BEST PRACTICES AND POLICIES FOR AN EVER MORE AI DEPENDENT WORLD

May 2018

Suellen Aguiar
Hannah Eibensteiner
Serene Shi-Ling Ho
Sho Ito
Madi Jacox
David Korenke
Maritza Navarrete
Hirofumi Sugano

Adam Quinton, Faculty Advisor

TABLE OF CONTENTS

ACKNOWLEDGMENTS

This report was produced for IBM by a Capstone Workshop Consultancy team at Columbia University's School of International and Public Affairs (SIPA) under the supervision of faculty advisor, Adam Quinton. Any views expressed in this report are the authors' own and do not represent those of SIPA, any affiliated organizations, or individuals consulted in the compilation of this report. We would like to thank the following experts for their valuable insights and contribution to this report:

Yushi Hagihara, Acquisition, Technology and Logistics Agency, Japan
Ronaldo Lemos, Columbia University
Reiko Mizutani, Ministry of Health, Labour, and Welfare, Japan
Cathy O'Neil, Author and Activist
Henning Schulzrinne, Columbia University
Yusuke Tanaka, Ministry of Economy, Trade, and Industry, Japan
Nicholas Tatonetti, Columbia University
David Topol, Scripps

Finally, we sincerely thank Adam Quinton and Jill Stockwell for their continuous support throughout this project.

Executive Summary

Artificial intelligence (AI) is revolutionizing the world we live in. Businesses and governments across the globe have harnessed its component technologies to cure and diagnose disease, analyze and trade financial products, and streamline business processes and boost productivity, among other things. However, while AI holds great promise, it also brings real risks. Many individuals have highlighted the potential for intelligent agents to ingrain existing biases, undercut privacy and anonymity, and even jeopardize public safety. This report uncovers and evaluates these concerns in light of five key applications of artificial intelligence. It then provides a series of recommendations to IBM and policymakers on how to counteract and mitigate these risks to increase public trust and acceptance of AI.

Key Findings and Recommendations

1. Address Perception Gap

Public perception often diverges from expert observations on the real risks and benefits of AI. Media publications further distort the narrative by exaggerating incidents and spreading fear about job losses, security threats, and ethical issues. This conflicting narrative makes it much harder for policymakers to align on issue priorities.

Recommendation

IBM and industry should partner with educational and research institutes to better communicate application-specific truths to the public and policymakers. They should also proactively engage the media in these narratives to ensure they reach the widest possible audience.

2. Proactively Shape Public Opinion

Negative public opinion has inhibited widespread adoption of many AI applications.

Recommendation

IBM and industry should work in closer collaboration with policymakers to design appropriate regulatory frameworks. Compliance with regulation and adherence to recommended best practices can significantly enhance the credibility of AI applications. IBM and industry should not view regulatory frameworks as an obstacle but as an opportunity to boost their legitimacy to the public.

3. Develop Robust and Thoughtful Regulation

Many individuals and organizations have called for a preemptive ban on AI applications with full autonomy, such as cars and weapon systems with no human-on-the-loop.

Recommendation

Policymakers should be careful not to design regulation that could stifle technological innovation or undercut an AI application’s efficacy.

4. Homogenize Language

Heterogeneity in language and terminologies across AI applications has inhibited greater regulatory reform.

Recommendation

Policymakers should work with industry to standardize key definitions and terms in order to build a strong foundation for regulation. A more precisely defined terminology and common understanding will also facilitate greater conversation and debate between policymakers and industry.

5. **Develop Clear Success Metrics**

   AI applications lack clear objectives and success metrics. For example, the goal of autonomous vehicles has pivoted from improving energy consumption to reducing car accident rates to replacing drivers.

   Recommendation

   IBM and industry need to better define and communicate the objectives and success metrics of AI applications, as well as their technological limitations.

6. **Prevent Bias**

   Datasets that feed into algorithmic systems may have inbuilt biases that could result in prejudiced AI decision-making.

   Recommendation

   IBM and industry should draw on the knowledge and insights of a diverse set of individuals when designing algorithms to avoid ingraining existing biases and traditional power structures. They should also scrutinize the usage and effects of such algorithms on marginalized and vulnerable communities.

7. **Ensure Appropriate Transparency**

   Transparency in algorithmic decision-making will strengthen public trust and adoption of AI but the required level varies according to application. Although some algorithms should be subject to greater oversight, like those used in consumer-facing applications, others require a level of opacity.

   Recommendation

   Policymakers must have a thorough understanding of the processes under which the product or service operates in order to design effective and meaningful regulation.[1] Policies mandating transparency in algorithmic decision-making must consider the specific application and intended purpose.

8. **Improve Cybersecurity**

   Firms and technologies across all applications face growing cybersecurity challenges such as ransomware threats and data breaches.

   Recommendation

   IBM and industry should conduct regular internal security audits based on data security standards and best practices.

Introduction

Defining AI

The growth of AI has outpaced the public's understanding of it; industry and policymakers often have wildly different definitions of intelligent agents. In this report, we define AI as the ability of an agent to simulate human thought processes to fulfill a pre-determined objective. We further divide AI into two categories: weak and strong. Weak or "narrow" AI describes the ability of an agent to perform a single, limited task whereas strong or "general" AI describes the ability of an agent to think and function exactly like a human. Today, AI technology exists in the form of augmented assistance to human tasks; it is limited to its weak form. Experts disagree about when and whether general AI will emerge. We focus on narrow AI because it has concrete near-term business impact.

Objectives

This report examines the current state of AI across key markets with a view to providing actionable recommendations to IBM and policymakers on how to maximize awareness and acceptance of AI. Specifically, it aims to:

- Understand the language policymakers, industry experts, and the public use to discuss a range of applications;
- Explain where risks are exaggerated, underappreciated, or mischaracterized;
- Examine past adverse outcomes in algorithmic decision-making and extract valuable insights;
- Grasp the momentum and direction of regulatory attention across the European Union (EU), the United States (US), Japan, and China.

Scope

This report examines five key applications of AI: autonomous vehicles (AV), autonomous weapon systems (AWS), consumer insights, financial risk pricing, and healthcare diagnostics across four key markets: the EU, US, Japan, and China.

Methodology

The preliminary work included ranking more than 20 applications of AI across five criteria: automation potential, market potential, political attention, public interest, and social risk to select our top five applications of focus.

Automation potential uses the projected degree of automation per industry from McKinsey's 2018 "A Future that Works" report.[2]

- 3 (High): Ability to Automate $\geq$ 50%
- 2 (Medium): 40 $\leq$ Ability to Automate < 50%
- 1 (Low): Ability to Automate < 40 %

Market potential uses projected AI revenue per industry for 2016-2025 from Tractica Business Intelligence[3] and projected AI revenue per use case/segment for 2016-2025 from Statista Business Intelligence.[4]

- 3 (High): Market size 2025 ≥ 10 billion
- 2 (Medium): 3 billion ≤ Market size 2025 < 10 billion
- 1 (Low): Market size < 3 billion

Political attention examines the amount of public discussion, regulation, and legislation within governing bodies through secondary research.

- 3 (High): Significant attention
- 2 (Medium): Moderate attention
- 1 (Low): Minimal or no attention

Public interest uses the number of comments, reactions, and shares from Facebook's total engagement tool (see Appendix 1 for details).

- 3 (High): 50,000+ engagement metrics
- 2 (Medium): 10,000 – 49,999 engagement metrics
- 1 (Low): 0 – 9,999 engagement metrics

Social risk examines the potential for AI to promote bias, erode civil liberties, and undermine public safety. It multiplies the number of risk factors by the level of AI intelligence adapted from PWC's "Sizing the Prize" report. Levels include assisted intelligence - low (1), augmented intelligence - medium (2), and autonomous intelligence - high (3).[5]

- 3 (High): 4+ risk factor level
- 2 (Medium): 3-4 risk factor level
- 1 (Low): 1-2 risk factor level

Exhibit 1. Selected Applications

	Automation Potential	Market Potential	Political Attention	Public Interest	Social Risk	Total
Autonomous Vehicles	3	2	3	3	2	13
Healthcare Diagnosis	1	2	3	2	2	10
Autonomous Weapon Systems	0	2	2	3	3	10
Financial Risk Pricing	2	2	2	2	2	10
Consumer Insights	3	3	0	1	2	9

Source: SIPA IBM Capstone Group

Sources

This report draws on a wide range of primary and secondary resources. These include interviews with industry experts, academics, and members of the NGO and think-tank communities; official government and military reports; legal and regulatory documents; and industry and academic articles, reports, and surveys.

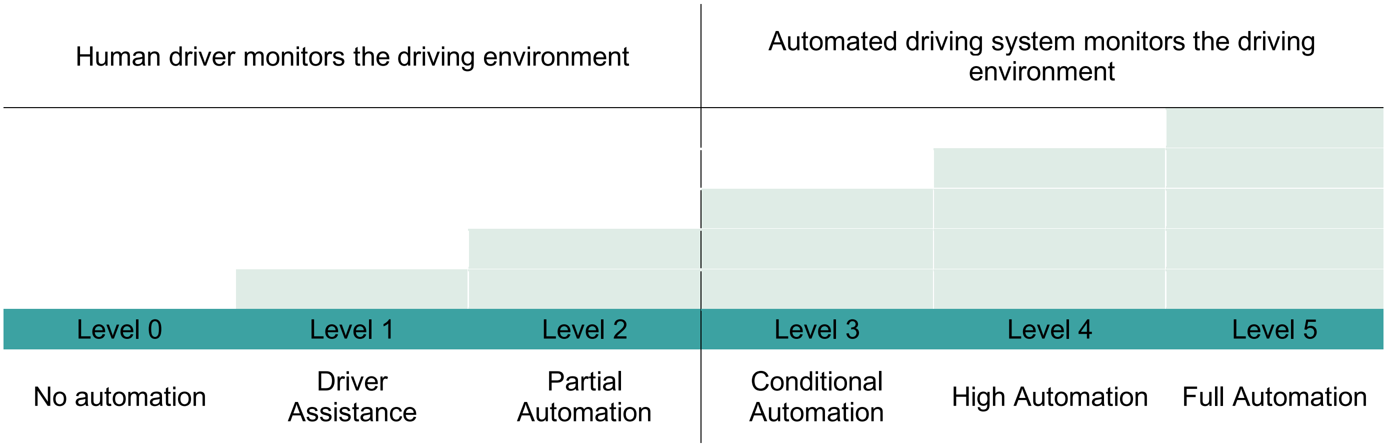
Glossary

Term	Description
Algorithm	A series of rules that systems use to solve problems
Agents	An autonomous entity that takes actions based on its environment
Artificial Intelligence	The ability of an agent to simulate human thought-processes
Artificial General Intelligence	The ability of an agent to think and function like a human
Artificial Narrow Intelligence	The ability of an agent to perform a single, narrow task like a human
Artificial Neural Network	A computing system that mimics the neural network configuration of the human brain, which learns and adapts through trial and error
Big Data	Large and complex datasets
Bot	A software that runs simple, automated tasks
Black box	A system whose internal workings are not well understood or known
Data Mining	The process of parsing data to identify patterns and extract information
Decision Model	The use of predictive analytics to establish the best course of action for a given situation
Deep Learning	A subfield of machine learning wherein intelligent agents learn and make decisions through artificial neural networks
Machine Learning	A subset of AI wherein intelligent agents learn through pattern matching rather than explicit pre-programming
Internet of Things	Physical objects connected to the internet that gather and share electronic information
Predictive Analytics	The act of looking at data to find patterns to predict future events
Reinforcement Learning	A form of machine learning wherein intelligent agents learn through experimentation and positive or negative reinforcement
Robot	A machine that carries out autonomous or semi-autonomous tasks
Supervised Learning	A form of machine learning where there are outputs for every input and intelligent agents learn through matching inputs to outputs
Technical automation	A process performed without human direction or assistance

Autonomous Vehicles

The US Department of Transportation's National Highway Traffic Safety Administration (NHTSA) defines AVs as vehicles "in which at least some aspects of a safety-critical control function (i.e. steering, acceleration, or braking) occur without direct driver input."[6] This includes levels of automation that require the human operator to monitor the environment and levels of automation where the automated driving system monitors the environment, as shown in Exhibit 2. AV development and funding have accelerated in recent years but it is still not clear when self-driving cars will enter the marketplace. Engineers are addressing technical challenges but regulation and public skepticism remain significant barriers to widespread adoption.

Exhibit 2. Levels of Autonomy in Autonomous Vehicles



Source: Adapted from "Autonomous Vehicles: Plotting a Route to the Driveless Future," Accenture, https://www.accenture.com/t20170720T104429Z__w__/us-en/_acnmedia/PDF-55/Accenture-Insight-Mobility-IoT-Autonomous-Vehicles.pdf

Current Challenges and Future Solutions

Strengthening Public Perception of AV

Phasing in semi-autonomous components of driving and conducting test cases, such as parking assistance and adaptive cruise control, could improve public perception. This phase-in would allow consumers and drivers to learn and adapt to the technology at their own pace, leading to a more gradual but rooted confidence in AV. Regulation and greater oversight could also shore up public confidence in self-driving cars. Meanwhile, overselling or exaggerating the capabilities of AV will likely backfire and risk alienating the people with the greatest buy-in for the technology.

Ensuring Cybersecurity for Self-Driving Cars

The threat of cyberattacks and remote hacking is an increasing concern for policymakers and consumers. In addition to closer collaboration with industry experts and relevant government agencies such as the NHTSA, AV manufacturers should reach out to cybersecurity agencies and experts. For instance, the National Institute of Standards and Technology (NIST) is developing a cybersecurity framework for critical infrastructure in the US Their recommendations can help the automotive industry develop best practices for connected vehicle technologies as they leverage cybersecurity expertise across industries with equal if not greater risk of cyberattacks, such as energy, infrastructure, and information technology (IT).[7]

Making Self-Driving Cars Safer

The lack of clear-cut standards on how to best test and measure AV safety has negative impacted public trust and acceptance of self-driving cars. Legislators must decide whether AVs should be allowed on the road, even when there are potential bugs in the software. Policymakers should engage industry stakeholders when designing testing and performance metrics. They should also work with automakers to collect performance measures such as near accidents. This data can serve as an indicator of dangerous behavior and result in some sort of penalty. Automotive companies would also be wise to voluntarily self-assess their technology and make data available for regulators to further strengthen public perception.

Building Transparency into Systems

Architectural and design decisions must have sufficient transparency to enable users to understand how AVs will react in different circumstances, as well as to make independent evaluations possible.[8] However, transparency should also respect corporate secrets, copyright, and security concerns. The appropriate federal regulator of transportation in each country should encourage the automotive industry to better explain AI decision-making models to their consumers.

Discussion of Risks and Benefits

Although experts agree that self-driving cars will enter the marketplace in the future, they disagree about the ethical risks and challenges posed by their entrance.

Decreasing Traffic Fatalities with Self-Driving Cars

Automobile manufacturers, academics, think-tanks, and governments across the world cite improved safety as the key benefit of self-driving cars. Companies like Toyota, Baidu, Audi, and Tesla from Japan, China, Germany, and the US respectively, all share the goal of developing a technology that increases vehicular safety. According to Gill Pratt, Head of the Toyota Research Institute, the company’s goal is to “create a car that will never be responsible for a crash, regardless of what the driver does.”[9] Tesla CEO Elon Musk is also a self-driving vehicle proponent, believing that AV can reduce – and potentially eliminate – the high percentage of traffic fatalities caused by human error.[10]

Filling the Gap: AV and Mobility

Self-driving cars offer innovative solutions to socioeconomic problems such as poor integration of public transportation modes, lack of decent public transit options for aging and disabled populations, and first and last mile connections. According to researchers from the Boston Consulting Group (BCG), automated shuttle buses could complement existing public transport by taking people from low populated or low-density areas to the nearest rail or subway station.[11] AVs could also provide better late-night services and bridge the first and last mile connections to and from major rail lines. Accenture envisions the redesign of first and last mile transit with an emphasis on logistical convenience for the end consumer. In their report, the firm sketches a future where AVs can pick up customers at homes and businesses using their smartphone locations.[12]

AVs Driving on the Wrong Road to Safety

While safety is critical for self-driving cars, the AV industry lacks clear-cut standards on how to best test and measure vehicular safety. According to academic Tobias Holstein, Gordana Dodig-Crnkovic, and Patrizio Pelliccione, ethical debates could emerge in situations where there is a tradeoff between safety and economic benefit, such as when a car manufacturer chooses a cheaper sensor over a more expensive one -- even though this could increase the chance of errors or accidents.[13] Although current regulation does not address the issue, many experts seem to prefer the "proven in use" argument, which assesses quality and compliance to legislative norms through AV testing, rather than mandating quality thresholds for hardware and software systems.

