Date: June 17, 2021

AI Regulations in Health and Data Governance

Challenging Africa to Be Better than the West

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

AI in Healthcare

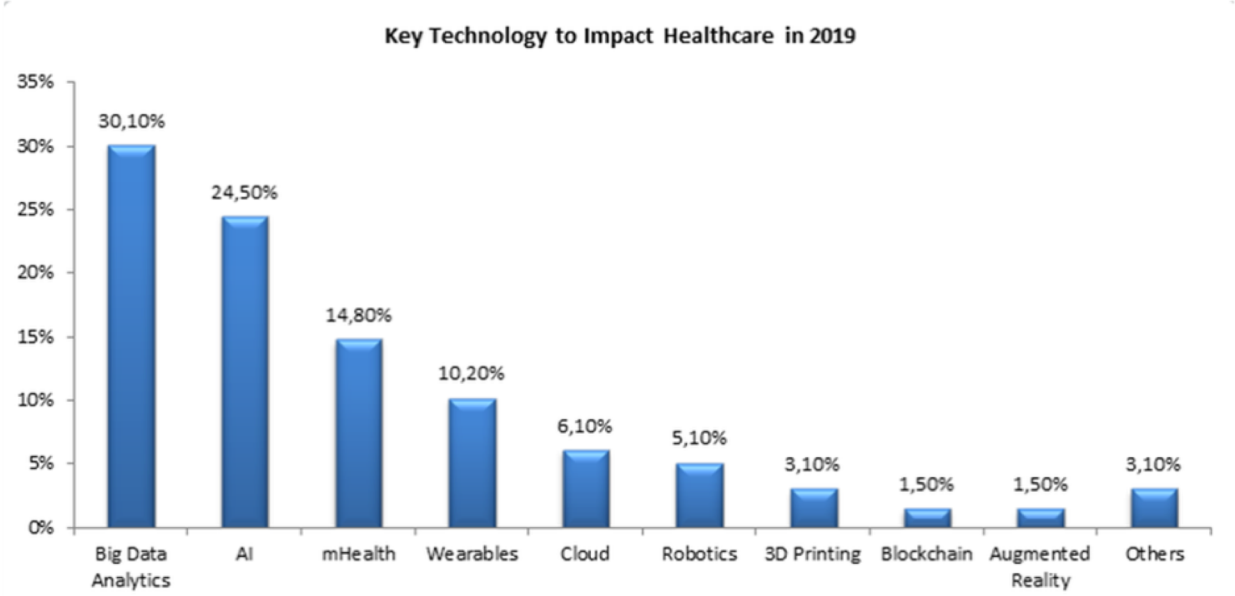
"The potential of AI in health is profound... AI is a 'general purpose' technology that can be deployed in just about any facet or activity of the health industry, from clinical decision-making and public health, to biomedical research and drug development, to health system administration and service redesign… this is a major opportunity to improve health outcomes and value for money."

