensure propriety, safety and ethics, apart from providing the broader business direction. For instance, the European Union’s General Data Protection Regulation (GDPR) was the pioneer and the gold standard of data privacy, and within just a few years, it has become the prototype for several other significant privacy legislations worldwide.

In the wake of growing global uncertainties due to the COVID-19 outbreak, knowledge sharing, technological cooperation and widespread access is the only way forward. The World Geospatial Industry Council (WGIC), which is a consortium of geospatial companies dedicated towards advancing the role of geospatial industry in the world economy and society, aims to forward its mission of knowledge sharing through this comprehensive Annual Edition of Policy Watch.
EUROPEAN UNION

In January 2019, the European Commission issued a new set of rules for Open Data and Public Sector Information. The new rules mandated the identification of relevant datasets which have a high commercial potential and may lead to the creation of region-wide products and services, information-based projects and the development of AI. It is important to note that the datasets mentioned in these rules include both statistical and geospatial data.

The new rules also mandate reworking the exceptions that currently permit public bodies to charge for the dissemination and use/reuse of data provided by them. Moreover, the idea is to expand the directive’s scope to data held by public undertakings and research data resulting from public funding; and increase transparency between public and private sector organizations.

Likely Impact

Easy access to public statistical and geospatial data
Ease of use and reuse of spatial data
More entrepreneurship and innovation opportunities in emerging technologies
New applications, products and services for socio-economic-environmental development
In February 2019, the Department of Defense released a report outlining the need to incorporate Artificial Intelligence into its strategy. The Pentagon was working towards using AI in almost all military operations, from intelligence gathering operations to maintenance problems requiring prediction models. The AI strategy implementation is focused on protecting tactical networks and preventing cyberattacks.

The strategy would help prepare for any conflict that may occur with other nations that are AI-ready. The American AI Initiative Executive Order called for the administration to “devote the full resources of the federal government” to help fuel AI innovation. Nation-wide investments in Machine Learning were expected to be affected, as intelligent solutions and predictive analysis become critical for both public and private sectors.
At the 11th European Space Policy Conference, the Third Amendment of the EU-ESA Copernicus Agreement was signed, resulting in an additional €96 million (US $108.45 million) for ESA’s space component budget for the Copernicus Program.

The additional budget builds upon the 2014 agreement signed between the EU and ESA under which over €3 billion (US $3.39 billion) was allocated to manage and implement the Copernicus space component between 2014 and 2021. Under the seven-year plan of the EU, known as the Multiannual Financial Framework (MFF), nearly €4.3 billion (US $4.86 billion) was allocated for the Copernicus Program for this period. Out of this, around €3.15 billion (US $3.4 billion) is to be with ESA as the coordinator and operator of the Sentinel satellites until mid-2021.

The additional budget is targeted to develop the Sentinel-6 mission of Copernicus and ensure easy access to reliable and timely data to Copernicus users. Further, the budget shall enable innovation by way of creating a healthier economy for commercial users of Copernicus data.

Copernicus is making a step change in the way we care for the planet by providing reliable, timely and accurate services to manage the environment, understand and mitigate the effects of climate change and help respond to crises.

LOWRI EVANS
Director General of the EC Internal Market, Industry, Entrepreneurship and SMEs
The Kingdom of Saudi Arabia last year issued its Cloud First Policy for review. The Ministry of Communications and Information Technology (MCIT) had been considering a comprehensive legislation to boost the growth of the digital economy in the country, which would further allow for greater spending on IT and build the technological capacity to attract foreign investments.

The strategy deploys three levels of cloud computing: Private Cloud, Government/Community Cloud and Public Cloud.

The Public Cloud is meant to provide a platform to be used and managed by various entities, ranging from businesses to academic organizations, and can be a combination of any or all of these entities. The Public Cloud is typically served by global players (e.g. AWS, Google Cloud, Microsoft Azure) as well as local players (e.g. local telecom and ICT companies).