Enhancing Cybersecurity Is Critical for a Driverless Future

Attacks on sensors and car systems pose a challenge to widespread AV adoption. According to Elon Musk, cyberattacks are a top security challenge for self-driving cars and will be an even bigger one in the future.[14] Although a number of regulatory entities within the US, UK, and EU have published best practices for preventing cyberattacks, Holstein argues that software engineering questions need to be better addressed. For example, should a self-driving car be allowed on the road if the software is not up-to-date? And who would be liable if an incident happens because the software was not updated or contained bugs? Holstein, Dodig-Crnkovic, and Pelliccione also believe better technical solutions can guarantee security and anticipate – and even prevent – worst case scenarios in security breaches.[15]

Exaggerated Risks, Mischaracterizations, and Concern Among the Public

Ethical Considerations of Self-Driving Cars Undercutting Trust

Given the compressed timescale of AV development, the general public has not had enough time to adapt to interacting and engaging with the technology. The idea of ceding driving agency to an autonomous device makes many people in the US nervous, according to a study by the American Automobile Association.[16] Although the public generally believes that AVs should operate under utilitarian principles – sacrificing one passenger to save the many – lots of people are uncomfortable with this idea in practice.[17] The 2004 science fiction film *I, Robot* explored this concept and it remains a key obstacle for public acceptance of self-driving cars. Moreover, the general opacity surrounding AV decision-making algorithms further undercuts public trust.[18]

Yet some experts see the debate around ethical dilemmas as an "abstract thought experiment" when focus should be on the "concrete conditions that influence the behavior of self-driving cars, [such as the] interdependencies between components, systems and stakeholders."[19] Dr. Rodney Brooks, an MIT robotics professor, argues these theoretical scenarios – sacrificing one person to save the other – do not accurately reflect real life problems.[20] He believes that the issue is "non-existent and irrelevant" and "will have no practical impact [...] nor lead to any practical regulations."[21] Despite the reassurances by Dr. Brooks and many researchers in his field, at least 78% of Americans fear riding in a self-driving car with only 19% indicating they would trust the car, suggesting that psychological factors are a greater barrier to widespread AV adoption than technical challenges.[22]

Managing Public Concern of Cyber Attacks on AVs

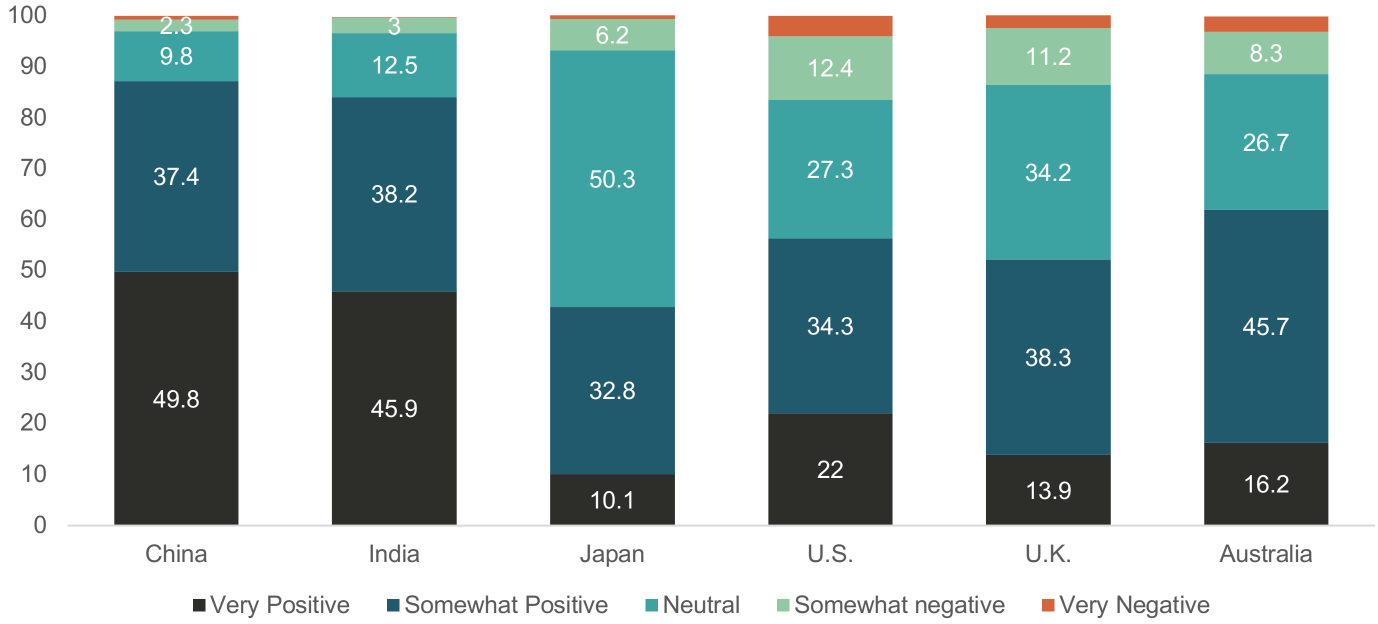
The public is also concerned about cyberattacks on self-driving cars. This concern increased in 2014 when two researchers took remote control of a Jeep Cherokee and cut its transmission on the highway as part of a research initiative.[23] Many in the public sphere believe that the industry has not taken such threats seriously and are failing to implement preventative measures.[24] Hacking and manipulation pose a greater risk for self-driving cars than those with lower levels of connectivity. However, such fears are somewhat exaggerated. More than half of non-autonomous vehicles sold in the SS. already have internet connectivity and are at risk.[25]

Major industry players are addressing the threat of cyberattacks through a combination of defensive software solutions and best practices for automotive cybersecurity.[26] According to a report by the Economist, several engineers in the field believe that a multiple sensor and control system is more than sufficient to protect the vehicle from cyberattacks.[27] One researcher argued that it is "easier to use an ordinary vehicle to kill people than to take control of a driverless car."[28] However, industry efforts in this arena have failed to bridge the trust gap between the public and self-driving cars.

Chinese Public Optimistic of AVs, Trusting Tech Companies to Make Them a Reality

A survey conducted in 2014 by researchers at the University of Michigan found that 49.8% of Chinese held positive attitudes towards self-driving cars, followed by 22% in the US, 13.9% in the UK, and 10.9% in Japan.[29]

Exhibit 3. Public Opinion Towards Self-Driving Cars by Country

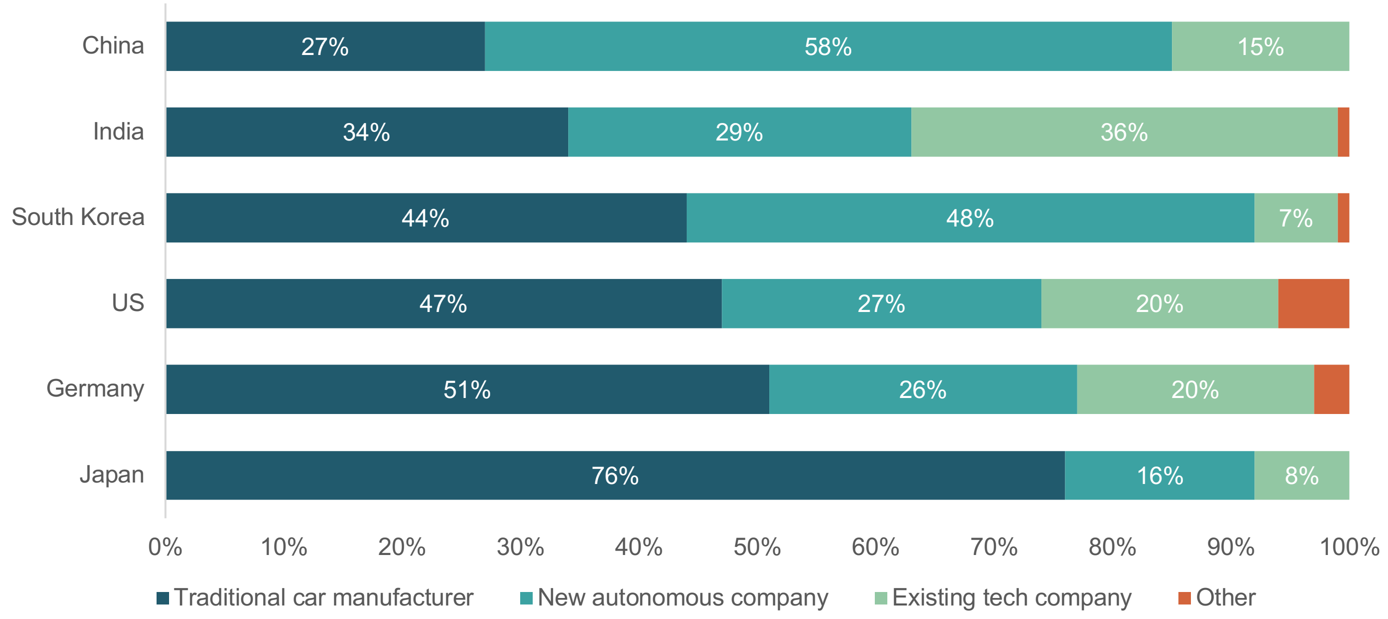


Source: Adapted from Brandon Schoettle and Michael Sivak, "Public Opinion about Self-Driving Vehicles in China, India, Japan, the US, the UK, and Australia," October 2014, https://deepblue.lib.umich.edu/bitstream/handle/2027.42/109433/103139.pdf

Respondents in China and the UK cited "safety concerns resulting from equipment failure" as a chief area of worry.[30] Meanwhile, Japanese and American interviewees expressed concern about "self-driving vehicles being confused in unexpected situations."[31] Generally speaking, Chinese drivers felt positive about the future of AVs while their Japanese counterparts held the most neutral attitudes towards the technology. According to the Automobile Division at the Japanese Ministry of Economy, Trade and Industry (METI), AVs are expected to first roll out in underpopulated areas that lack sufficient public transportation.[32] Perhaps the dearth of self-driving cars could explain the general apathy among the Japanese public towards them. Moreover, Japanese society is more risk averse and the government has sought to engage the public in discourse around AV safety.[33]

More specifically, public trust in self-driving cars is tied to the companies that are bringing these autonomous technologies to market. For instance, Deloitte's Global Automotive Consumer Study found that 76% of Japanese respondents trust traditional car manufacturers the most to bring fully autonomous vehicles to market. 51% of German consumers also place their trust in automotive companies.[34] On the other hand, China trusts new technology companies more than traditional car manufacturers. Although public trust is key to the acceptance and subsequent success of AVs, the way in which that trust is attained – through technology or brand reputation – is crucial.

Exhibit 4. Level of Public Trust per AV Manufacturer by Country



Source: Adapted from "What's Ahead for Fully Autonomous Driving, Consumer Opinions on Advanced Vehicle Technology", Deloitte Development LLC, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manufacturing-consumer-opinions-on-advanced-vehicle-technology.pdf

Adverse Outcomes and Lessons Learned

The aforementioned concerns, characterizations, and risks associated with AVs may seem fictitious and exaggerated to industry experts. However, the many accidents involving self-driving cars have amplified these concerns and fears. As a result, AV manufacturers have instituted steps to mitigate the potential for these incidents to reoccur.

Hackers Force Jeep to Stop on Highway

A recent hacking incident stoked fears in the AV community about cyberattacks. In 2015, former National Security Agency (NSA) hacker Charlie Miller and IOActive researcher Chris Valasek took remote control of a Jeep Cherokee and disabled it on the middle of a highway. The hackers rewrote the vehicle's entertainment system code to issue a new set of commands to the internal steering, brakes, and engine network. Fiat-Chrysler Automobiles (FCA), the company that manufactures the Cherokee, recalled 1.4 million vehicles and issued a patch in an attempt to prevent future breaches. In response, Miller and Valasek hacked the new software and released a document with their original research detailing the diagnostic packets and service IDs other actors can use.[35] Their effort sought to raise awareness about the vulnerability of devices that "connect to the outside world."[36]

To help the AV industry address the growing risk of cybersecurity threats, the Automotive Information Sharing and Analysis Center (Auto-ISAC) released a set of vehicular cybersecurity best practices in 2016. The best practices include guidelines for assessing the organizational and technological robustness of automotive cybersecurity by providing additional guidance on how to design, assess, detect, and report incidents in order to facilitate collaboration, governance, and training.[37] Similarly, in 2016, the NHTSA released suggested guidelines for the automotive industry to improve vehicular security. Although this guidance is not yet law, it shows the industry is heading towards a more unified approach on cybersecurity. A number of organizations including automakers, nonprofits, university programs, and security technologists are working to develop vehicle-specific security technology.[38]

Sharing the Road: Partly Autonomous Driving and Fatalities

Accidents involving self-driving cars garner significant media attention and distort public perceptions about their frequency. These accidents inflame discussions about the risks versus the benefits of AV technology. The first self-driving car fatality occurred in 2015 when a Tesla Model S collided with a truck while in autopilot mode.[39] Although a subsequent investigation put the blame on the driver of the Tesla, the incident highlights the challenges inherent in human-machine collaboration. Police investigators concluded that it was the driver's overconfidence in the 'autonomous' aspect of the vehicle that lured him into a false sense of security when he should have been paying attention to the road. The driver's family subsequently filed a lawsuit against the vehicle manufacturer claiming they oversold its autonomous capabilities.[40] Although such accidents are not a result of AI decision-making, they show that manufacturers must clearly advertise what the system can and cannot do. The highest level of autonomy available today is level three where the vehicle can only take full responsibility for certain aspects of driving at specific parts of a journey. AV operators should clearly delineate the distinction between a level three vehicle and a fully autonomous level five vehicle.

Regardless of autonomy level, self-driving cars still have to interact with fallible human drivers and pedestrians. Despite logging over two million miles in the US and having the lowest at-fault rate of accidents, AV manufacturer Waymo found human drivers continue to hit their vehicles. The prevailing theory is that self-driving cars, like Waymo, adhere to the letter of the law, which human drivers do not anticipate, leading to a high number of non-fatal collisions where the human is at fault.[41] Thus algorithms must not only understand and adhere to traffic law and the safety of their passengers but also understand and anticipate human behavior.

Current and Pending Regulations

The lack of universal rules and regulations for AVs presents security and liability questions. According to legal experts, current regulatory instruments for human-controlled vehicles are not adequate for self-driving cars.[42] To be commercially available, the AV sector in each country must address cybersecurity and liability concerns and adapt their current regulatory framework to the rapid advance of self-driving cars.

Most criminal liability regimes assume that the person in the driver's seat is in control of the vehicle – yet this does not apply to AVs. Although no liability regulation for self-driving cars currently exists, academics and experts tend to put accountability on car manufacturers. Attributing responsibility to them may seem natural as they already adhere to safety standards for human-controlled vehicles. However, the production of AVs involves a complex supply chain of operating system providers, sensor producers, and software developers. Mark Schaub and Atticus Zhao at KWM Corporate & Securities Group argue that the "party liable for accidents and incidents involving AV will then face a considerable burden to ensure that all suppliers meet safety standards and best practices for cybersecurity."[43] They explain that this scenario gets considerably more "challenging in the context of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) interaction – environments where AVs are potentially more vulnerable to cyberattacks."[44] A further complexity on the cybersecurity front is that software updates are required to deal with any security vulnerabilities. Policymakers must grapple with questions like whether car manufacturers should be responsible for software updates after their vehicles are sold to consumers or whether AVs should be allowed to circulate if there are bugs in the software.[45]

United States

It is difficult to govern the AV sector in the US because State and Federal governments handle different levels of regulation. Additionally, as Darrell West at the Brookings Institution points out, this regulatory fragmentation complicates innovation since manufacturers want to build cars and trucks for national and international markets.[46] Each state in the US determines its own rules on how to allocate liability among owners, operators, passengers, manufacturers, and others when a crash occurs.[47]

Although there are no national laws in place on AVs in the US, the Federal government and Congress have sought to regulate self-driving cars. The NHTSA recently released the 2.0 version of its voluntary guidance for automated driving systems to industry and States and is preparing the 3.0 version for 2018.[48] The Guidance encourages best practices and prioritizes safety. For example, it recommends actions for assessing risk and testing vehicles for cybersecurity vulnerabilities. It also clarifies Federal and State roles going forward and provides technical assistance to states.[49]

AV manufacturers gained regulatory approval in several states to run predetermined routes. According to the National Conference of State Legislatures (NCSL), a bipartisan non-governmental organization, at least 41 states and Washington D.C have considered legislation related to self-driving cars since 2012, of which 22 states passed legislation and 10 issued executive orders related to AVs.[50]

European Union

The EU lacks regulatory clarity on topics such as liability, cybersecurity, and ethics of AVs.[51] Given this status, individual member states, like Germany, have created their own individual regulations.