"Trustworthy AI in Health", OECD, April 2020

eWORLDWIDE GROUP

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

Growth Predicted by the Private Sector

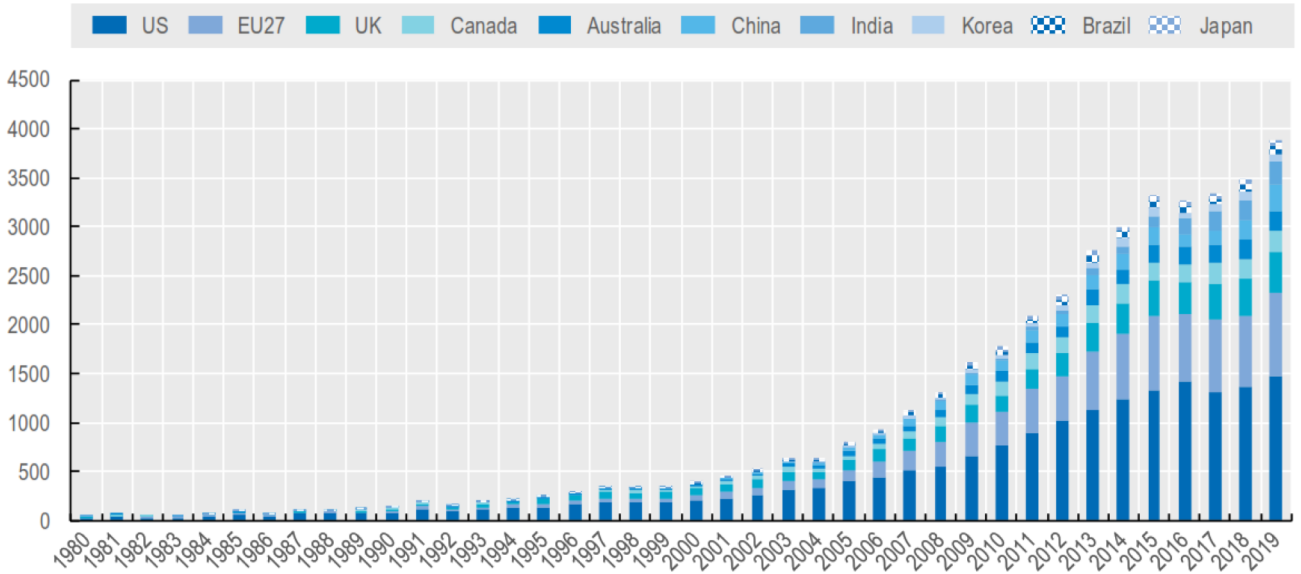


Source: https://www.forbes.com/sites/reenitadas/2019/02/04/the-top-five-digital-health-technologies-in-2019/#2a6bc4146c0f

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

AI is Booming

Number of relevant scientific publications in health, by country, from 1980 to 2019



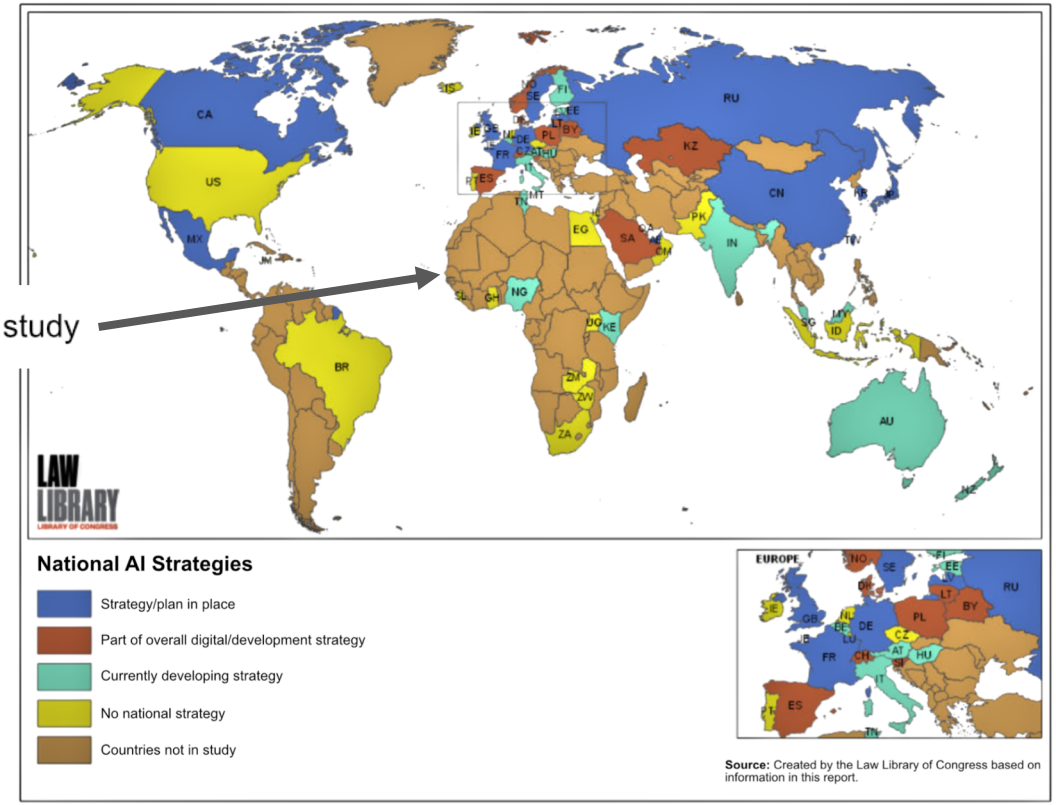
Note: Please see methodological note (https://www.oecd.ai/assets/files/Methodology_20200219.pdf) for more information.
Source: OECD.AI (2020), visualisations powered by JSI using data from MAG, accessed on 3/3/2020, www.oecd.ai