The model offers a plug-and-play approach, which would increase the speed of deployment of solutions. The policy also looks into the commercial aspect of Cloud adoption to ensure that it positively effects businesses and the selected model of Public or Hybrid cloud computing offers a cost-effective solution for organizations.
In early 2019, the Canadian government announced a national space strategy that recognized the strategic value of space and space exploration for Canada. The strategy was aimed at leveraging Canadian strengths like robotics, while advancing science and innovation in exciting areas in Artificial Intelligence and biomedical technologies.

The Strategy placed priority on harnessing space science and technology to address challenges on Earth, such as:

- Investing in satellite communications technologies for broadband, including connectivity in rural and remote regions;
- Exploring how the delivery of healthcare services in isolated communities can be improved through lessons learned in space;
- Funding the development and demonstration of lunar science and technologies in fields that include AI, robotics and health; and
- Leveraging the unique data collected from Canada’s space-based assets to grow businesses and conduct cutting-edge research, including about the impact of Climate Change on Earth's atmosphere

By aiming for the moon, we allow our children to reach for the stars. Space represents limitless possibilities and endless discoveries. For every astronaut we send to space, there are thousands of Canadians who are part of the journey. Canada's space strategy will foster our next generation of astronauts, engineers and scientists and will ensure Canadians and Canadian businesses benefit from the growing opportunities in the space economy.

**NAVDEEP BAINS**
Minister of Innovation Science and Economic Development
In March 2019, the United Arab Emirates (UAE) government approved and launched the National Space Strategy 2030. The strategy is expected to be treated as a framework for function and regulation. Apart from boosting private-public partnership, the strategy focuses on six objectives, 21 programs and 79 initiatives, which will benefit more than 80 entities in the UAE.

The space sector plays an important role in the National Innovation Strategy, which was highlighted as one of the seven innovation priority sectors of the country’s economy. Under the new strategy, the UAE Space Agency will also be responsible for international strategy development and cooperation with over 20 space agencies and centers.
With the confirmation of Brexit, the UK Space Agency (UKSA) realized the need to strengthen the local space industry to achieve its commercial launch ambitions. The launch of a new webpage, LaunchUK, on the official government website (gov.uk) was seen as the first effort to provide insights on critical space legislations and latest statistics concerning the space industry.

The official LaunchUK prospectus highlights the UK government’s investment of £5 billion in civil space activities between 1995 and 2015. The UKSA aims to increase the share of the country’s space industry in the global space economy from 6.5% to 10% by 2030. To further its vision, the UKSA has allocated £50 million (US $64.52 million) for a small satellite launch program, and another £600,000 (US $774,000) to the LaunchUK program.

### Three-stage Plan

**STAGE 1**

**MARKET CAPTURE (2019 TO 2020)**

Initiate commercial launch for a UK spaceport from 2020

**STAGE 2**

**MARKET DEVELOPMENT (2020 TO 2025)**

Encourage investments in developing additional space ports and creating advantages of domestic access to space

**STAGE 3**

**MARKET LEADERSHIP (2025 ONWARDS)**

Adopt new technologies, new innovation by pursuing new opportunities in the global market for sustainable and resilient growth of the UK commercial spaceflight market
SINGAPORE PROPOSES TASKFORCE FOR AI GROWTH

Last year, the Singapore government released a Model AI Governance Framework, articulating the key ethical principles that will lay the foundation for growth in the AI industry. An inter-agency taskforce was recommended for testing the scale and deployment of AI solutions on a trustworthy platform. The taskforce would help advance the requirements of AI being human-centric, transparent and fair.

Core Focus Areas

- Governance structures and measures
- Risk management in autonomous decision-making
- Operations management
- Customer relationship management

We need to double down on these efforts. This year, an inter-agency taskforce will study how Singapore will develop AI as a strategic capability and become a trusted global hub for test-bedding, deploying and scaling up AI solutions, especially in the context of a highly urbanized city like ours.

VIVIAN BALAKRISHNAN
Minister-in-Charge of The Smart Nation Initiative
SINGAPORE UPS INVESTMENT IN DIGITAL INNOVATION

In April 2019, Singapore decided to further invest US $222 million to boost research in innovation, specifically in areas including AI and 5G technologies, hoping to transform the government and the nation. The investment amount was to be allocated before the end of the National Research Foundation (NRF) five-year plan that ends in 2020.