In late 2017, the German Ethics Commission at the Federal Ministry of Transport and Digital Infrastructure issued guidelines for the programming of automated driving systems. According to the former Minister, Alexander Dobrindt, the Commission "performed absolutely pioneering work in this field and developed the first guidelines in the world for automated driving."[52] The report comprises 20 propositions, including recommendations on data sovereignty, liability, and transparency.[53]

Moritz Pustow, Partner at KPMG in Germany, believes the legislation "could discourage AV use since the driver might be liable for damages even if the vehicle caused the accident."[54] Spain and France have also addressed regulatory implications of AVs. According to a KPMG report, Spain receives strong scores for its AV-specific regulation and government work, having allowed testing on public roads since 2015.[55]

China

China recently completed the first draft of its nationwide regulation allowing AV tests on public roads. This news came on the heels of China's first provisional regulation for testing self-driving cars on city roads.

A review of the Regulation by Schaub and Zhao shows it follows some of the best practices adopted by Australia, Germany and the US[56] It states that testing must ensure a human on-the-loop security alternative so drivers can take control of the vehicle if it malfunctions or issues a warning.[57] The Regulation also state that test drivers and ultimately the car manufacturer are liable in case of incidents, accidents, or any violation of traffic laws. Experts in China believe that AV testing in cities like Shanghai, Hangzhou, and Wuhan will follow Beijing's lead.[58] These regulatory changes are part of a broader push for China to become the leader in AV technology.[59]

Japan

Japan has actively set guidelines on self-driving cars in the past few years. In 2016, Japanese and European leaders partnered to write common AV standards to accelerate industry development. One year later, the National Police Agency in Japan issued a set of rules for testing self-driving cars on nation roads after receiving feedback from the public and industry experts. The legislation determined, among other things, that tests will not be permitted on roads that are crowded.[60] The Japanese Government is currently drafting rules specific to cars with level three automation or higher.[61]

Autonomous Weapon Systems

AWS are a growing presence on the battlefield and in the skies. More and more countries are developing and fielding autonomous technologies in combat and for defense. Prominent examples in operation include air defense systems such as missile defense, anti-aircraft, and close-in weapon systems; robotic sentry weapons – the so-called "killer robots"; and loitering weapons.[62]

The Department of Defense (DoD) defines AWS as a weapon system that "once activated can select and engage targets without further intervention by a human operator."[63] This includes human-on-the-loop or human supervised autonomous systems wherein machines select and engage targets yet humans can intervene and stop engagements, as well as human-out-of-the-loop or fully autonomous systems wherein machines select and engage targets without human supervision or intervention.[64] With the exception of some loitering weapons, operational AWS are semi-autonomous or autonomous. Yet some countries have developed, or are developing, weapons with full autonomy.[65]

Exhibit 5. Overview of Autonomous Weapon Systems

Type of Weapon	Examples	Notable Users	Autonomous Modes
Air Defense Systems	Phalanx (US), Iron Dome (Israel)	China, Germany, Japan US, UK	Human-in-the-loop, human-on-the-loop
Active Protection Systems	Arena (Russia), Trophy (Israel)	China, Germany, Israel, Russia, South Korea	Human-on-the-loop
Robotic Sentries	DODAAM Super aEgis II (South Korea), Samsung SGR-AI (South Korea), Raphael's Sentry Tech (Israel)	Israel, South Korea	Human-in-the-loop, human-on-the-loop*
Loitering Weapons	Switchblade (US), Harpy (Israel)	China, Germany, US, UK	Human-in-the-loop, Human-on-the-loop, Human-out-of-the-loop**

Source: Adapted from "Mapping the Development of Autonomy in Weapon Systems", Stockholm International Peace Research Institute, November 2017, https://www.sipri.org/publications/2017/other-publications/mapping-development-autonomy-weapon-systems.
** The DODAAM has a human-out-of-the-loop setting.*
*** The Orbiter 1K "Kingfisher", the Harpy, The Harop and The Harpy NG are fully autonomous systems.*

Current Challenges and Future Solutions

Enhancing Security and Reliability with Human Oversight

AWS bring additional risks over semi-autonomous or non-autonomous weapons. They can be hacked or manipulated, malfunction or perform unexpectedly. Moreover, they lack the situational awareness and agency to exercise appropriate discrimination and proportionality on the battlefield. For the foreseeable future, human operators should exercise "meaningful control" over these weapon systems. This encompasses more than just the human as the "fail-safe"; operators should receive significant training on how to use systems while the latter must undergo rigorous and continuous testing and evaluation. Keeping a human on-the-loop cannot prevent weapon failures -- but it can significantly mitigate them.

Strengthening Public Perception Through Dialogue and Understanding

The public holds extremely negative attitudes towards AWS. Majorities across countries support a ban on lethal autonomous weapon systems (LAWS). Yet banning LAWS would not stop many actors from producing them. Moreover, a ban could stifle technological innovation and restrict a technology that might save more lives. The UN and other multilateral forums however, can provide a forum to raise awareness about AWS, develop norms and codes – if not binding resolutions – around their use and discuss new issues raised by their entrance. They can also correct some of the exaggerations, mischaracterizations, and downright confusion on AWS, particularly around terminology.

Discussion of Risks and Benefits

AWS have provoked widespread debate among AI experts, members of the military, and academia. Proponents tout their operational and economic advantages while critics highlight the ethical, legal, and moral challenges they present.

AWS Provide Militaries Greater Speed and Reach

A key advantage of autonomy is speed. AWS can process more information from more sources quicker than humans possibly can and significantly reduce the kill chain sequence. According to former DoD official and academic Paul Scharre, these weapons are advantageous in communication-degraded or denied environments or when the speed of incoming attacks might overwhelm human operators.[66] A second operational advantage of autonomy is reach. AWS can operate in high threat environments where human soldiers cannot and reach otherwise inaccessible areas like underwater or space. Academics Vincent Boulanin and Maaike Verbruggen note their suitability for "dull, dirty, or dangerous missions" (3D tasks) such as air defense, extended surveillance missions, or actions in enemy territory.[67]

…. While Saving Money and Resources

Autonomous systems act as force multipliers: fewer weapons are needed per mission and their efficiency is superior to human soldiers. Moreover, AWS do not need to be in constant contact with command and control centers (C&C), which reduces the overall number of human operators and analysts that oversee a system. An Air Force Study found that having one operator supervise several unmanned aerial vehicles (UAVs) could bring a 50% or greater reduction in personnel.[68] Autonomous systems could help the military contend with historically low personnel levels and shrinking enrollment.

Machines Possibly More Humane Than Human Soldiers

AWS are not subject to human emotions like fear, anger, or frustration that cloud judgment and distort decision-making. Moreover, autonomous systems are not susceptible to scenario fulfillment wherein humans absorb information that conforms to pre-existing biases.[69] Roboticist Ronald Arkin believes AWS can possibly reduce military and civilian casualties given their immunity to such human fallibilities. If a military robot can exceed human performance one day, then nations should develop and field AWS according to Arkin. He likens this to the moral imperative of using precision-guided missiles in urban settings that reduce collateral damage versus more indiscriminate attacks that wreck widespread destruction.[70]

> *"If a warfighting robot can eventually exceed human performance with respect to international humanitarian law adherence, that then equates to a saving of noncombatant lives, and thus is a humanitarian effort. Indeed, if this is achievable, there may even exist a moral imperative for its use."*
> *- Robotist Ronald Arkin[71]*

System Complexity Brings Increased Security Risk

Like all complex systems, AWS are vulnerable to hacking, manipulation, system errors, or unexpected interactions with the environment. Paul Scharre argues that the increased complexity of autonomous systems makes it harder for humans to understand and predict where and when failures might occur.[72] Moreover, machines might start to exhibit emergent behaviors – actions outside of their programming. Scharre notes that better system design, testing, evaluation, and user training can mitigate some of these risks but not completely eliminate them.[73]

Technological Limitations Inhibit Widespread AWS Deployment

Despite great strides in machine learning and robotics, AWS do not yet have human levels of cognition and situational awareness. They are still relatively inflexible and unable to adapt to novel situations or complex environments. According to Boulanin and Verbruggen, autonomous systems can only operate safely and reliably in "complex, uncertain, or adversarial" environments with human supervision.[74]

…. And Pose Ethical and Moral Challenges

Computer scientist Noel Sharkey argues AWS violate international humanitarian law (IHL) since they lack the situational awareness to distinguish between combatants and non-combatants and make calculations about acceptable force. He points out that the Israeli Harpy, an anti-radar system, can detect friendly versus unfriendly radar signals but cannot tell if the radar is on an anti-aircraft barrier or the roof of a school.[75] These technological limitations increase the risk of mass-casualties or fratricide.

> *"Decisions about what constitutes a level of force proportionate to the threat posed by enemy forces are extremely complex and context dependent and it is seemingly unlikely that machines will be able to make these decisions reliably."*
> *- Philosopher Robert Sparrow[76]*

Fully Autonomous Weapons Hotly Debated in Expert Communities

Many experts want to preemptively ban autonomous systems given their inherent risks. In 2015, Elon Musk, Apple co-founder Steve Wozniak, and physicist Stephen Hawking among others, signed a public letter calling for a ban on offensive AWS "beyond meaningful human control."[77] In addition to the aforementioned risks, the authors argued that development of these weapons could spark a global arms race while bad actors might use them for targeted assassinations, ethnic cleansing, and to subdue local populations.[78] Other experts, like Paul Scharre, argue that fully autonomous weapons might be appropriate in limited and controlled contexts. Public safety risk, he concludes, is ultimately dependent on the "action performed" and the "failure to correct action."[79] To illustrate, Scharre contrasts the HARM anti-missile system that can engage targets independently but has strict time and space limitations versus the Harpy which can stay in the air for long periods of time and have a greater line of vision. While human operators can halt subsequent Harpy launches, they cannot recall launched ones that could continue to operate for over two hours.[80] The Harpy thus has a much greater public safety risk than the HARM anti-missile system. To date, no experts have publicly called for the unrestrained use of fully autonomous weapons.

Exaggerated Risks, Mischaracterizations, and Public Concern

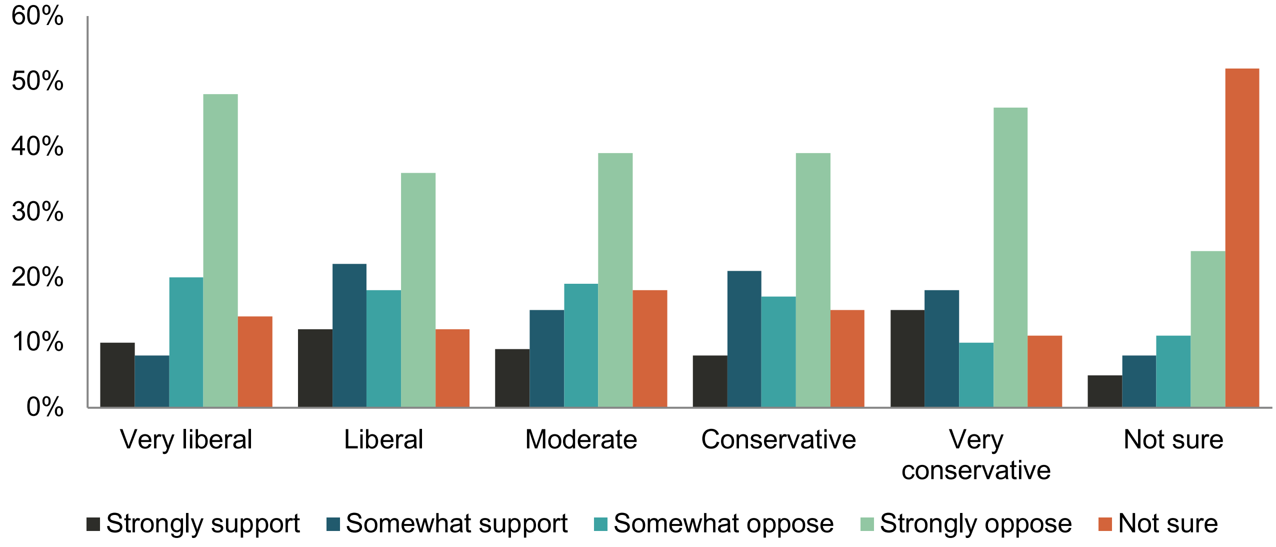
Critics Misunderstand the True Intent of AWS

Many critics believe AWS will supplant human decision-making on the battlefield. Machines, they fear, will one day make combat decisions with little or no input from human operators. Yet many countries including the US, UK, and Japan have endorsed the concept of meaningful human oversight in autonomous and lethal autonomous systems.[81,82,83] American military experts in particular, have highlighted the importance of human-machine collaboration over pure human or pure machine decision-making. Paul Scharre argues that hybrid structures leverage the "predictability and reliability" of automation with the "robustness and flexibility" of human beings and can achieve superior outcomes over demarcated systems.[84] The Pentagon's Third Offset Strategy also emphasizes the concept of "centaur warfighting" or human-machine teaming to augment the capabilities of both entities.[85] Some future weapons – like cyber defense – might be fully automated given aforementioned time and space limitations. Yet the overall intent of AWS is not to replace humans on the battlefield but to enhance their efficacy.

"Slaughterbot" and "Skynet" Scenarios Grip Public Imagination

The public has proven receptive to fearful scenarios from people and organizations that seek to ban LAWS. The Campaign to Stop Killer Robots recently published a video showing terrorists getting ahold of hundreds of military swarming drones and slaughtering innocent school children en masse. While this scenario is possible, it might not be plausible. Paul Scharre notes that the US, China, and other military powers are largely developing AWS to target foreign nation's militaries – not their civilians. Moreover, Scharre continues, it is unlikely terrorist groups could get ahold of, or mass produce, so many weapons and successfully pull off dozens of attacks.[86] However, convincing the public remains a bigger challenge. In 2015, an international survey of 1000 participants from 54 different countries reported that 67% of respondents believed LAWS should be internationally banned, 56% thought they should not be developed or used, and 85% believed they should not be used for offensive purposes.[87]

Exhibit 6. Public Opinion of Autonomous Weapon Systems



Source: Adapted from "Public Opinion on Autonomous Weapon Systems," YouGov America and University of Massachusetts Amherst, 2013, http://www.newswise.com/articles/new-survey-shows-widespread-opposition-to-killer-robots-support-for-new-ban-campaign.