Source: "Trustworthy AI in Health", OECD, April 2020

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

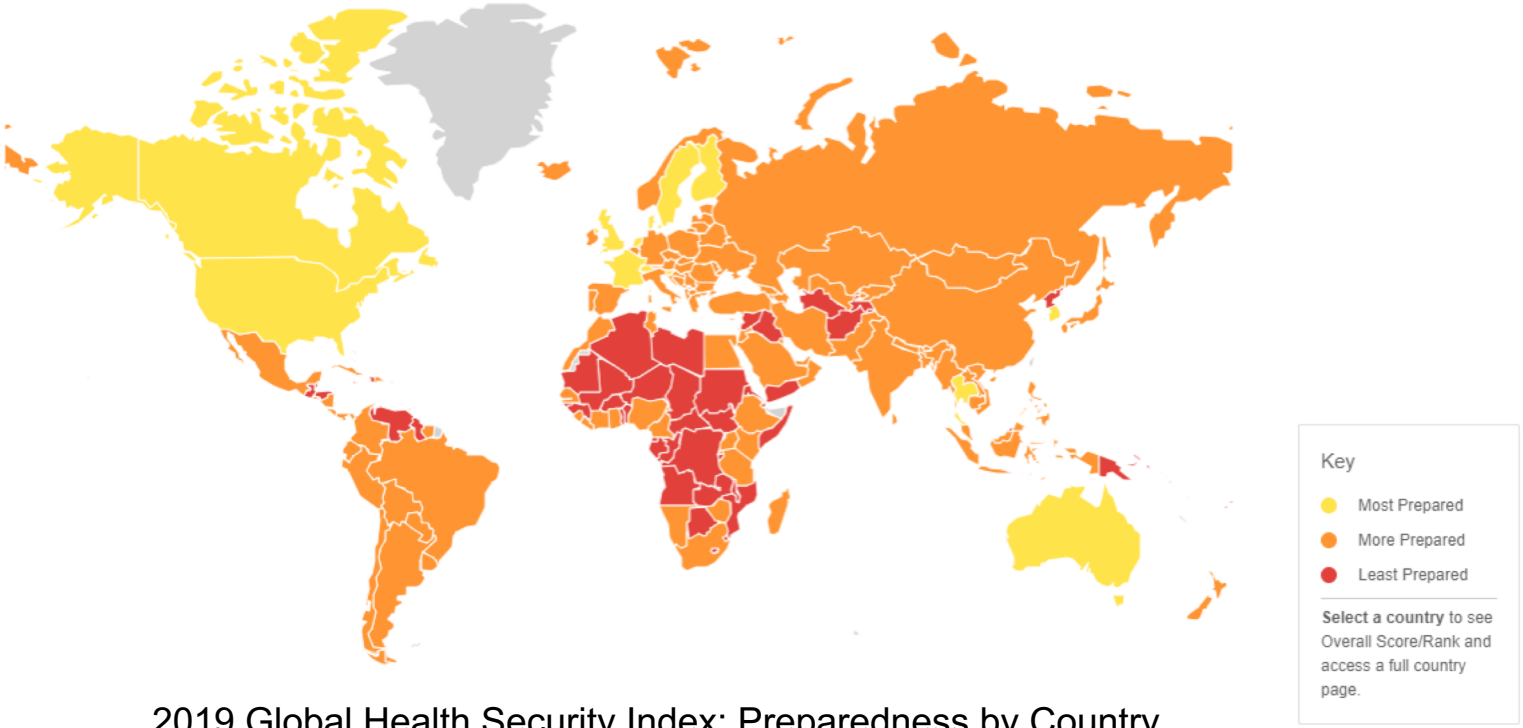
AI is Booming… but...