The investment was to be augmented by a range of measures for spending and allocation to help smaller businesses align themselves digitally and help create a solid workforce. Singapore has plans to roll out AI and Cloud-based solutions to every business sector by 2020. The Infocomm Media Development Authority has formulated plans alongside these investments to roll out 5G technology and mobile phone networks by the deadline.

Investment in research and development is essential to help our industries innovate and stay competitive, even as technology rapidly evolves. It is the citystate’s vision that all businesses, workers and citizens are digitally connected and skilled.

S ISWARAN
Minister of Communications and Information
Angola, a country in southwestern Africa, has been a leader in multiple sectors ranging from healthcare to technology. In May 2019, the country’s National Space Program Management Office launched the 2019-2022 strategic plan, which augments the 2016-2025 National Space Strategy, the 2018-2022 National Plan and several other policies.

The Plan presents a strategic diagnosis for the revision and approval of the legislations that govern the space activities in the country, the construction, launch and operation of ANGOSAT-2 satellite, future satellites and studies for the implementation of the space agency.

**Areas of Focus**

1. A strategic diagnosis for the revision and approval of the legislative acts that govern the space activities in country

2. The construction, launch and operation of future satellites

3. To detail 14 growth and sustainability result-based performance indicators
MALAYSIA DECIDES TO BUILD ITS FIRST AI PARK

In May last year, Malaysia allocated Malaysian $1 billion (US $240 million) to establish an AI park. The park will be constructed by Malaysian and Chinese companies, including China Harbour Engineering Company, G3 Global and SenseTime. This will enable focused growth in building AI applications to take advantage of different growing technologies, including computer vision, speech recognition and natural language processing. The park will also serve as a base within the country to foster local talent and build a commercial ecosystem for AI research. The user domains in focus are government agencies, banking, manufacturing and finance.

A Cloud service and a research base platform, built by SenseTime, will be created to help support the park both before and after the construction. G3 Global will be responsible for industry partnerships and support. Malaysia, which already has a National Big Data Framework, was looking to introduce a national AI framework, enhancing the guidelines mentioned in the Big Data Framework.

The idea to set up the AI park is vital to building Artificial Intelligence research-related public service infrastructure as the base to promote AI technology in Malaysia. Also, this becomes a place for talents to be trained on AI and machine learning.

WAN KHALIK
WAN MUHAMMAD
Executive Chairman, G3 Global
In May 2019, the United Kingdom revealed its plans to update the Internet of Things (IoT) regulations, requiring the government to frame guidelines to ensure cybersecurity for all connected devices. The government was looking at introducing a labeling scheme, which would require all retailers to sell products with approved labels to ensure their safety. The scheme was to be supported by mandatory, device unique passwords and disclosure policies.

In January 2020, the government announced a draft law in this regard, with an eye on the IoT market that is expected to expand massively in the next few years. The updated regulations will not only address the issue of security of devices, but will also ensure sustained profitability for the industry. Prior to this, the average cost to businesses due to data loss owing to cyberattacks was £4,180 (US $5,298) in 2019, as against £3,160 (US $4,005) in 2018.
G20 FORMS GUIDING PRINCIPLES FOR AI USE

At the G20 Summit in Japan last year, representatives of the 20 major global economies formulated a set of guidelines for commercial construction and utilization of Artificial Intelligence. Though the guidelines were non-binding, they were focused around safety, transparency and responsible disclosure.

The guidelines suggested that the users and developers of AI must respect the rule of law and values, including privacy, equality, diversity and internationally recognized labor rights; commit to transparency and responsible disclosure; and ensure that AI systems are robust and secure.