Adverse Outcomes and Lessons Learned

The Patriot Incidents Showcase Human-machine Teaming Challenges

Adverse outcomes in simple autonomous systems can provide lessons for AI-enhanced AWS. During the invasion of Iraq in 2003, the MIM-104 Patriot, a human-on-the-loop missile defense system, shot down a British Tornado and a Navy F-18 fighter, killing three. In the first incident, the Patriot misidentified the Tornado as an anti-radiation system while its Identification Friend or Foe system (IFF) malfunctioned. In the second incident, the Patriot misidentified an incoming ballistic missile.[88]

These incidents showcase two truisms of human-machine interactions: First, operators have a tendency to over-trust intelligent agents.[89] In the first incident, the soldier approved the Patriot's decision without additional review. According to army researchers, he demonstrated "unwarranted and uncritical trust in automation" and ceded "control responsibility" to the machine.[90] Second, operators can misunderstand machine behavior and take incorrect actions due to poor system design or lack of sufficient training.[91] In the second incident, the soldier brought the system online to prepare for an engagement but did not realize it was in auto-fire mode. Following a lengthy investigation, the Army concluded that operators need to have more involvement and control over machine decision-making.[92] They changed operational protocols to give humans more oversight over the kill chain sequence, while updating trainings to include similar incidents and encouraging trainees to question results.[93]

Yet many experts contend that unexpected system failures – as in the Patriot incidents – are bound to occur in "complex, tightly-coupled systems" where errors can "cascade from one subsystem to the next with little slack to absorb and react to failures."[94] According to Paul Scharre, improved training, testing, and design can mitigate errors but not eliminate them.[95]

"Even with our improved knowledge, accidents and thus, potential catastrophes are inevitable in complex, tightly coupled systems with lethal possibilities. We should try harder to reduce failures – and that will help a great deal – but for some systems it will not be enough. These systems are currently too complex and tightly coupled to prevent accidents that have catastrophic potentials. We must live and die with their risks, shut them down, or radically redesign them." – Sociologist Charles Perrow[96]

Current and Pending Regulations

United States

The US is the only country with a comprehensive policy on AWS usage. Its DoD-authored 2012 Directive on Autonomy in Weapon Systems states that:

- Autonomous weapons "shall be designed to allow commanders and operators to exercise appropriate levels of human judgement over the use of force."
- Persons who operate or direct autonomous and semi-autonomous weapon systems must "do so with appropriate care and in accordance with the laws of war…."
- Human supervised AWS can be used to select and engage targets "with the exception of selecting humans as targets."
- Autonomous weapons can only be used to apply "non-lethal, non-kinetic force, such as some forms of electronic attack against material targets." [97]

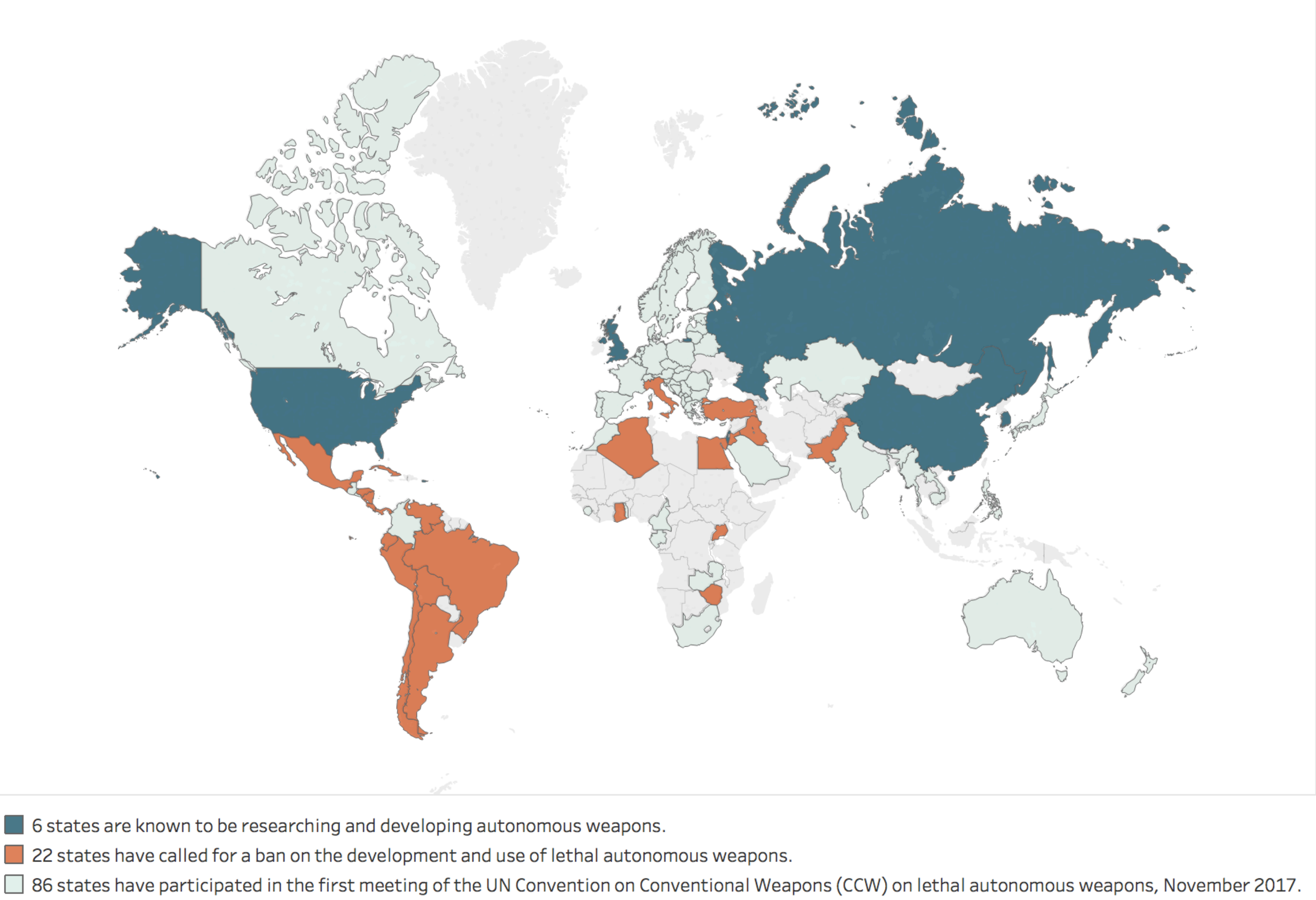
European Union and Japan

The UK has endorsed the concept of human oversight over autonomous systems. The Ministry of Defense Joint Doctrine Publication (JDP) on Unmanned Aircraft Systems proclaims that the "the operation of [UK] weapons will always be under human control as an absolute guarantee of human oversight, authority, and accountability for weapon usage."[98] The EU and Japan have also instituted restrictions on AWS development. In 2014, the European Parliament passed a non-binding resolution calling for a ban on the "development, production, and use of fully autonomous weapons which enable strikes to be carried out without human intervention."[99] In 2016, Japan published a position paper stating it has "no plans to develop robots with humans out of the loop, which may be capable of committing murder."[100]

China

China does not have a published policy on AWS. However, it was the first permanent member of the UN Security Council to call for a legally binding protocol on LAWS citing an earlier treaty that prohibited blinding lasers as precedent. China has since altered its position, calling for responsible use of LAWS in accordance with IHL.[101]

Exhibit 7. Global View of Autonomous Weapons Debate



■ 6 states are known to be researching and developing autonomous weapons.

🟧 22 states have called for a ban on the development and use of lethal autonomous weapons.

□ 86 states have participated in the first meeting of the UN Convention on Conventional Weapons (CCW) on lethal autonomous weapons, November 2017.

Source: Adapted from "The GGE on Lethal Autonomous Weapon Systems", Campaign to Stop Killer Robots, 2017, https://www.diis.dk/en/research/four-reasons-why-denmark-should-speak-up-about-lethal-autonomous-weapons.

International Regulations

In 2017, the UN Group of Governmental Experts (GGE) convened a formal meeting on AWS under the aegis of the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons (CCW). Countries in attendance expressed concern about the legal, ethical, and technological challenges of LAWS and agreed they should conform to IHL. Yet no consensus emerged on how to regulate or restrict AWS. The US and UK, among others, opposed a ban on LAWS while the China and several other nations opposed any action on LAWS at this time.[102]

Definitional, Technological Questions Inhibit Regulatory Action

Two challenges emerged during the recent GGE meetings. First, delegates significantly differed in their interpretations of key AWS terminology. Debates over "autonomous" versus "automated" and "meaningful human control" plagued much of the proceedings.[103] Second, many delegates showed reluctance to institute legally-binding rules that could constrain existing research and development programs. China's shifting stance on regulation could be indicative of their growing interest and investment in autonomous technologies.

Academics Kenneth Anderson and Matthew Waxman argue that the US should focus on developing norms rather than binding rules to avoid stifling technological innovation. This “downstream” regulatory approach formulates laws as new advancements occur rather than anticipating and preemptively legislating against future challenges.[104] Ronald Arkin has argued that AWS might one day be able to discriminate between combatants and non-combatants, demonstrate proportionality, and otherwise adhere to existing rules of law -- and rallied against a ban that could ultimately save more lives.[105]

Consumer Insights

Consumer insights analyze patterns in human behavior to optimize the effectiveness of a good or service for the customer with the ultimate goal of increasing sales or optimizing operations.[106] Advances in machine learning combined with growing customer datasets have transformed the consumer-business relationship from responsive and personalized to predictive. Retailers have increased their reliance on algorithms to provide insights that can better forecast demand, set prices, and recommend products to their customers. Predictive analytics can even suggest ideas for new products by uncovering changes in customer preferences.[107] The power of consumer insights is not limited to retailers; technology giants like Google and Facebook rely on machine learning to optimize their advertising. Overwhelmingly, customers are welcoming the increased personalization and convenience that consumer insights provide. However, they are also concerned about how data is obtained, stored, and used.

Current Challenges and Future Solutions

Ensuring Privacy and Building Trust

Customers are demanding increased transparency on how their data is used and shared by companies, with trust of third-party data collectors at an all-time low. Companies must first establish informed consent by being clear about the collection of customer data and utilizing a blend of approaches to provide meaningful privacy notices at appropriate stages. After ensuring informed consent, companies must provide tools that help customers control if, when, and how their data is collected. Strengthening "Do Not Track" tools is particularly significant, as they can help consumers control if or when their data is collected. Ultimately, ensuring costumers have adequate control over their information will lead to greater trust between the two parties.

Companies should also implement ethical principles to strengthen protection standards. Employees in smaller organizations can use these principles as benchmarks when working on consumer insights projects. Larger companies should create ethics boards to help scrutinize projects and assess complex issues arising from data-reliant analytics.

Discussion of Risks and Benefits

From Insight to Foresight

Data-driven consumer insights have provided useful analytics for years. However, advancements in machine learning have moved them from static analysis to responsive and predictive insights. Retailers in every market – from grocery store chains to the US Postal Service – have dedicated teams that sift through consumers' shopping patterns and personal habits to produce better insights.[108] According to PwC's 2018 Global Consumer Insights Survey, "45% of store operators say they plan to increase their use of AI within the next three years."[109] In a press release, PwC Global Consumer Markets chairman John Maxwell commented on this growth, "AI is moving very rapidly into the consumer and retail sectors. Consumers are shifting their shopping behaviors […] within two to three years AI could revolutionize how companies profile, segment, and serve customers."[110]

AI Enables the Shift from Mass to Personal Marketing

Retailers are turning to firms specializing in customer relationship management (CRM) to reap the full benefits of algorithms. Founded in 2012, StoryStream is a veteran among firms helping brands enhance their consumer insights. CEO and co-founder of StoryStream, Alex Vaidya, explains that “today’s customers are ultra-connected, looking for instant gratification and searching for high-quality personalized purchasing experiences from brands."[111] When Co-Op*,* the UK’s fifth largest retailer*,* used StoryStream’s AI platform to provide personalized marketing, their average length of website visit increased five times with an eightfold increase in content curation time for the retailer’s marketing team.[112]

Japanese retailers are also taking advantage of AI-backed consumer insight platforms. After cosmetics company Shiseido used Saleforce’s AI consumer insights platform, their Chief Digital Officer Alessio Rossi praised the technology and said it helped the company build a better view of their customer by “aggregating and analyzing all the data fragments to build customer profiles that are more meaningful and actionable.”[113] Similarly, Japanese clothing company Uniqlo touts itself as a retailer specializing in “clothing with innovation” and utilizes AI technology for various tasks, from managing inventories to customer communication.[114] CEO Tadashi Yanai explains that the company is expanding into a "digital consumer retail company" and “turning information into superior products.” Their use of consumer insights extends beyond the online sphere to the real-world by using past purchase histories to display products on customers’ phones when they visit stores.[115]

Increasing Operational Efficiency: Managing Inventories

The discussion around AI consumer insights often focuses on CRM. The technology, however, can also optimize operations. Japanese convenience store chain Lawson is one of a growing number of retailers that uses algorithms to calculate product inventories using consumer data and other factors like past sales and weather patterns to predict customer demand.[116] In 2017, citing workforce shortages in Japan, the retailer announced the opening of the "Lawson Innovation Lab,” a facility focused on investigating how to integrate AI technology into convenience store management.[117] Likewise, German e-commerce retailer Otto uses algorithms to examine billions of customer transactions and predict future purchases. As a result, Otto has cut surplus stock by 20% and decreased the number of product returns by more than two million items per year. Furthermore, Otto orders 200,000 items a month from vendors without human involvement, trusting their AI platform’s extraordinary accuracy.[118]

Finding the Perfect Price: Price Optimization and Dynamic Pricing

Advancements in AI have widened the use of price optimization to retailers outside of airlines and hotels. [119] In a recent study, University of Pennsylvania professor David Simchi-Levi found that retailers “increased their revenue, market share, and profit for selected products by double digits by using technology that set optimal prices in near real time and on an ongoing basis.”[120] Going beyond simple price optimization, Uber uses dynamic pricing in its ridesharing application.

The Unconvinced: Marketers and AI

While many retailers enthusiastically use AI technologies to advance their consumer insights, create content, manage product selection, increase personalization, and ultimately increase customer retention and acquisition, not all marketing experts believe that AI will transform the industry. Resulticks surveyed more than 300 marketers and found almost half believed “artificial intelligence was an overhyped industry buzzword,” while 40% were skeptical of the term. The survey also noted that 47% of respondents believed “AI was more fantasy than reality.”[121] Marketers’ skepticism may be rooted in the difficulty of integrating AI technologies and consumer insights, especially for smaller brands and retailers. The shortage of data scientists and the need to rapidly build new systems make it hard to implement AI technology in consumer insights.[122]

The Tug of War Between AI in Consumer Insights and Transparency

Critics chide the industry’s overreliance on massive datasets of customer information. Industry experts agree that retailers must properly handle these vast troves of data. Sanjay Srivastava, Chief Digital Officer of professional services firm Genpact, agrees that AI is a “game-changer” for improving the customer experience but warns that “real challenges remain regarding trust and privacy.”[123] Citing a Genpact study, he warns that consumers are increasingly worried about how their information is tracked and used in retail. Srivastava notes that companies should have “visibility into AI decisions” and have the capability to uncover their reasoning and ensure responsible storage and use of data.[124]

The “black box” refers to the lack of clear logic or explanations behind many algorithms and remains a barrier to transparency between businesses and consumers. A recent White House report observed “big data analytics may create such an opaque decision-making environment that individual autonomy is lost in an impenetrable set of algorithms.”[125] Autonomy of data refers to ensuring businesses have consumers’ informed consent when tracking their information. Also commenting on the opaque nature of AI decision-making, Federal Trade Commission Chairman Edith Ramirez says there is “no traditional way for operators to make disclosures about what information they are collecting and how they will use it.”[126] Ramirez also points to challenges in governing algorithms due to the haziness surrounding data collection.[127]

The tug of war between providing personalized, quality customer service and protecting data in a transparent manner is not new. Julie Bernard, CMO of Macy’s, expressed a common frustration among marketers during the D2 Digital Dialogue conference in 2013: “There’s a funny consumer thing... They’re worried about our use of data, but they’re pissed if I don’t deliver relevance … how am I supposed to deliver relevance and magically deliver what they want if I don’t look at the data?”[128] This tug of war will continue as retailers struggle to find a balance between personalization and data privacy and consumers grapple with how much data they wish to share.

Ensuring the Autonomy and Anonymity of the Consumer

The public’s general tech ignorance and businesses’ long and complicated terms of conditions jeopardize consumer autonomy.[129] John Edwards, New Zealand’s Privacy Commissioner, cited a pervasive lack of informed consent by consumers, saying that algorithms “pose challenges for a consent model of data collection,” and increase data privacy risks. Furthermore, Edwards noted that decision-making machines may be used to “engender or manipulate the trust of the user.”[130]

In addition to autonomy over personal information, customers demand anonymity during data collection. They misunderstand that re-identification of data is sometimes possible. Peter Fleischer, Global Privacy

Counsel at Google, says that “privacy standards [will] continue to be pertinent for new technologies but AI decision algorithms [raise] particular problems such as finding ways to re-identify data.”[131] To maintain consumer trust, businesses that have access to consumers’ private information, such as “medical histories, personal habits, financial situations, and family relations,”[132] must establish security measures to ensure information cannot be re-identified or made public. Not adequately protecting the anonymity of consumers’ data bring undercut the reputations of businesses.