Countries not in study



Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

A Clear Lesson from COVID-19

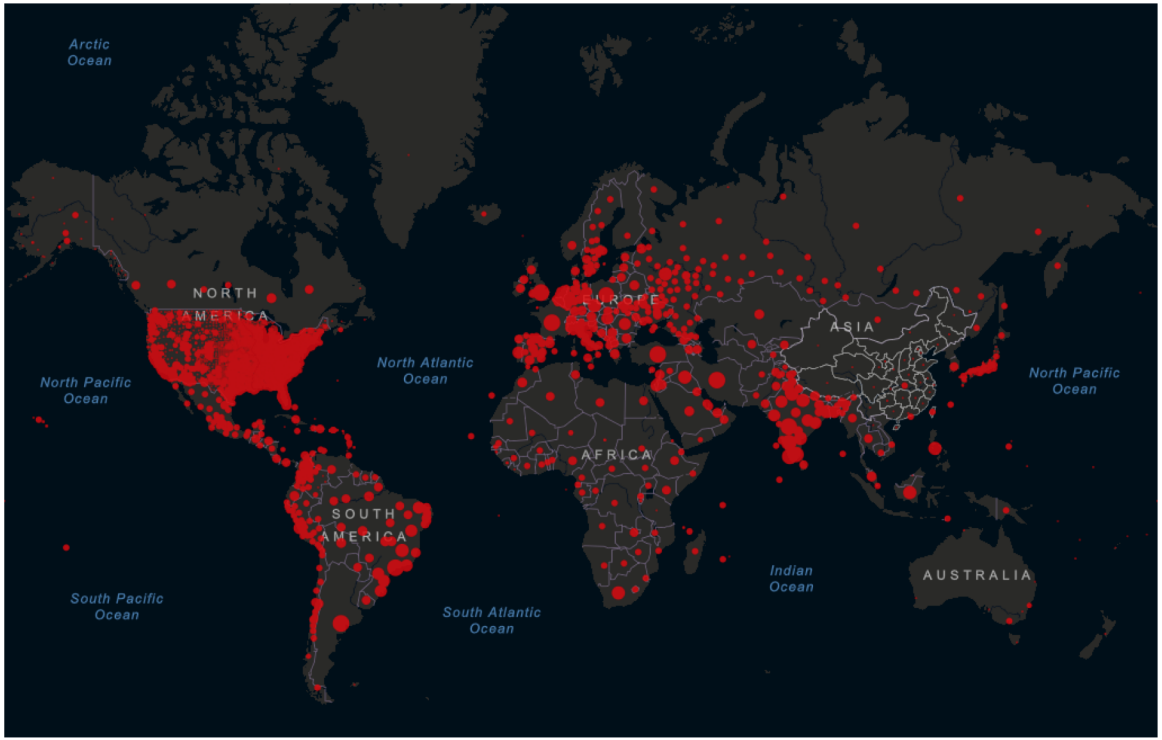


2019 Global Health Security Index: Preparedness by Country

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

Source: https://www.ghsindex.org/

A Clear Lesson from COVID-19



COVID-19 Dashboard
by the Center for Systems
Science & Engineering,
Johns Hopkins University