Focus Areas
1. Long-term public investment and encouraging private investment in R&D
2. Supporting the transition of AI from R&D to deployment stage
3. Ensuring a fair transition for workers through training programs
INDIA ROLLS OUT ITS DATA PROTECTION BILL

The Indian Data Protection Bill, which includes the Geospatial Data Bill, underwent four rounds of consultations and changes, before being rolled out in June 2019. The Bill focuses on personal data — how individuals can control their data, what are the limits to access and how the same data has to be processed by all government and private entities both nationally and across borders.

The Bill also includes data security and the need for data anonymity. According to the government, in combination, these factors will ensure data availability, utility, innovation and localization.
NEW YORK IMPLEMENTS THE SHIELD ACT

On July 30, 2019, the New York state signed into law its Stop Hacks and Improve Electronic Data Security (SHIELD) Act. This legislation, which signals a new approach towards the issue of data privacy, requires companies to delete private information after it is no longer needed; designate one or more people for the security program; frequently test and monitor the effectiveness of data controls, systems and procedures; train employees in the security program; and assess risks in network and software design.

The Act is aimed at preventing data breaches that jeopardize the personal, financial and health information of people, as almost all organizations that gather and store personal data are vulnerable — especially since they share this data with contractors, vendors and other parties.
In 2019, Brazil created a National Data Protection Authority (ANPD), a segment of the federal government that is directly related to the President’s Office.

Though the ANPD reports to the President’s Office for all technical applications, the entity functions independently — and is free to evaluate and address all matters pertaining to data protection, privacy and sharing.
FCC ENFORCES NEW RULES FOR VERTICAL LOCATION

The Federal Communications Commission in November last year approved new rules that mandate wireless carriers to provide emergency callers (911) with the vertical location component that is accurate up to three meters. As per the new order, over 80% of indoor wireless 911 calls would have to incorporate a vertical or a ‘Z axis’ that is accurate till 3 meters. The fact sheet states that it is necessary for the carriers to abide by the new requirements till April 3, 2021 in the top 25 markets, and by April 3, 2023 in the top 50 markets.

The new 3-meter requirement is essential from the perspective of public safety because it denotes the approximate height of ceiling of floors in most multi-story buildings. Earlier, the carriers sought a 5-meter metric.

When you call 911 from a wireless phone in a multistory building — as many Americans do every day — it can be a challenge. First responders may know what building address you're calling from, but they might find it difficult to figure out which floor you're on. We aim to close this gap by adopting a vertical, or ‘Z-axis,’ location accuracy metric of plus or minus 3 meters for 80% of wireless E911 calls from Z-axis-capable handsets. This means that first responders will now be able to more accurately identify the floor level for most 911 calls and reduce emergency-response time.

AJIT PAI
FCC Chairman
On 26 December 2019, the US Federal Aviation Administration (FAA) released its proposal regarding remote identification rules for small unmanned aircrafts to ensure their safety. There are three methods that fulfill remote ID compliance: standard identification, limited identification and an ‘FAA-recognized identification’.

**METHODS OF IDENTIFICATION**

- **Standard identification** would either require a serial number assigned to the drone on production, or a session identification number assigned by a remote ID unmanned service supplier (USS).

- **In limited identification**, operators could broadcast their location, but operations would be limited to 400 feet.

- **FAA-recognized identification** would permit users to fly without remote ID capabilities, though they would not be allowed to venture beyond the visual line of sight.
US CURBS GEOSPATIAL IMAGERY SOFTWARE EXPORT

In January this year, the United States administration imposed restrictions on the export of AI-based geospatial imagery software. As per the new rule, companies now must apply for a license to export certain types of geospatial imagery software from the US to any country other than Canada. The directive, which came into effect on January 6, 2020, has been applied under a 2018 law called the Export Control Reform Act (ECRA). The measure covers software that could be used by sensors, drones and satellites to automate the process of identifying targets for both military and civilian use.

The measure is the first to be finalized by the US Department of Commerce from the 2018 law, which required the agency to write rules to boost oversight of exports of sensitive technology for economic and security reasons. The restriction only applies to software with a graphical user interface — a feature that makes programs easier for non-technical users to operate.