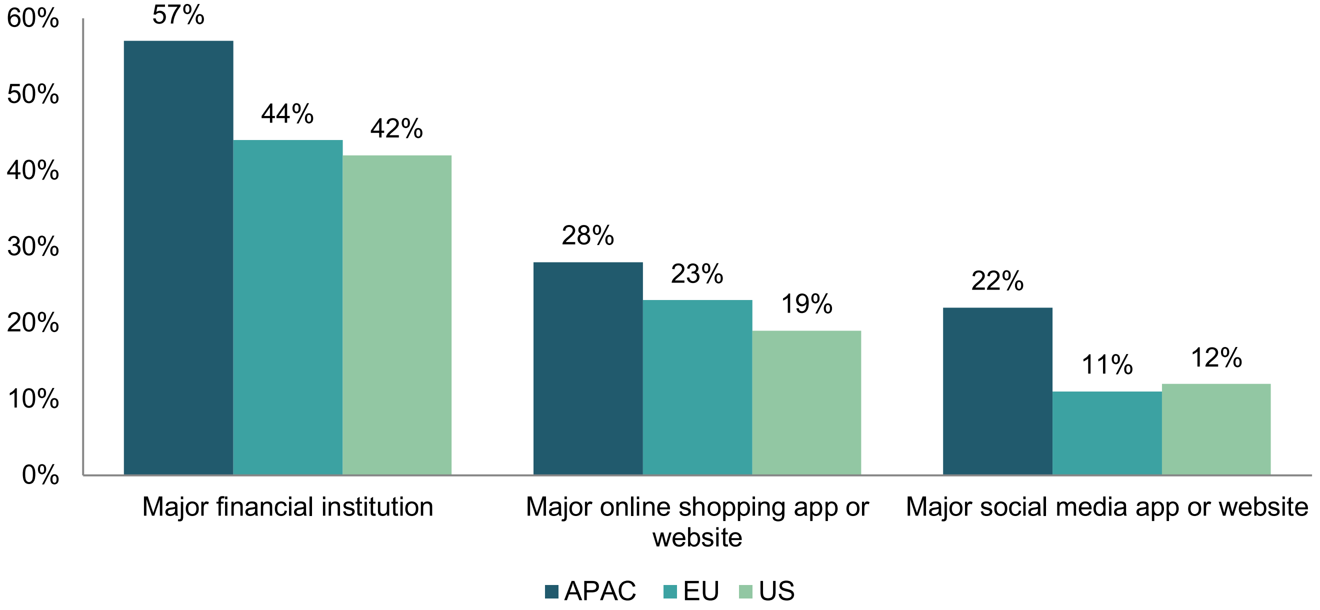
Exaggerated Risks, Mischaracterizations, and Public Concern

Rising Consumer Expectations on Data Protection Affect Retailers More than Other Industries

Customers are increasingly aware of data breaches and data storage and use violations. According to a 2018 survey by the Harris Poll, only 20% "completely trust" organizations to maintain the privacy of their data.[133] The survey also indicates trust of companies’ ability to protect customer information is the highest in China, where 69% of respondents say they ‘strongly agree’ or ‘somewhat agree’ with statement, “I am very confident in companies’ current ability to securely protect information.” [134] Conversely, German respondents showed the most distrust in companies’ current ability to securely protect information. [135]

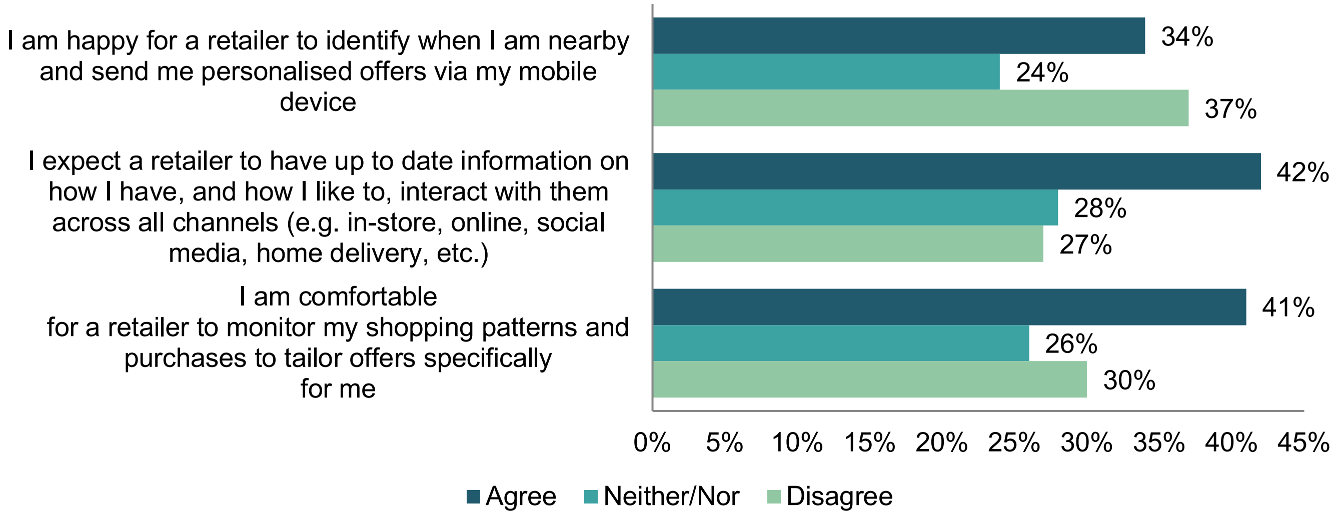
Retailers have borne the brunt of this public distrust. According to IBM’s Future of Identity Study, only 19% of US consumers, 23% of EU ones, and 28% of Asia-Pacific (APAC) ones would trust a retail organization to protect their biometric data, as shown in exhibit 8.[136] A much larger percentage of consumers – 42%, 44%, and 57% in the US, EU, and APAC respectively, do not trust financial institutions to safely store this data.[137] Retails must work harder to strengthen trust with consumers and correct these mischaracterizations.

Exhibit 8. Customers are most likely to trust their biometric data to major financial institutions



Source: Adapted from "IBM Security: Future of Identity Report”, IBM, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=22012422USEN

Exhibit 9. Consumer Sentiment on Data Collection by Retailers



Source: Adapted from "Artificial Intelligence: Touchpoints with Consumers," 2018, PricewaterhouseCoopers, https://preview.thenewsmarket.com/Previews/PWC/DocumentAssets/503395.pdf

Is Too Much Personalization a Bad Thing?

There is a subtle balance between improvements in customer service through personalization and knowing so much that consumers experience the "creep factor," a popular term cited by opponents of heavy personalization in consumer insights.[138] However, according to the aforementioned PwC survey, 41% of respondents feel comfortable with retailers monitoring their shopping habits to tailor special offers for them, detailed in exhibit 9.[139] Jason VandeBoom, CEO of ActiveCampaign, acknowledges "there is definitely a 'right' and a 'wrong' way to do personalization," stating that "personalization can certainly increase the effectiveness of your marketing communications, but companies need to be conscious of privacy. Yes, there's a moral reason to consider privacy, but also consider the fact that 'over-personalized' content may cause some to tune out."[140] While many doubt this "creep factor" will deter consumers from specific brands, retailers should still consider how to make the customer experience personalized yet comfortable.

Adverse Outcomes and Lessons Learned

Amazon's Failed Experiment with Price Discrimination

Taking price optimization one step further, some retailers are engaging in price discrimination, where firms charge different prices for different consumers based on their willingness to pay more or less for a product. In September 2000, Amazon employed price discrimination, possibly violating the Robinson–Patman Act.[141] After a buyer deleted cookies that identified him as a regular Amazon customer, he was offered a DVD for a substantially lower price than before. Amazon CEO Jeff Bezos said it was "a mistake" for the company to experiment with setting different prices for different customers.[142] He has subsequently ensured pricing methods do not use demographic information when determining the cost of a sale. Amazon refunded an average of $3.10 to 6,896 customers as a result of this controversy.[143]

Dynamic pricing has become more widespread over the years yet the Amazon controversy serves as a warning for companies using this technology. Some experts have suggest targeted coupons could make differential pricing more acceptable to the general public: “as long as things are presented in the form of a discount for your special behavior, people accept it.”[144]

OfficeMax Blunder and the Danger of Moving Humans out of the Loop

In 2014, Mike Seay received an advertising email from OfficeMax that was addressed to "Mike Seay, Daughter Killed in Car Crash."[145] Seay's 17-year-old daughter had died in a car crash the previous year.[146] This marketing mishap had disastrous reputational consequences for the company. Media outlets rushed to cover it, which OfficeMax blamed on a data broker for merging the wrong information fields. In a statement, the company said the mistake was "a result of a mailing list rented through a third-party provider" but did not say whether the company held similar data on other customers.[147] The OfficeMax incident is a blunt reminder of the reputational risks undertaken when humans do not supervise marketing decisions.

Current and Pending Regulations

Data-driven, AI-backed consumer insights provide outstanding opportunities for retailers to offer personalized, responsive customer service. However, reliance on massive datasets brings heightened regulatory scrutiny. Europe is leading the charge, creating robust standards for data protection and privacy.

European Union

On April 6, 2016, the EU adopted the General Data Protection Regulation (GDPR). The GDPR requires regulatory modifications to virtually every area of customer data management. On May 2018, retailers serving European customers will have to comply with new regulatory standards, additional administrative burdens, and accountability for violations, as well as more severe enforcement penalties.[148] As of July 2017, a study from software firm Compuware indicates 77% of retailers have not implemented a robust GDPR strategy and less than half of retailers felt that they were “well briefed on the regulation and how it will impact the way consumer data is handled.”[149] Retailers should carefully examine these new regulations. Failure to follow the GDPR mandate could significantly impact their businesses.

United States

The United States has enacted pieces of legislation on federal privacy and data security.[150] States and territories also have their own standards on data protection. California alone has more than 25 privacy and data security regulations.[151] Furthermore, companies regulated by the Federal Trade Commission (FTC) are subject to penalties if they employ unfair or deceptive trade practices – a regulation often used to pursue companies that lack sensible data security measures.

Japan

The Personal Information Protection Commission (PPC) serves as the supervisory organization on matters concerning privacy protection in Japan.[152] The organization recently amended legislation to require companies to obtain prior affirmative consent for cross-country transfers of Japanese consumer data unless the country is designated as having adequate protection by the PPC.[153]

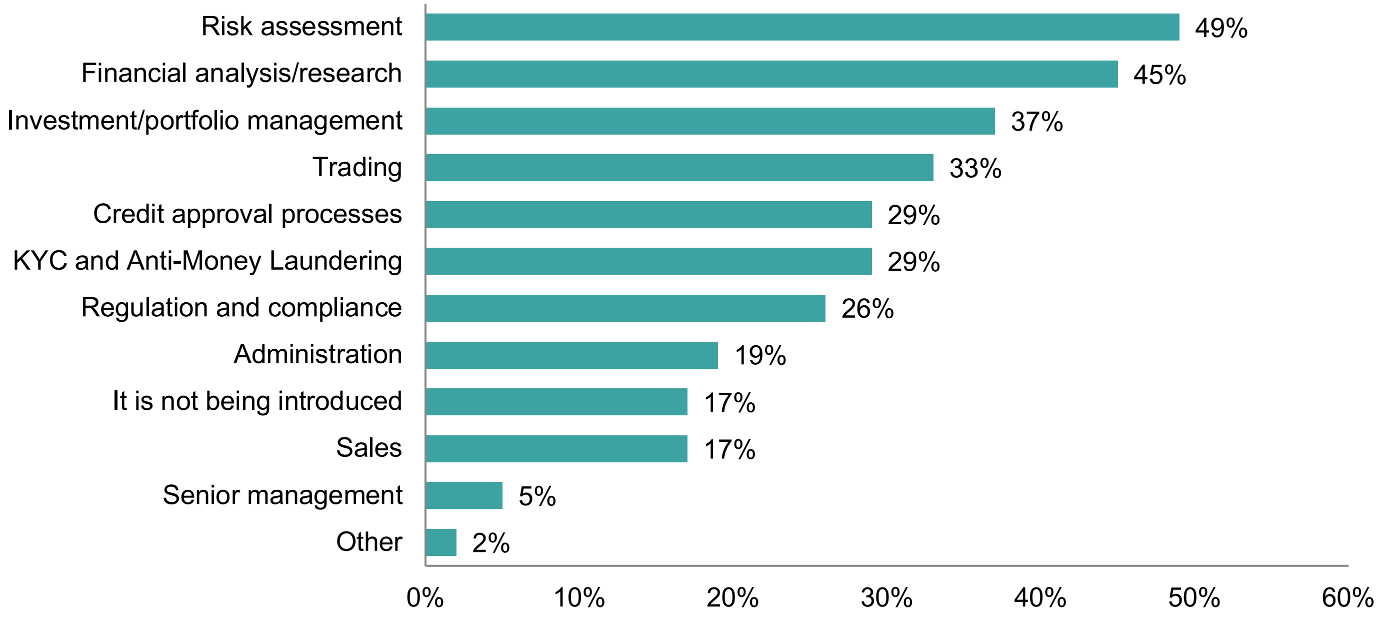
China

In 2017, China introduced its National Cybersecurity Law, the country's first domestic mandate on cybersecurity and data privacy protection.[154] However, China does not have wide-spread, comprehensive data protection legislation. Provisions in laws such as the General Principles of Civil Law and the Tort Liability Law can be used to infer data protection as a right.[155] However, such understanding of the law is ambiguous and often hard to enforce.

Financial Risk Pricing

Financial risk pricing uses AI to gather and parse client data to assess credit risk, insurance claims, and other assessments. According to a Euromoney survey, almost half of 424 senior financial executives and industry experts believe that AI will be introduced to risk assessment applications in the next three years.[156] This section focuses on a prominent example of financial risk pricing: AI credit scoring.

Exhibit 10. Where do you expect AI/machine learning technology to be introduced in your organization in the next three years?



Source: Adapted from "Ghosts in the Machine: Artificial Intelligence, Risks and Regulation in Financial Markets," Euromoney, April 25, 2016, https://www.euromoney.com/article/b12knxplnphttt/ghosts-in-the-machine-artificial-intelligence-risks-and-regulation-in-financial-markets

Current Challenges and Future Solutions

Explaining Algorithmic Decision-Making Takes Priority

The public and financial institutions are primarily concerned with black box scoring and the associated legal risks. Algorithmic decision-making must be more transparent to alleviate public trust issues before widespread adoption is feasible. To do this, companies must be able to explain how their product reaches assessment results in an understandable way for the general public. Moreover, policymakers should clarify the expected level of transparency and explainability so financial companies can comply with related laws.

Degree of Financial Inclusion Might Determine Acceptance

Many organizations expect AI credit scoring to generate greater financial inclusion. Countries with relatively low levels of financial inclusion might be more receptive to AI credit scoring. Stronger pushback is anticipated in countries where a large portion of citizens already have traditional credit scores. China is a special case. The Chinese government is developing its own social credit score, so entities developing similar technology might face added scrutiny or restrictions.

The Jury Is Still Out on the Social Benefits of AI Credit Scoring

It is still unclear whether AI credit scoring enhances financial inclusion or perpetrates biases in existing systems. Scoring developers should explain how AI achieves inclusion instead of exclusion. Policymakers need to study the effects of using non-traditional datasets when determining legislative outcomes. They should also recognize that bias cannot be completely eliminated in credit scoring systems. Banning or restricting this application would be a wasted opportunity to improve financial inclusion across the world.

Discussion of Risks and Benefits

AI Credit Scoring Could Bring Greater Financial Inclusion

Under traditional scoring systems, those lacking sufficient credit cannot attain a score. A 2015 Consumer Financial Protection Bureau (CFPB) report found that 26 million consumers in the US lack a credit history and another 19 million cannot be scored.[157] These "credit invisible" people are unable to access traditional financial services such as credit cards, loans, or home leases. However, utilizing a wider array of information to calculate scores can make these people "visible" and also enable financial companies to increase their customer base without incurring greater risk. FICO and a number of startup companies across the world are developing AI credit scoring systems.[158] ZestFinance, one such company, says these systems will help increase approval rates.[159] In countries where a large portion of citizens still rely on non-traditional sources of credit, financial inclusion is even more critical. According to Forbes Magazine, only 25% of Chinese have a credit history.[160] In trying to fix this problem, China is developing a Social Credit System, which rates 1.4 billion citizens on a wide variety of attributes including online behavior, social media connections, educational background, and employment records to judge their eligibility for financial services and other benefits.

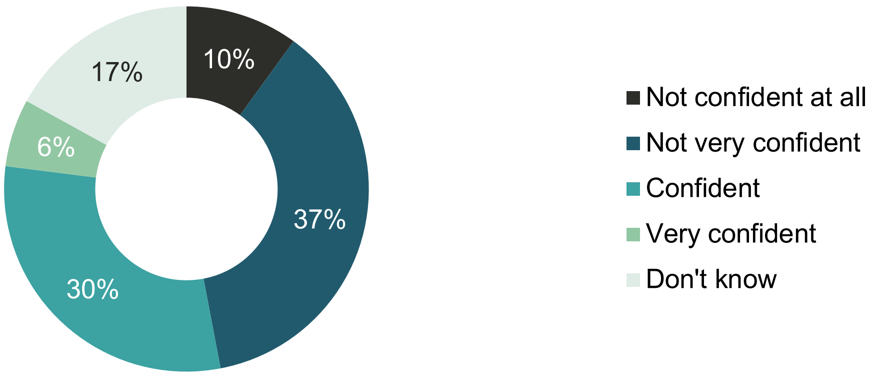
… But Not All Experts Agree

Despite expectation that AI will improve financial inclusion, some entities raise concerns about using broad and granular data in algorithms. Attorney Chi Chi Wu of the US National Consumer Law Center in a 2015 Report noted that minorities have significantly lower credit scores than whites due to the racial-economic divide and wealth gap in America.[161] According to Wu, minority and low-income consumers are often denied credit, insurance, or other services and have to pay more than other racial groups. An OECD report on Technology and Innovation in the Insurance Sector notes that data aggregation for actuarial purposes could "lead to potentially too high premiums or un-insurability of certain segments of the society or individuals, or ethically questionable outcomes."[162]

AI Credit Scoring Systems Lack Transparency and Accountability…

Experts contend that AI credit scoring might exacerbate transparency issues due to their "black box" procedure. In Germany, a non-profit organization recently launched a campaign called "OpenSchufa."[163] Credit scores calculated by Schufa are used for a variety of purposes such as lending, leasing, or mobile phone contracts. The OpenSchufa campaign argues that the public and even the German government do not know how the company calculates its scores. The non-profit has attempted to uncover the credit bureau's methods by collecting and analyzing actual credit reports. Schufa says it does not use any information from social media nor other discriminating data.[164]

Exhibit 11. How confident are you that all material legal risks associated with new financial technologies have been properly understood by your organization?