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

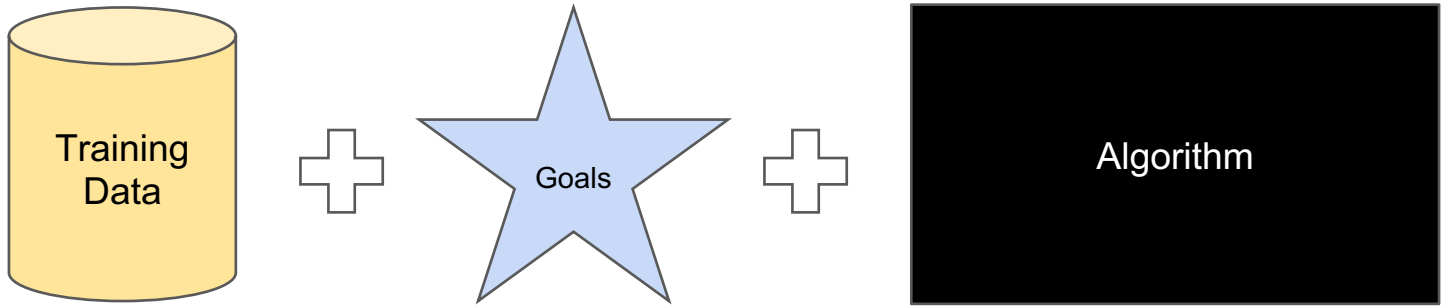
Source: https://coronavirus.jhu.edu/map.html

Defining Artificial Intelligence

Definition:

"Artificial Intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals."

High-Level Expert Group on AI, European Commission



Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

Downplaying the Risks

“The report does not attempt to cover all facets of this complex issue, in particular the ethics of AI or managing AI-related risks”

Transforming healthcare with AI, McKinsey & Company, March 2020

“attempts to regulate ‘AI’ in general would be misguided, since there is no clear definition of AI (it isn’t any one thing), and the risks and considerations are very different in different domains”,

One Hundred Year Study on Artificial Intelligence, Stanford University, 2016

eWORLDWIDE GROUP

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

Incomplete Training Data

The tractor trailer was turning and the training data mostly used images of the fronts and backs of tractor trailers.

This left the AI unable to identify the threat, resulting in loss of life.

When an AI makes a bad decision based on poor data, who is at fault?

Tesla driver dies in first fatal crash while using autopilot mode

The autopilot sensors on the Model S failed to distinguish a white tractor-trailer crossing the highway against a bright sky

Danny Yadron *and* Dan Tynan *in San Francisco*

Thu 30 Jun 2016 19.14 EDT

▲ Joshua Brown, the first person to die in a self-driving car accident. Photograph: Facebook

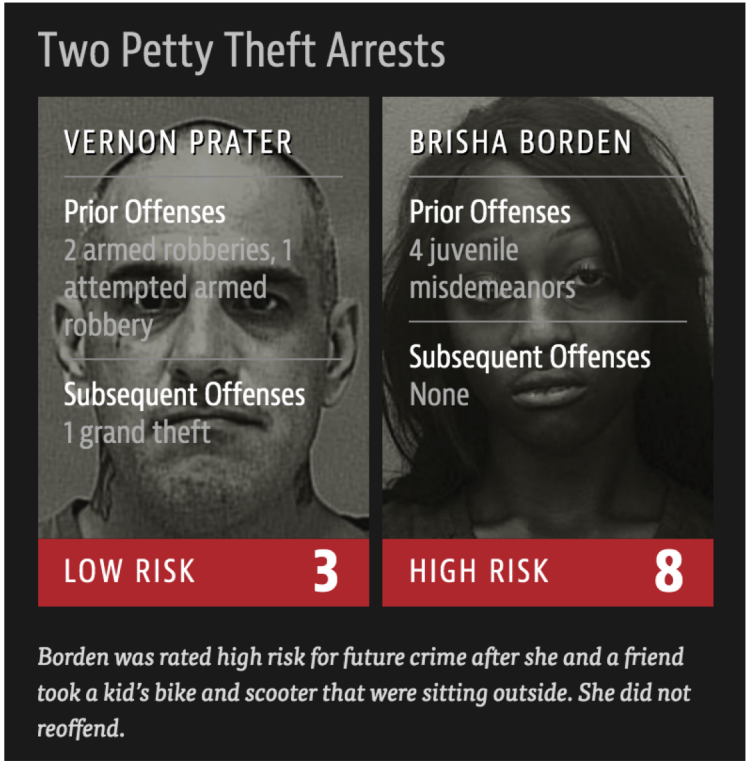
Source: https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