Restrictions have been imposed on the geospatial imagery “software specially designed” for training a deep convolutional neural network to automate the analysis of geospatial imagery and point clouds, and having all of the following:

- Provides a graphical user interface that enables the user to identify objects (e.g., vehicles, houses, etc.) from within geospatial imagery and point clouds in order to extract positive and negative samples of an object of interest
- Reduces pixel variation by performing scale, color, and rotational normalization on the positive samples
- Trains a deep convolutional neural network to detect the object of interest from the positive and negative samples
- Identifies objects in geospatial imagery using the trained deep convolutional neural network by matching the rotational pattern from the positive samples with the rotational pattern of objects in the geospatial imagery
The California Consumer Privacy Act (CCPA) came into effect on January 1, 2020. It is the most comprehensive US legislation so far on privacy, covering all aspects of data protection. As per the Act, a consumer has the right to request a business that collects personal information to disclose it. Also, the business has to intimate the customer about the purpose for which data is being collected.

**CCPA Applies to Any Firm That**

1. Operates in California and has an annual revenue of $25 million
2. Gathers data of more than 50,000 users
3. Half of whose revenue is based on data
On Jan 16, 2020, the National Institute of Standards and Technology (NIST), which is a non-regulatory agency of the US Department of Commerce, released the first draft of a new privacy framework. With the privacy issue continuing to spark debate and the call for ethical use of data growing louder, the proposed framework will help balance privacy with innovation and enable small businesses to develop privacy standards.

Getting privacy right will underpin the use of technologies in the future, including AI and biometrics, quantum computing, the Internet of Things and personalized medicine. These technologies will be a big part of our future.

WALTER COPAN
NIST Director
CRUCIAL SPACE BILL DELIVERED TO CONGRESS

The proposal on how space force would be organized was delivered to the US Congress on February 3, 2020. US President Donald Trump signed the NDAA (National Defense Authorization Act) for 2019 that mandates the creation of US Space Force as the sixth wing of the armed forces. A major chunk of the Space Force funding initially will be from the Air Force.

Our reliance on space-based capabilities has grown dramatically and today outer space has evolved into a warfighting domain of its own. Maintaining American dominance in that domain is now the mission of the United States Space Force.

MARK ESPER
Defense Secretary
In February 2020, the European Commission announced its plan to regulate AI by drafting new laws, including prohibiting use of AI systems used in self-driving cars, medical devices, etc. that humans can’t interpret. The commission envisages a framework for reliable Artificial Intelligence. Its aim is to mobilize resources along the entire value chain and to create the right incentives to accelerate deployment of AI, including by small and medium-sized enterprises. The commission will come up with an “action plan” for integrating AI into public services and updating its 2018 AI development strategy.

We want every citizen, every employee, every business to stand a fair chance to reap the benefits of digitalization, whether that means driving more safely or polluting less thanks to connected cars; or even saving lives with AI-driven medical imagery that allows doctors to detect diseases earlier than ever before.

MARGRETHE VESTAGER
Executive Vice-President for A Europe Fit for the Digital Age
South Korean drone operators will have to register drones that weigh more than 2kg. Earlier, drones that weighed less than 12kg were exempted from registration. The new law, which will be promulgated in May this year, will come into effect on 1 January 2021, said the Ministry of Land, Infrastructure, and Transport.

The regulation has been introduced due to an increase in the number of drone accidents. The registration process would be done online and testing and licensing for drones that weigh over 250 grams would also become compulsory. Currently, in several countries like the United States, Germany and Australia, all drones weighing over 250 grams have to be registered.

The latest road map (for UAVs) reflects the considerable growth potential of drones and highlights the country’s commitment to meet the needs of the industry.

KIM HYUN-MEE
Minister of Land, Infrastructure & Transport, South Korea
SINGAPORE PLANS TO BOOST CYBERSECURITY

In its 2020 annual budget, the Singapore government has earmarked SG$1 billion to bolster its cybersecurity systems, while simultaneously looking forward to embrace technologies like AI and IoT. Enhancing cyber and data security capabilities would enable protecting critical information along with citizens’ data.