Source: Adapted from "Ghosts in the Machine: Artificial Intelligence, Risks and Regulation in Financial Markets."

However, if they or other companies try to incorporate more granular data in the future, the public will likely push back even more. In response to rumors that Schufa wanted to use social media data in 2012,[165] then German Justice Minister Sabine Leutheusser-Schnarrenberger told Spiegel Online that they and other credit agencies "must fully disclose their intentions on how they will use Facebook data to determine creditworthiness."[166]

And Also Bring Legal Risks

Using AI credit scoring algorithms without understanding their specific mechanics could violate data privacy or fair lending laws. World Privacy Forum, a non-profit public interest research group, warned in a recent report that consumer scores could utilize discriminatory factors like race or gender or sensitive factors like health or financial data "without any public notice."[167] A survey conducted by Euromoney reveals that only 30% of companies surveyed feel confident their organizations understand the legal risks associated with new financial technologies like AI credit scoring.[168]

Exaggerated Risks, Mischaracterizations, and Public Concern

Many experts have highlighted the potential bias within algorithms and learning data for credit scoring. However, this risk is already present in existing systems. For example, critics condemn Schufa for its opaque algorithms even though they do not incorporate non-traditional data. According to the Washington Law Review, critics have long-questioned the fairness of credit scoring systems in the US, specifically their "opacity, arbitrary results, and disparate impact on women and minorities."[169] All risk pricing systems are subject to bias to some extent. AI credit scoring will not eliminate bias but might lead to superior outcomes and better inclusion than existing systems.

Yet the benefits of financial inclusion might also be exaggerated. Credit invisible people could still get low scores with expanded data inputs. A better measurement is whether or not these scores provide greater access to financial resources and services.

ZestFinance claims its credit scoring technology has helped e-commerce client JD.com approve 150%

more borrowers and allowed a top five US credit card issuer to increase approvals by 9%.[170] However, this data is too short-term and narrow to extrapolate a broader pattern. There are simply not enough comprehensive studies to ascertain whether AI credit scoring has generated greater financial inclusion.

Adverse Outcomes and Lessons Learned

While AI credit scoring systems have become more popular and widespread, it is hard to tell if they violate discrimination laws because of the complexity and opacity of their algorithms.

Credit scoring is opaque for two reasons: First, opening calculation methodologies to public scrutiny might make scores prone to manipulation. If people know what affects their score, then they are likely to try to improve it. Consumers can more easily change their behavior on social media or online than their financial activities. Moreover, disclosing calculation methodologies can put companies at a competitive disadvantage. The German Federal Court of Justice (BGH) said that Schufa's score procedures are equivalent to trade secrets.[171]

Even if consumers know how companies compute their scores, proving discrimination is almost impossible given the enormous amount of data inputs in credit scoring. In addition, watchdogs must analyze numerous score reports to find patterns of discrimination. Consumer Reports, for instance, analyzed more than two billion car insurance price quotes in an attempt to reveal price discrimination in car insurance.[172]

Some companies are hesitant to adopt AI credit scoring due to its opacity and the associated legal risks. However, ZestFinance claims they have built an explainable machine learning system to mitigate client fears. Their Automated Machine Learning solution (ZAML) will allow companies to harness "the power of machine learning" while ensuring models are "safe, fair, and compliant with the law."[173]

Current and Pending Regulation

Consumers are mainly concerned about the accuracy and fairness of their scores. In general, data privacy and fair lending laws protect them from discrimination. The 2013 OECD Guidelines on the Protection of Privacy and Transborder Flows of Data enshrine consumer data protection rights. [174] In addition, each country has specific data privacy or fair lending laws based on the OECD guidance.

European Union

The EU's Directive 95/46/EC prescribes the right of individuals to obtain data from a data controller and to have that data rectified, erased, or blocked if it is inaccurate or incomplete.[175] On May 25, 2018, the GDPR will become effective, which prescribes the same rights for individuals as Directive 95/46/EC. [176] In addition, the GDPR prohibits "fully automated decision-making, including profiling that has a legal or similarly significant effect," and Ricital 71 gives "automatic refusal of an online credit application" as an example of fully automated individual decision-making which has a "similarly significant effect." The GDPR also includes a series of guidelines on automated individual decision-making and profiling[177] but it is still unclear how this legislation will be implemented "at a technical level in practice."[178]

Japan

The Act on the Protection of Personal Information states that a business operator handling personal information "shall disclose the retained personal data when the person requests, and the person also has a right to request correction of the data if it is not accurate or complete."[179] Historically, there is no universal credit score like FICO or Schufa in Japan. However, Mizuho Bank and SoftBank Group launched a lending service company "J. Score" in 2016, which uses AI technology for credit scoring.[180]

China

Although China does not have a comprehensive data protection law, Personal Information Security Specification will come into effect in May 2018[181]. Samm Sacks in Center for Strategic & International Studies analyzes "the Standard more permissive for companies than the GDPR,"[182] but thus far the actual effect of this standard is uncertain. Moreover, credit scoring companies should keep a close watch on additional potential regulation. According to Business Insider, the People's Bank of China (PBoC) is casting doubt on credit scoring systems built by private firms such as Tencent and Alibaba despite the fact that the PBoC selected those companies to build a pilot system in 2015.[183] Now PBoC is developing its own social credit scoring system and fears these companies might threaten it. However, the Government has not revealed how it plans to regulate them.

United States

In contrast to Europe and Japan's more general data privacy laws, the US has specific legislation related to credit assessments. These include the Fair Credit Reporting Act (FCRA) and the Equal Credit Opportunity Act (ECOA). The Federal Trade Commission (FTC) has the authority to enforce compliance with these acts. The FCRA determines the "permissible purposes of consumer reports" and requires agencies that assemble or evaluate consumer credit information to disclose all information in a costumer's file if requested.[184] The ECOA prohibits discrimination against credit applicants on the basis of race, color, religion, national origin, sex, marital status, or age and plaintiffs must show disparate treatment or disparate impact to prove discrimination. [185] A recent FTC report discusses big data research considerations such as financial inclusion versus exclusion and steps companies should take to avoid violating laws like the FCRA and ECOA. However, the Report does not mention any amendment of the laws in response to the increasing use of big data. Many experts including researcher Mikella Hurley believe policymakers should expand these laws to cover these concerns.[186]

"To the extent that FCRA requires alternative credit-scoring companies to provide consumers with the opportunity to access and correct information about them, it may prove practically impossible for consumers, when dealing with big-data scoring systems that potentially integrate thousands of variables, to verify the accuracy of their scores and reports or to challenge decisions based on alternative models… Proving a violation of ECOA is burdensome, and the use of highly complex big-data credit-scoring tools may only exacerbate that difficulty." - Mikella Hurley and Julius Adebayo[187]

Healthcare Diagnostics

AI holds immense potential for the healthcare industry. Consequently, the AI healthcare market is expected to grow at a compounded rate of 40% over the next three years and tenfold in the following five.[188] While the technology impacts the entire spectrum of healthcare services, this section primarily focuses on AI-enhanced diagnostics or any application that deals with the diagnosis of an illness or other problem, either directly with patients or within a laboratory research setting.

Current Challenges and Future Solutions

Three core themes influence the future trajectory of AI in healthcare: privacy, transparency, and liability. First and foremost, the way in which patient data is handled will significantly affect AI development in healthcare. If used with precision, it will substantially contribute to the advancement of AI technology, creating a range of benefits but if handled carelessly, it could jeopardize patient trust that might prove difficult to regain. Medical practitioners are bound by strict codes of ethics and privacy. As AI healthcare devices become more integrated into the industry, they too must exist within a space of tightly controlled privacy. Proactive, preventative steps should be taken by both the private and public sector to bolster privacy and encourage the development of potentially life-saving technologies. Just as the financial sector experiences regular auditing, so too must AI healthcare platforms. Within the private sector, DeepMind is working on a platform to increase transparency trust through a tracking project called the Verifiable Data Audit (VDA).[189] The project will enable partners to see who has accessed data, when, where and why.[190] Projects such as VDA increase transparency through accountability. These “spot checks” help ensure data privacy protections. Regulatory bodies within the public space should also encourage data protection measures and audits.

The second theme concerns the challenge of addressing transparency and creating regulatory certainty. Technological innovation and legislation must work hand-in-hand. Experts agree there is no single answer but a necessary synthesis of solutions: give patients choices, further public trust through appropriate regulatory and legislative frameworks, develop appropriate technical safeguards and privatize information by removing identifying components, and use verifiable auditing techniques to ensure confidential data is handled properly.[191]

Questions surrounding liability represent the third core theme: As AI healthcare devices become increasingly common, the risks associated with them pose liability concerns to both patients and medical professionals providing care. In order to mitigate the potential of medical malpractice, the degree of discretion physicians exercise alongside AI platforms should remain high. By keeping human oversight over AI devices, these technologies may actually reduce the viability of negligence claims against healthcare providers – all while advancing an industry with the potential to save hundreds of millions of lives.[192]

Discussion of Risks and Benefits

Few experts oppose using AI healthcare applications, as they hold the potential to save costs, increase access, and boost quality of care. Yet they tend to highlight the risks that go hand-in-hand with rapid, unplanned, and unsecured expansion. In particular, experts believe AI healthcare applications should be subject to human oversight and heightened data and privacy protections.

AI Can Save Healthcare Industry Expense, Improve Accuracy of Diagnostics

AI healthcare applications have the potential to create $150 billion in annual savings for the US healthcare economy by 2026.[193] In addition to cost savings, Simon Stevens, Chief Executive of the National Health Service (NHS) in England, argues that AI has "the potential to interpret clinical data more accurately and more rapidly than medical specialists."[194] Bill Gates also highlights the positive impact AI can have for healthcare workers.[195]

Data Sharing and Protection Concerns Unite Academics and Practitioners

Experts, academics, and practitioners alike share common concerns surrounding proper data usage. Norman Lamb, Chair of the Science and Technology Select Committee in the UK Parliament, represents the group of thinkers who push for stronger privacy. He highlights the diligence required in using patient data to underline the potential downsides of careless handling: "Trust is going to be of central importance – if we lose the trust of people then we won't be able to realize the great opportunities ahead of us."[196] Practitioners, meanwhile, tend to underscore the challenges to adoption of data sharing, rather than focusing on the risks of high-speed adoption. Sally Daub, CEO of medical deep learning company Enlitic, echoes the importance of protection while emphasizing the need for sharing: "Keeping healthcare records secure is obviously very important, but in AI the true benefit will come from sharing data while respecting patient privacy. If everybody sits in their silos, we're not going to progress."[197]

Usage Concerns: Human Agency

The general sentiment in the UK and Germany is skeptical about fully autonomous AI healthcare applications. Human intuition, a personal touch, and quick decision-making in unexpected situations, are living qualities that many fear will be absent or weaker in AI systems.[198] Consequently, majorities in these regions would prefer a human health care professional over a machine.[199] This attitude is mirrored in expert assessments as well. For example, Eric Schmidt spoke about the preference for human oversight in his speech at the 2018 Healthcare Information and Management Systems Society Conference.[200] Even in China, often cited as a country with little public concern for privacy, the story is more complex. Hu Weiguo, Vice President and Director of the AI Project at Ruijin Hospital in China says: "Ethics, family values, and financial circumstances all need to be taken into consideration for a final treatment decision. That's what [IBM] Watson can't accomplish, so it can only ever be an assistant."[201]

Some Practitioners Remain Skeptical of the AI Hype

Experts point to a variety of AI risks that might negatively impact the healthcare industry. Dr. Joseph Kvedar, Vice President for connected health at Partners HealthCare in Boston and an Associate Professor of Dermatology at Harvard Medical School, points to the lack of evidence proving the clinical accuracy of AI healthcare applications.[202] Others are concerned that data generated by this technology will create information overload for doctors. Moreover, Kvedar is unsure if the data coming in from physical monitoring devices is even helpful.[203] Other healthcare providers are unsure that AI is as reliable as other technologies they have used for years, oftentimes decades. Lukasz Piwek, a University of Bath data scientist, summarizes succinctly: “In a practical sense the implementation of this is still quite problematic.”[204]

Exaggerated Risks, Mischaracterizations, and Public Concern

Narrow Scope of Current Applications Mitigates Risks

AI healthcare diagnostics bring real risks. Accuracy is the most predominant one, especially for applications in clinical settings. AI systems rely on expansive datasets but clinical trials may face challenges when algorithms meet unknown data or scenarios. Protection of data is yet another risk. The information collected and utilized by AI healthcare applications is the most sensitive in the world. Trust must also be maintained between physicians and patients, as well as healthcare companies and the greater public. AI applications should consider integrating transparency mechanisms, such as audits, in order to ensure solutions are thoughtful and legitimate.

While the above risks are real, current AI applications – like diagnostics – are specific, narrow, and limited in scope. Due to technological limitations, narrow systems will perform individual tasks for the foreseeable future: the ability for a system to fully integrate each and every capacity of a doctor is currently impossible and will likely remain so for the foreseeable future.[205] Technologists thus believe that current applications are relatively low risk. In fact, many practitioners are concerned that unrealistic expectations and hype surrounding AI healthcare could derail the industry. Some believe that an “overwhelming amount of misinformation and myth” about the technology will negatively impact healthcare.[206]

AI Might Aggravate and Propagate Existing Healthcare Inequalities

Many speculate that AI healthcare applications may propagate existing inequalities. A component of this risk comes from current biases in the data. For example, evidence-based medicine is far more accurate for white men than other groups, leading to concerns about unmodified data “unwittingly perpetuating” societal norms for the majority – but not everybody.[207] Jonathan Bush, CEO of Athena Health, states in the Harvard Business Review: “Most healthcare executives are still unsure of their AI strategy. They sense that AI will be a game changer, but they’re not sure how. […] But while we shoot for the moon, let’s clean up the muck that’s bogging us down today, unleashing our potential to transform healthcare.”[208]

> *"AI systems often function as black boxes, which means technologists are unaware of how an AI came to its conclusion. This can make it particularly hard to identify any inequality, bias, or discrimination feeding into a particular decision. The inability to access the medical data upon which a system was trained—for reasons of protecting patients' privacy or the data not being in the public domain—exacerbates this … By masking these sources of bias, an AI system could consolidate and deepen the already systemic inequalities in healthcare, all while making them harder to notice and challenge. Invariably, the result of this will be a system of medicine that is unfairly stacked against certain members of society." – Robert Hart, Cambridge University*[209]

Adverse Outcomes and Lessons Learned

Cyber Breaches, Negligent Transfer of Data Spook Industry

No high-profile case of detrimental AI decision-making in healthcare diagnostics has been reported yet. This is largely due to the fact that fully autonomous systems are not yet widely deployed in the healthcare field. So far, the focus lies on augmenting and supporting doctors' decision-making process through analyzing data via IBM Watson for Oncology or image recognition software for x-ray analysis.

However, adverse outcomes have resulted from inadequate handling of patient data, resulting in the unintentional exposure and questionable transfer of sensitive patient information. This encompasses cyberattacks on healthcare providers, such as the 2015 breach of the insurance company Anthem, which affected the data of almost 80 million Americans,[210] as well as intentional but negligent transfer of data between hospitals and companies, such as the cooperation between the NHS and DeepMind.[211]

Lack of Care for Data in the DeepMind - NHS Cooperation Project

The Deepmind-NHS cooperation and subsequent controversy provided a useful lesson on how to handle patient data in AI healthcare projects. In September 2015, the Royal Free NHS Foundation Trust agreed to transfer 1.6 million partial patient records that contained personally identifiable information to DeepMind for the purpose of clinical safety testing.[212] DeepMind wanted to use this data to develop its Streams app to detect and diagnose acute kidney injury in hospitalized patients based on results from blood tests.[213] Subsequently, researchers, as well as the UK's Information Commissioner's Office (ICO), found significant shortcomings in the protection of patient privacy.[214] The ICO's investigation revealed that the process lacked transparency, patient consent and thus the agreement violated the Data Protection Act of 1998.[215] These findings caused substantial negative publicity in the British and international press. This incident and its negative reputational effects highlight the need to carefully consider privacy concerns and implications before implementing data sharing agreements.