Biased Training Data

COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) is used to provide judges with guidelines for criminal sentencing.

“Black defendants were twice as likely as white defendants to be misclassified as a higher risk of violent recidivism, and white recidivists were misclassified as low risk 63.2 percent more often than black defendants.”



Source: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

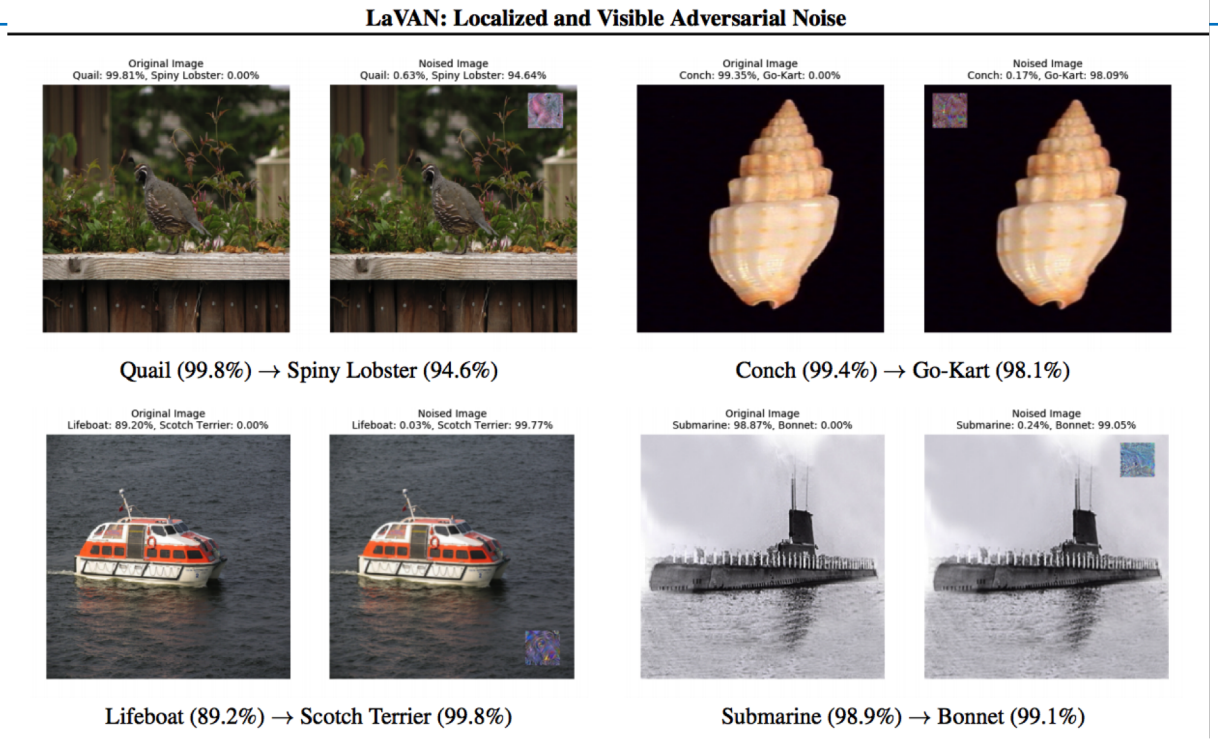
Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

Exploitable Data

Minor changes to these images completely corrupts the ability of the AI to recognize the object.