The amount allocated would be spent over the next three years as digitalization gains momentum. The government also plans to invest in deep tech startups. Data security is a key enabler and vital prerequisite of Singapore’s digital economy. To enhance its cybersecurity capabilities, the island nation had set up a Cyber Security Agency (CSA) in 2015 and passed the Cybersecurity Act in 2018.

Protecting Singapore remains a high priority and efforts to do so must be funded adequately. We must also be prepared to deal with cyber threats as digitalization becomes more pervasive.

HENG SWEE KEAT
Finance Minister, Singapore
Bill to create data protection agency in US

Senator Kirsten Gillibrand (NY-D) has authored and sponsored a bill ‘Data Protection Act 2020’ that calls for the creation of a federal data protection agency responsible for enforcing data privacy in the country. The senator believes that the US is far behind other countries when it comes to comprehensive data protection. If enacted as a law, the newly created agency would be empowered to judge privacy violations and launch investigations against companies accused of wrongdoings. The agency would also have the power to impose fines of up to $1 million a day on companies that default.

Data has been called the new oil. Companies are rushing to explore and refine it, ignoring regulations, putting profits above responsibility, and treating consumers as little more than dollar signs. Like the oil boom, little thought is being given to the long-term consequences.

Kirsten Gillibrand
Senator (NY-D)
US RELEASES STRATEGY FOR 5G SECURITY

In the last week of March this year, the White House released the National Strategy to secure 5G which focuses on how the US will safeguard its 5G infrastructure. The policy document highlights President Trump’s vision to lead the development, deployment and management of secure and reliable 5G communications infrastructure globally. The release of the strategy demonstrates the first move by the US President to fulfill all the requirements mentioned in the Secure 5G and Beyond Act, which has got his nod.

The strategy aims to facilitate the domestic rollout of 5G; assess the risks and identify the core security principles of 5G infrastructure; assess the risks to United States economic and national security during development and deployment of 5G infrastructure worldwide; and promote responsible global development and deployment of 5G.

Fifth generation wireless technology, or 5G, will be a primary driver of the Nation’s prosperity and security in the 21st century. This new technology will provide consumers, businesses, and governments with remarkably fast network connections that will enable tens of billions of new devices to harness the power of the Internet, transforming the way we live, work, learn, and communicate.

DONALD TRUMP
US President
The COVID-19 global pandemic has forced decision-makers to break out of their comfort zone and find innovative ways to tackle the spread of the virus. This has led to extensive use of contact tracing technology with the help of location tracking and analysis. Keeping aside privacy concerns, several countries in the world are currently using people’s data to combat the Novel Coronavirus.
CHINA USES SURVEILLANCE TECH TO CONTAIN CASES

Utilizing its sophisticated and expansive surveillance network for the public good, the Chinese government joined hands with tech giants Alibaba and Tencent to develop a color-coded health rating system that is tracking millions of people daily. The smartphone app was first deployed in Hangzhou in collaboration with Alibaba. It assigns three colors to people — green, yellow or red — on the basis of their travel and medical history. Whether a person should be quarantined or allowed in public spaces is decided based on the color code.

Smartphone apps are also being used to keep track of peoples’ movements and ascertain whether or not they have been in contact with an infected person. With the help of data analytics and predictive models, medical professionals are able to understand more about this, and other diseases.

Technology to the Rescue

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color coding</td>
<td>AI</td>
<td>Big Data</td>
<td>Drones</td>
<td>Location Tracking</td>
</tr>
<tr>
<td>There are three color codes — Red, Yellow, Green. Only those who have been given a green color code are allowed in public spheres after using the designated QR code at metro stations and offices.</td>
<td>By using predictive modeling, healthcare professionals are able to understand the disease better.</td>
<td>Several organizations are developing COVID-19 dashboards using Big Data.</td>
<td>Drones are transporting both medical equipment and patient samples, thus saving time, enhancing the speed of delivery and preventing the risk of contamination.</td>
<td>The administration is collecting people’s smartphone location data, body temperatures, travel history and other details in a centralized database, in which the data is being analyzed using Big Data and Machine Learning.</td>
</tr>
</tbody>
</table>
In the European Union, there are strict requirements that apply to the processing of health and location data. Organizations can process health data under the General Data Protection Regulation (GDPR) without the consent of data subjects, but only if this is necessary for reasons of “public interest”.