Current and Pending Regulations

As startups around the globe begin to tackle healthcare questions through AI technology, a regulatory framework for the industry is emerging. Currently, regulations for AI healthcare differ across countries. As a result, many healthcare companies that use AI operate in one country, rather than across multiple jurisdictions. The WHO underscores the importance of regulating medicines and medical devices including AI applications.[216] However, they fail to offer concrete suggestions for global regulatory engagement or international standards moving forward.

European Union

While some countries have existing frameworks for regulation, prominent rulemaking is at the supranational level. The European Commission (EC) has addressed several issues in AI healthcare. Their Medical Devices Directive thoroughly outlines which technologies can be used in the healthcare space,[217] while their Products Liability Directive seeks to mitigate responsibility for those working with existing technologies.[218] The EC supports the use of AI healthcare but recognizes the barriers to deployment. In response, the EU H2020 Funding Programme dedicated €700 million to robotics, including those working in the field of medicine and €120 million to future and emerging technologies such as the Human Brain Project.[219]

With the advent of the GDPR, strict rules surrounding data use will create challenges for AI healthcare companies globally. The GDPR's requirement for total algorithm transparency means European residents have a "right to explanation" for AI-induced decisions. Researchers are now required to explain how machine learning and neural networks reach a decision.[220] Future regulatory initiatives will likely hinge on the implementation and results of the GDPR.

United States

US healthcare regulation is controlled at the national level by the Food and Drug Administration (FDA). In early 2017, the agency announced plans to create a new unit dedicated solely to digital health.[221] The FDA has released multiple documents elucidating its position on digital health in order to help AI developers understand what the agency does and does not regulate.[222] The FDA focuses on high risk products and regulates AI technologies according to the same standards as regular healthcare ones. Research labs, for example, must adhere to the same regulatory standards no matter the technology.[223] Additionally, the Office of the National Coordinator for Health (ONC) and the Agency for Healthcare Research and Quality (AHRQ) are working with other Department of Health agencies, including the National Institutes for Health (NIH) and the FDA to "define and identify possible opportunities for the use of AI in their efforts to improve biomedical research, medical care, and outcomes, including work related to the advent of precision medicine."[224]

Today, it costs two years and seven figures for companies to receive the FDA's basic device standards certification.[225] In order to prevent stifling innovation, some experts have proposed two alternate regulatory requirements: require physicians to rate the appropriateness of all AI-generated decisions; and mandate the FDA collect and publish all ratings.[226] This type of continuous evaluation is already practiced by physicians in other healthcare spaces and could be easily applied.[227]

Japan

Currently, Japan does not have any AI-focused regulations for healthcare. However, its new Council on Promotion of AI in the Field of Healthcare within the Japanese Ministry of Health, Labour, and Welfare (MHLW) has selected six high-priority areas for AI healthcare and proposed measures for future development.[228] In the area of diagnostic and treatment support specifically, the Ministry is considering the role of AI in both the Medical Practitioners' Act and the Pharmaceutical and Medical Device Act.[229]

China

The National Health and Family Planning Commission has published guidelines for the development of AI healthcare.[230] The Commission wants to use the technology to establish a tiered healthcare system to help improve services.[231] According to a guideline on the development of AI released in July 2017 by the State Council, China's Cabinet, AI healthcare applications are encouraged for the country's growing elderly population.[232] The Commission said it is "committed to overseeing amendments to the relevant laws and regulations that will encourage medical institutions and companies working in the sector to use information technology to improve the services on offer while reducing risks and ensuring that patient privacy is fully respected."[233]

Regulatory Frameworks Struggle to Contend with Growing Applications of AI in Healthcare

Regulations the world over will need to acknowledge and account for AI's permeation in the medical industry – regardless of application type or bureaucratic body. The aforementioned global regulations will only control AI-informed devices and treatments.[234] The technology is already trickling into the practice of medicine at every level – not just at the stage of final approval. Biomedical researchers harness AI to navigate hordes of genetic data, pharmaceutical firms to find new drugs,[235] public health officials to predict the next epidemic,[236] and doctors and scientists to grapple with their data-saturated workplaces.

Appendices

Appendix 1: Public Interest

To get data on public interest, this report used Facebook's total engagement analysis for each AI application. Total engagement is defined as the number of comments, reactions, and shares on Facebook acquired through Google search, Google Web Scraper and Facebook API.[237] This analysis uses specific keywords that represents each application (i.e. "artificial intelligence" and "autonomous vehicle") and focuses on websites written in English and published in 2017.

According to this analysis, (Exhibit 12), the general public is most interested in AW, which has more than 120 thousand engagements, followed by AV, Credit Scoring, Healthcare Diagnostics, and Customer Insights.

Exhibit 12. Facebook total engagement for each application

Applications	Search Words	Google Search	Facebook Total Engagement
Autonomous Weapons	"artificial intelligence" + "autonomous weapon"	491	125,372
Autonomous Vehicles	"artificial intelligence" + "autonomous vehicle"	524	79,931
Credit Scoring	"artificial intelligence" + "credit scoring"	494	40,229
Healthcare Diagnostics	"artificial intelligence" + "healthcare" + "diagnostics"	535	39,273
Customer Insights	"artificial intelligence" + "customer insight"	492	12,096

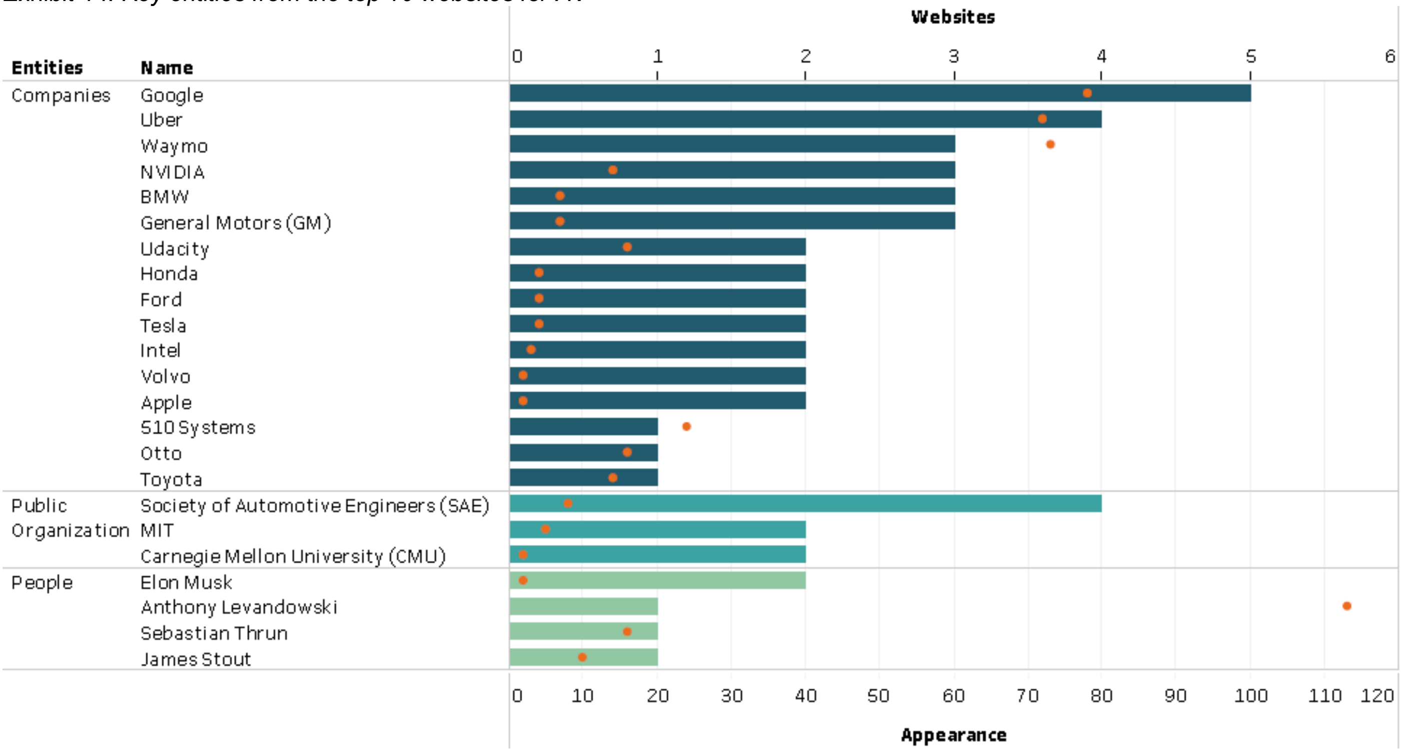
∗ *The output is as of March 30th, 2018.*

The results also show the most popular websites and key entities (i.e. names of companies, public organizations, and people) for each application.[238] Exhibits 13 and 14 display the top ten websites and popular entities for AV. In the case of AVs, the public is more interested in specific companies than individuals in this field. In addition, the public is more interested in tech companies like Google, Waymo, Uber, Udacity and NVIDIA versus traditional automobile companies, like BMW, Honda, GM, Ford, Volvo, and Toyota. Carnegie Mellon University (CMU) and MIT, which have strong AI research programs, also appeared in the top ten search.

Exhibit 13. Top 10 websites for AV

Title	Publisher	Publish Date	Total Engagement
Nanodegree Program: Complete your journey to a Self-Driving Car career	Udacity	09/19/17	16,002
A Single Autonomous Car Has a Huge Impact on Alleviating Traffic	MIT Technology Review	05/10/17	5,211
God is a bot, and Anthony Levandowski is his messenger	WIRED	09/27/17	4,135
National Transport Commission Says People in Autonomous Cars Should be Exempt From DUI Laws	Futurism	10/05/17	3,901
Inside Waymo's Secret World for Training Self-Driving Cars	The Atlantic	08/23/17	2,826
What would the average human do?	The Outline	10/16/17	1,854
Toyota Says They Will Have Intelligent Talking Cars by 2020	Futurism	10/19/17	1,592
NVIDIA CEO Says We're 4 Years Away From Fully Autonomous Cars	Futurism	10/27/17	1,517
Twelve things you need to know about driverless cars	The Guardian	01/15/17	1,500
Autonomous Vehicles: Are You Ready for the New Ride?	MIT Technology Review	11/09/17	1,424

Exhibit 14. Key entities from the top 10 websites for AV



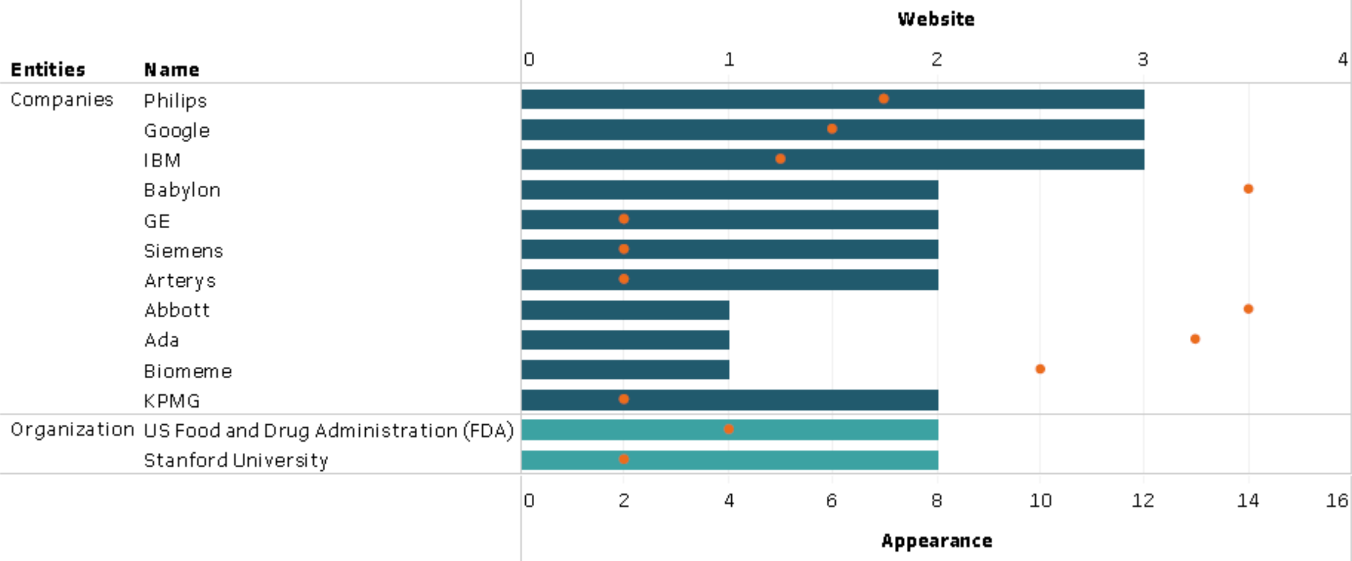
∗ *The numbers without parentheses in the Count section means the number of website that the entity appeared in the top 10 websites, while the numbers with parentheses means the total number of the entity appeared in the top 10 websites.*

Like AV, the public showed more interest in companies over individuals for healthcare (Exhibit 15 and 16). They also displayed more interested in startups, such as Babylon, Arterys, Biomeme, and Ada versus traditional healthcare companies.

Exhibit 15. Top 10 websites for Healthcare

Title	**Publisher**	**Publish Date**	**Total Engagement**
Ada [Homepage]	Ada	03/13/17	4,988
If you're not a white male, artificial intelligence's use in healthcare could be dangerous	Quartz	07/10/17	3,374
Artificial Intelligence is Completely Transforming Modern Healthcare	Futurism	04/03/17	2,785
Game-Changing Technology is Revolutionizing Medical Diagnostics	Bloomberg	10/19/17	2,528
Artificial Intelligence & Real World Data: The Next Steps In Your Big Data Journey	Bio.IT World	11/08/17	1,687
A digital revolution in health care is speeding up	The Economist	03/02/17	1,620
AI 100: The Artificial Intelligence Startups Redefining Industries	CB Insights	12/12/17	1,233
The Future of Radiology and Artificial Intelligence	Medical Futurist	06/29/17	1,063
The rise of artificial intelligence means doctors must redefine what they do	STAT	10/16/17	877
How smartphones are transforming healthcare	Financial Times	01/12/17	857

Exhibit 16. Key entities from the top 10 websites for Healthcare



ENDNOTES

[1] Peha, J., “Bridging the Divide between Technologists and Policy Makers,” IEEE Spectrum, March 2001, https://users.ece.cmu.edu/~peha/bridging_divide.pdf

[2] “A Future That Works: Automation, Employment and Productivity,” McKinsey Global Institute, January 2017, https://www.mckinsey.com/~/media/McKinsey/Global%20Themes/Digital%20Disruption/Harnessing%20automation%20for%20a%20future%20that%20works/MGI-A-future-that-works-Executive-summary.ashx

[3] Tratica data from “The True Business Impact of AI,” AI Business, 2017, https://s3.amazonaws.com/big-data-tokyo/Pitchford-AI-Business-BDAT-2017-02_and_Wheelock-Tractica-BDAT-2017-02.pdf

[4] “Cumulative Revenue of Top 10 Use Cases/Segments of Artificial Intelligence (AI) Market Worldwide, Between 2016-2025,” Statista, https://www.statista.com/statistics/607835/worldwide-artificial-intelligence-market-leading-use-cases/

[5] “Sizing the Prize: What’s the Real Value of AI for Your Business and How Can You Capitalise?,” PricewaterhouseCoopers, https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

[6] "Automated Vehicles," NHTSA, https://one.nhtsa.gov/Research/Crash-Avoidance/Automated-Vehicles.

[7] Ibid.