This type of *adversarial attack* could be used to commit fraud.

Doctors could use this to fake positive outcomes in clinical trials, increase the number of procedures performed, or otherwise manipulate the system.



Source: LaVAN: Localized and Visible Adversarial Noise | https://arxiv.org/pdf/1801.02608.pdf

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

Unintended Consequences

In the first case, a clear goal led to unexpected behavior.

In the second case, the goal to find the route with the least traffic led to nav systems suggesting dangerous routes.

Unintended Consequences in Healthcare

He and his colleagues had one such problem in their their study with rulers. When dermatologists are looking at a lesion that they think might be a tumor, they'll break out a ruler—the type you might have used in grade school—to take an accurate measurement of its size. Dermatologists tend to do this only for lesions that are a cause for concern. So in the set of biopsy images, if an image had a ruler in it, the algorithm was more likely to call a tumor malignant, because the presence of a ruler correlated with an increased likelihood a lesion was cancerous. Unfortunately, as Novoa emphasizes, the algorithm doesn't know why that correlation makes sense, so it could easily misinterpret a random ruler sighting as grounds to diagnose cancer.

Source: "Dermatologist-level classification of skin cancer with deep neural networks" Andre Esteva et al, Nature, Feb 2017

eWORLDWIDE GROUP

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

AI, Data & Privacy: The Need for Governance

AI uses vast amounts of data. This **directly conflicts** with preservation of privacy.

An Example:

1. We would like to record/copy all of your conversations on Facebook, Twitter, Instagram, etc., and combine that with comments on blogs, news articles and online forums.
2. Based on what we hear, we will decide what to tell you about situation X.

Does this sound acceptable to you?

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

COVID-19 Privacy Issues

The New York Times

Major Security Flaws Found in South Korea Quarantine App

The defects, which have been fixed, exposed private details of people in quarantine. The country has been hailed as a pioneer in digital public health.

He found that the software's developers were assigning users ID numbers that were easily guessable. After guessing a person's credentials, a hacker could have retrieved the information provided upon registration, including name, date of birth, sex, nationality, address, phone number, real-time location and medical symptoms.

With such weak encryption, monitoring all of the app's communications with the server would be possible simply, for instance, by being on the same unprotected Wi-Fi network as someone else using the app.

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

KAISER FUNG IDEAS 05.13.2020 08:00 AM

Beware the Lofty Promises of Covid-19 'Tracker' Apps

A popular symptom-tracking app made a splash for its surprising discoveries. But a deeper look at the data calls those findings into question.

COVID-19 contact tracing apps create privacy pitfalls around the world

Two presentations at the Defcon security conference show that government apps consume an unhealthy amount of data.

Laura Hautala Aug. 8, 2020 5:00 a.m. PT

LISTEN - 04:39

Public health experts rushed to create contact tracing apps in countries all over the world this spring. They serve an important purpose in determining who might've been exposed to the novel coronavirus so they can be tested and isolated. But the risks were clear too. Contact tracing apps have the power to amass personal data that reveals your movements, activities and relationships.

Qatar: Contact tracing app security flaw exposed sensitive personal details of more than one million

26 May 2020, 18:42 UTC

Serious security vulnerabilities in Qatar's mandatory contact tracing app, uncovered by Amnesty International, must act as a wake-up call for governments rolling-out COVID-19 apps to ensure privacy safeguards are central to the technology.