The European Data Protection Board has recently emphasized the need to anonymize location data or obtain prior authorization. As a result of which, EU Member States’ governments and market parties are prone to look for privacy-friendly alternatives. Good examples for this are apps that work on the basis of prior authorization. On March 23, the European Commission urged some of Europe’s telecom giants, including Deutsche Telekom and Orange, to share anonymized and aggregated mobile phone big data.

AT A GLANCE

1. **Italy**
   ISI Foundation and consumer insights company Cuebiq collaborated to make a first quantitative assessment of the impact of these interventions. They went by mobility flows, individual mobility and contact patterns.

2. **Austria**
   As, the country’s biggest network operator, passed on anonymized data to the government, which comprises more than 20 million people.

3. **The Netherlands**
   In the Netherlands, the Public Health Act is the basis for data processing in the event of a threat to public health. The virus has been added to this via a new ministerial emergency regulation.

4. **Germany**
   Deutsche Telekom wishes to support the national health organization, the Robert Koch Institute (RKI), in containing the Coronavirus. The mobile operator has apparently already handed over part of its customer data to the federal authority in an anonymous form.
UK TO USE PERSONAL DATA TO COMBAT VIRUS

The UK government can officially collect personal data from citizens’ smartphones to combat the COVID-19 outbreak, as per the country’s privacy watchdog. It has been reported that the government was in deliberations with leading telecom companies, including British Telecom to leverage location data for real-time tracking and mapping of the virus-affected regions. The Information Commissioner’s Office (ICO), which regulates privacy in the country, said that the magnitude of the outbreak may call for the use of personal data. The ICO has also clarified that the existing laws do not restrict the government or state healthcare organizations from broadcasting health-related information to the public.

Data protection is not a barrier to sharing data. Public bodies may require additional collection and sharing of personal data to protect against serious threats to public health. Data protection law enables the data sharing in the public interest and provides the safeguards for data that the public would expect.

ICO SPOKESPERSON
US LOOKS TO USE PHONE DATA TO FIGHT PANDEMIC

It is reported that the US government is in deliberations with tech giants like Facebook, Google and other healthcare experts to figure out how location data from smartphones can be utilized to fight the pandemic. Healthcare experts are showing keen interest in the compilation of anonymized and aggregated data that can be used to map the virus, track people and identify hotspots.

Google has launched Verily, a website that directs potential patients in the San Francisco area to COVID-19 testing sites. The site has raised privacy concerns due to its requirement that patients have a Google account, and led Senators Kamala Harris (D-Calif.) and Cory Booker (D-NJ) to question Google on whether data it gathers could be used for commercial purposes.

The US Center for Disease Control and Prevention has also become digital to track the spread of COVID-19. Over $500 million have been allocated for the upgrade of CDC’s public health data surveillance and analytics infrastructure.

Unless carefully circumscribed, location data can reveal deeply sensitive information about people’s private lives. The Administration must take extreme care not to implement location data-use policies that run the risk of violating Americans’ privacy.

ED MARKEY
Senator (D-Mass.), Massachusetts
The increase in the Novel Coronavirus cases around the world has prompted several countries like Singapore, Israel, and South Korea to use “people’s data” to ensure their safety. In Singapore, the government has rolled out an app that uses Bluetooth signals between cell-phones to see if potential carriers of the virus have been in close contact with other people.

In South Korea, there have been reports of the government using records such as credit card transactions, smartphone location data and CCTV videos to build a system to track COVID-19 cases. In Hong Kong, people were made to wear wristbands linked to a smartphone app that could alert authorities if a person left quarantine.

Meanwhile, in Israel, the authorities are using citizens’ cell phone location data to track where they have been so they can enforce quarantine controls and monitor the movements of those infected.

How are governments using location tracking in combination with personal data to track and combat COVID-19?