An investigation by Amnesty's Security Lab discovered the critical weakness in the configuration of Qatar's EHTERAZ contact tracing app. Now fixed, the vulnerability would have allowed cyber attackers to access highly sensitive personal information, including the name, national ID, health status and location data of more than one million users.

> "While the Qatari authorities were quick to fix this issue, it was a huge security weakness and a fundamental flaw in Qatar's contact tracing app that malicious attackers could have easily exploited."
>
> Claudio Guarnieri, Head of Amnesty International's Security Lab.

Sources:
https://www.nytimes.com/2020/07/21/technology/korea-coronavirus-app-security.html
https://www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/
https://www.cnet.com/news/covid-contact-tracing-apps-bring-privacy-pitfalls-around-the-world/
https://www.wired.com/story/beware-the-lofty-promises-of-covid-19-tracker-apps/

eWORLDWIDE GROUP

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

COVID-19: A Broader Perspective on AI & Data Privacy

Pros

- AI used for COVID-19 management, mitigation, response and vaccine research.
- Highlighted growing concerns about data privacy, security, transparency, ownership, destruction and data governance.
- New laws, regulations, bills and acts got fast tracked.
- New data governance models have been discussed.

Cons

- Many new tools have had significant privacy breaches, exposing sensitive personal data .
- Concern is being downplayed by governments (“in the public interest”), and also by Big Tech (“not our problem”).
- Are these new laws reasonable and well thought out?
- Have new data governance models been implemented?

eWORLDWIDE GROUP

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

What About AI in Africa?

1. Developing National AI Strategies:
   - Botswana, Egypt, Mauritius, Tunisia, Zambia.
2. Establishing AI Agencies, Task Forces and Commissions
   - Egypt, Kenya, Mauritius, Nigeria, South Africa, Tunisia, Uganda.
3. Amending Existing Laws and Creating New Regulations
   - Ghana, Kenya, Nigeria, Senegal, Sierra Leone, South Africa, Tunisia, Uganda, Zambia, Zimbabwe.
4. Driving AI Education, Training and Research
   - Cameroon, Egypt, Ethiopia, Lesotho, Morocco, Namibia, Rwanda, Senegal, South Africa.
5. Initiating Public Sector Reform with AI
   - Cameroon, Kenya, Rwanda, South Africa, Tanzania, Tunisia, Uganda.
6. Building Strategic Partnerships
   - Côte d'Ivoire, Egypt, Ethiopia, Ghana, Kenya, Malawi, Mali, Namibia, Nigeria, Rwanda, Senegal, Tunisia, Uganda, Zimbabwe.

Source: https://openair.africa/7-ways-that-african-states-are-legitimizing-artificial-intelligence/

eWORLDWIDE GROUP

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

Considerations

- How will you educate your legislators so they make wise choices?
- How will you regulate systems that “learn” and evolve over time?
- How much will you allow human decision making to be removed from the process?
- How will data be used, validated, stored and shared?
- How will you avoid accidental incentives?
- **How will you hold AI systems accountable?**

eWORLDWIDE GROUP

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

Recommendations

- Understand the implications of AI; its rewards **and risks**.
- Don’t repeat the mistakes of the past; learn from them.
- Develop data and privacy policies that favor the individual, not Big Tech.
- Always be mindful of communication and engagement.

And above all:

- Focus on narrow, well defined problems that AI can actually solve

eWORLDWIDE GROUP

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

“Intelligent systems at scale need regulation because they are an unprecedented force multiplier for the promotion of the interests of an individual or a group.”

From “AI Algorithms Need FDA-Style Drug Trials”, Groth, Nitzberg and Russell, Wired Magazine, August 2019

Source: https://www.wired.com/story/ai-algorithms-need-drug-trials/

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.

There is urgent need for us to Unite and Collaborate for Human Resilience

Thank You

Prof. Salma Abbasi
Salma@e-wwg.com

eWORLDWIDE GROUP

Private and Confidential. Copyright © 2021 eWWG. All rights reserved.