[8] "Transparency of Autonomous Systems," IEE Standards Association.. https://standards.ieee.org/develop/project/7001.html

[9] Kristen Lee, "Toyota Won't Make A Self-Driving Car Until It's 100 Percent Safe," last modified October 11, 2017. https://jalopnik.com/toyota-wont-make-a-self-driving-car-until-its-100-perce-1820326849

[10] Gene Munster, "Here’s When Having a Self-Driving Car Will Be a Normal Thing," Fortune, last modified September 13, 2017. http://fortune.com/2017/09/13/gm-cruise-self-driving-driverless-autonomous-cars/

[11] Nikolaus Lang et al, "Making Autonomous Vehicles a Reality: Mobility in 21st-Century,” last modified October 17, 2017. https://www.bcg.com/publications/2017/automotive-making-autonomous-vehicles-a-reality.aspx

[12] “Accenture Mobility,” Accenture Digital. https://www.accenture.com/t20170720T104429Z__w__/us-en/_acnmedia/PDF-55/Accenture-Insight-Mobility-IoT-Autonomous-Vehicles.pdf

[13] Tobias Holstein, Gordana Dodig-Crnkovic, and Patrizio Pelliccione. "Ethical and Social Aspects of Self-Driving Cars," arXiv:1802.04103v1 [cs.CY] 5 Feb 2018. https://arxiv.org/pdf/1802.04103.pdf

[14]Fred Lambert, "Elon Musk says preventing a ‘fleet-wide hack’ is Tesla’s top security priority," Electrek, last modified July 17, 2017. https://electrek.co/2017/07/17/tesla-fleet-hack-elon-musk/

[15] Tobias Holstein, Gordana Dodig-Crnkovic, and Patrizio Pelliccione. "Ethical and Social Aspects of Self-Driving Cars," arXiv:1802.04103v1 [cs.CY] 5 Feb 2018. https://arxiv.org/pdf/1802.04103.pdf

[16] Stepp, E, “Americans Feel Unsafe Sharing the Road with Fully Self-Driving Cars.”, AAA Newsroom, 7th March 2017, http://go.nature.com/2i296OW

[17]“Autonomous-vehicle technology is advancing ever faster”, The Economist, 1st March 2018, https://www.economist.com/news/special-report/21737420-making-vehicles-drive-themselves-hard-getting-easier-autonomous-vehicle-technology

[18] Shariff, A., Bonnefon. J, Rahwan, I, “Psychological roadblocks to the adoption of self-driving vehicles”, Nature Human Behavior, Vol 1. Macmillan Publishers Limited. 2017.

[19] Holstein, T, “The Misconception of Ethical Dilemmas in Self Driving Cars,” Proceedings 2017, 1, 174; doi:10.3390/IS4SI-2017-04026.

[20] Brooks, R, “Unexpected Consequences of Self Driving Cars,” 12th Jan 2017, http://rodneybrooks.com/unexpected-consequences-of-self-driving-cars/

[21] Ibid.

[22] Stepp, E, “Americans Feel Unsafe Sharing the Road with Fully Self-Driving Vehicles,” AAA Newsroom, 7th March 2017, http://go.nature.com/2i296OW

[23] Greenberg, A, “Hackers remotely kill a jeep on the highway - with me in it,” 21st July 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[24]Towes, R., “The biggest threat facing connected autonomous vehicles is cybersecurity,” Techcrunch.com, 25th Aug 2016, https://techcrunch.com/2016/08/25/the-biggest-threat-facing-connected-autonomous-vehicles-is-cybersecurity/

[25] In 2014

[26] Abel, R., “Auto-ISAC release automotive cybersecurity best practices,” SC Magazine, 22nd July 2016, https://www.scmagazine.com/auto-industry-experts-develop-best-practices-for-securing-connected-vehicles/article/529888/

[27] “Autonomous vehicle technology is advancing ever faster,” The Economist, 1st Mar 2018, https://www.economist.com/news/special-report/21737420-making-vehicles-drive-themselves-hard-getting-easier-autonomous-vehicle-technology

[28] Quote from Christophe Sapet of Navya, a maker of driverless shuttles. “Autonomous vehicle technology is advancing ever faster,” The Economist, 1st Mar 2018, https://www.economist.com/news/special-report/21737420-making-vehicles-drive-themselves-hard-getting-easier-autonomous-vehicle-technology

[29] Brandon Schoettle and Michael Sivak,“Public Opinion about Self-Driving Vehicles in China, India, Japan, the US, the UK and Australia,” https://deepblue.lib.umich.edu/bitstream/handle/2027.42/109433/103139.pdf.

[30] Ibid.

[31] Ibid.

[32] Based on interviews with the Automobile Division at the Japanese Ministry of Economy, Trade and Industry (METI), conducted 3rd March 2018.

[33] Ibid.

[34] “What’s Ahead for Fully Autonomous Driving, Consumer Opinions on Advanced Vehicle Technology”, Deloitte Development LLC, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manufacturing-consumer-opinions-on-advanced-vehicle-technology.pdf.

[35] Bradbury D., “How to hack a jeep cherokee - but don’t try this at home kids,” Naked Security by Sophos, 10th May 2017, https://nakedsecurity.sophos.com/2017/05/10/how-to-hack-a-jeep-cherokee-but-dont-try-this-at-home-kids/

[36] “Fiat Chrysler recalls 1.4 million US vehicles to prevent hacking after researchers remotely ‘killed’ cars,” ABC News, 24th Jul 2015, http://www.abc.net.au/news/2015-07-25/fiat-chrysler-recalls-united-states-vehicles-to-prevent-hacking/6647624

[37] Automotive Information Sharing and Analysis Center, Auto-ISAC, https://www.automotiveisac.com/best-practices/

[38] “Cybersecurity”, Auto Alliance, https://autoalliance.org/connected-cars/cybersecurity/

[39] Conger, K., “We need to be okay with self driving cars that crash, researchers say,” Gizmodo, 7th Nov 2017, https://gizmodo.com/we-need-to-be-okay-with-self-driving-cars-that-crash-r-1820205503

[40] Boudette, N., “Autopilot Cited in Death of Chinese Tesla Driver”, NYTimes, 14th Sept 2016, https://www.nytimes.com/2016/09/15/business/fatal-tesla-crash-in-china-involved-autopilot-government-tv-says.html

[41] Jeruld Weiland, and Allison Crow. "How Safe Are Self-Driving Cars?," HuffPost, last modified May 2, 2017. https://www.huffingtonpost.com/entry/how-safe-are-self-driving-cars_us_5908ba48e4b03b105b44bc6b

[42] Tobias Holstein, Gordana Dodig-Crnkovic, and Patrizio Pelliccione. "Ethical and Social Aspects of Self-Driving Cars," arXiv:1802.04103v1 [cs.CY] 5 Feb 2018. https://arxiv.org/pdf/1802.04103.pdf

[43] Mark Schaub, "Cybersecurity: Achilles’ Heel for Self-driving Cars?," China Law Insight, last modified February 9, 2018. https://www.chinalawinsight.com/2018/02/articles/corporate/cybersecurity-achilles-heel-for-self-driving-cars/

[44] Ibid.

[45] Tobias Holstein, Gordana Dodig-Crnkovic, and Patrizio Pelliccione. "Ethical and Social Aspects of Self-Driving Cars," arXiv:1802.04103v1 [cs.CY] 5 Feb 2018. https://arxiv.org/pdf/1802.04103.pdf

[46] Darrell M. West, "Moving forward: Self-driving vehicles in China, Europe, Japan, Korea, and the United States," Center for Technology Innovation at Brookings, September 2016. https://www.brookings.edu/wp-content/uploads/2016/09/driverless-cars-3-ed.pdf

[47] "Automated Driving Systems 2.0: A Vision For Safety," NHTSA, accessed April 6, 2018. https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[48] Ibid.

[49] "US DOT releases new Automated Driving Systems guidance," NHTSA. https://www.nhtsa.gov/press-releases/us-dot-releases-new-automated-driving-systems-guidance

[50]"Autonomous Vehicles: Self-driving Vehicles Enacted Legislation," NCSL. http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[51] "A Global Race For Autonomous Vehicles: Views From The United States, Europe, And Asia," FTI Consulting. https://fticommunications.com/2017/06/global-race-autonomous-vehicles-views-united-states-europe-asia/

[52] Press Release, “Federal Government adopts action plan on automated driving,” Federal Ministry of Transport and Digital Infrastructure, 28th Aug 2018, http://www.bmvi.de/SharedDocs/EN/PressRelease/2017/128-dobrindt-federal-government-action-plan-automated-driving.html

[53] Ethics Commission, “Automated and Connected Driving”, Federal Ministry of Transport and Digital Infrastructure, June 2017, http://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission.pdf?__blob=publicationFile

[54] “Autonomous Vehicles Readiness Index”, KPMG, January 2018, https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/01/avri.pdf

[55] Ibid.

[56] Ibid.

[57] Ibid.

[58] Dai, S., “China formulates new policies for autonomous cars in bid to catch up to US”, South China Morning Post, 8th Feb 2018, http://www.scmp.com/tech/start-ups/article/2132591/china-formulates-new-policies-autonomous-cars-bid-catch-us

[59] “China completes first draft of national rules to allow road tests for driverless vehicles,” The Straits Times, 23rd Jan 2018, http://www.straitstimes.com/asia/east-asia/china-completes-first-draft-of-national-rules-to-allow-road-tests-for-driverless

[60] Jiji, “Japan sets approval criteria for driverless vehicle road tests,“ The Japan Times, 1st Jun 2017, https://www.japantimes.co.jp/news/2017/06/01/business/japan-sets-approval-criteria-driverless-vehicle-road-tests/#.WrpFC4jwZPY

[61] Based on interviews with the Automobile Division at the Japanese Ministry of Economy, Trade and Industry (METI), conducted 3rd March 2018.

[62] Vincent Boulanin and Maaike Verbruggen, “Mapping the Development of Autonomy in Weapon Systems,” Stockholm International Peace Research Institute, November 2017, https://www.sipri.org/sites/default/files/2017-11/siprireport_mapping_the_development_of_autonomy_in_weapon_systems_1117_0.pdf

[63] “Directive 3000.09: Autonomy in Weapon Systems,” US Department of Defense, November 21, 2012, http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf

[64] Ibid.

[65] Vincent Boulanin and Maaike Verbruggen

[66] Lucien Crowder, “Don’t Fear the Robopocalypse: Autonomous Weapons Expert Paul Scharre,” Bulletin of the Atomic Scientists, January 10, 2018, https://thebulletin.org/don’t-fear-robopocalypse-autonomous-weapons-expert-paul-scharre11423

[67] Boulanin and Verbruggen, 62.

[68] Ibid.

[69] Gary E. Marchant, et al. “International Governance of Autonomous Military Robots,” The Columbia Science and Technology Law Review 12 (2011).

[70] Ronald C. Arkin, “Warfighting Robots Could Reduce Civilian Casualties, So Calling for a Ban Now is Premature,” IEEE Spectrum, August, 5, 2015, https://spectrum.ieee.org/automaton/robotics/artificial-intelligence/autonomous-robotic-weapons-could-reduce-civilian-casualtie

[71] Ibid.

[72] Paul Schare, “Autonomous Weapons and Operational Risk,” Center for a New American Security, February 29, 2016, https://www.cnas.org/publications/reports/autonomous-weapons-and-operational-risk

[73] Ibid.

[74] Boulanin and Verbruggen, 65.

[75] Noel E. Sharkey, “The Evitability of Autonomous Robot Warfare,” International Review of the Red Cross, 94, No. 886 (2012): 788-789

[76] Marchant, et al., 285.

[77] Autonomous Weapons: An Open Letter From AI & Robotics Researchers,” Future of Life Institute, July 28, 2015, https://futureoflife.org/open-letter-autonomous-weapons/

[78] Ibid.

[79] “Autonomous Weapons and Operational Risk”, 10.

[80] Ibid.

[81] “Directive 3000.09: Autonomy in Weapons Systems”

[82] “Joint Doctrine Publication 0-30.2: Unmanned Aircraft Systems,” UK Ministry of Defense, August 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/673940/doctrine_uk_uas_jdp_0_30_2.pdf

[83] “Japan’s Views on Issues Relating to LAWS,” The United Nations Office of Geneva, 2016, https://www.unog.ch/80256EDD006B8954/(httpAssets)/4E8371EAD5E34263C1257F8C00289B5E/$file/2016_LAWS+MX_CountryPaper+Japan.pdf

[84] “Autonomous Weapons and Operational Risk,” 5.

[85] “Autonomous Weapons and Operational Risk”

[86] Paul Scharre, “Why You Shouldn’t Fear Slaughterbots,” IEEE Spectrum, December 22, 2017, https://spectrum.ieee.org/automaton/robotics/military-robots/why-you-shouldnt-fear-slaughterbots

[87] Ibid.

[88] “Autonomous Weapons and Operational Risk”

[89] Ibid

[90] Ibid, 31.

[91] Ibid.

[92] “Report of the Defense Science Board Task Force on Patriot System Performance,” Office of the US Under Secretary of Defense, January 2005, https://www.acq.osd.mil/dsb/reports/2000s/ADA435837.pdf

[93] John K. Hawley, “Patriot Wars: Automation and the Patriot Air and Missile Defense System,” Center for a New American Security, January 2017, https://www.cnas.org/publications/reports/patriot-wars

[94] “Autonomous Weapons and Operational Risk”

[95] Ibid, 25.

[96] Ibid, 33.

[97] “Directive 3000.09: Autonomy in Weapons Systems”

[98] “Joint Doctrine Publication 0-30.2: Unmanned Aircraft Systems”

[99] “Resolution on the Use of Armed Drones,” European Parliament, February 2014, www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session25/.../A-HRC-25-59.doc

[100] “Japan’s Views on Issues Relating to LAWS”

[101] Bedavyasa Mohanty, “Lethal Autonomous Dragon: China’s Approach to Artificial Intelligence Weapons,” Observer Research Foundation, November 15, 2017 http://www.orfonline.org/expert-speaks/lethal-autonomous-weapons-dragon-china-approach-artificial-intelligence/

[102] “Report on Activities,” Campaign to Stop Killer Robots, November 2017, https://www.stopkillerrobots.org/wp-content/uploads/2018/02/CCW_Report_Nov2017_posted.pdf

[103] Ray Acheson, “Losing Control: The Challenge of Autonomous Weapons for Laws, Ethics and Humanity,” CCW 5, No. 3 (2017): 1, http://www.reachingcriticalwill.org/disarmament-fora/ccw/2017/laws/ccwreport/12166-ccw-report-vol-5-no-3

[104] Kenneth Anderson and Matthew Waxman, “Law and Ethics for Autonomous Weapon Systems: Why a Ban Won’t Work and How the Laws of War Can,” Hoover Institution - Stanford University, March 2013,

[105] Ronald C. Arkin et. al, “An Ethical Governor for Constraining Lethal Action in an Autonomous System,” Georgia Institute of Technology, 2009, https://www.cc.gatech.edu/ai/robot-lab/online-publications/GIT-GVU-09-02.pdf

[106] "What Are Consumer Insights and How Do They Impact Marketing Effectiveness?," HuffPost, last modified December 2, 2014, https://www.huffingtonpost.com/jure-klepic/what-are-consumer-insight_b_5906624.html.

[107] "How Can Analytics and AI Allow Marketers to Predict the Future?," ClickZ, last modified August 2, 2017, https://www.clickz.com/how-can-ai-allow-marketers-to-predict-the-future/112268/.

108 Charles DuHigg, “How Companies Learn Your Secrets,” New York Times ,https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

109 "Artificial intelligence: Touchpoints with consumers," PwC, last modified 2018, https://www.pwc.com/gx/en/retail-consumer/assets/artificial-intelligence-global-consumer-insights-survey.pdf.

110 "Almost a Third of Consumers Plan for New AI Home Devices," PwC Press Room, March 13, 2018, https://press.pwc.com/News-releases/almost-a-third-of-consumers-plan-for-new-ai-home-devices/s/3340cc8a-75e9-44f8-8db4-f39cff1b52d1.

111 Rupa Ganatra, "Is Artificial Intelligence In Marketing Overhyped?" Forbes, March 4, 2018, https://www.forbes.com/sites/rganatra/2018/03/04/is-artificial-intelligence-in-marketing-overhyped/#53da8ba06681.

112 Ibid.

113 Ibid.

114 Ibid.

115 "CEO Message." Fast Retailing. February 28, 2018. http://www.fastretailing.com/eng/ir/direction/message.html.

116"Lawson Unveils Facility to Test Next-generation Convenience Store Tech Using IT, AI." The Mainichi. December 06, 2017.
https://mainichi.jp/english/articles/20171206/p2a/00m/0na/004000c.
https://mainichi.jp/english/articles/20171206/p2a/00m/0na/004000c

117"Lawson Unveils Facility to Test Next-generation Convenience Store Tech Using IT, AI." The Mainichi. December 06, 2017.
https://mainichi.jp/english/articles/20171206/p2a/00m/0na/004000c.
https://mainichi.jp/english/articles/20171206/p2a/00m/0na/004000c

118 "How Germany's Otto Uses Artificial Intelligence." The Economist. April 12, 2017. https://www.economist.com/news/business/21720675-firm-using-algorithm-designed-cern-laboratory-how-germanys-otto-uses.

119 David Simchi-Levi, "The New Frontier of Price Optimization," MIT Sloan Management Review, September 7, 2017, https://sloanreview.mit.edu/article/the-new-frontier-of-price-optimization/.

120 Ibid.

121 Rupa Ganatra, "Is Artificial Intelligence In Marketing Overhyped?" Forbes, https://www.forbes.com/sites/rganatra/2018/03/04/is-artificial-intelligence-in-marketing-overhyped/#3b8b0f1a6681.

122 “Customer Data Meets AI,” MIT Technology Review, https://www.technologyreview.com/s/608294/customer-data-meets-ai/.

123 "Consumers Want Privacy, Better Data Protection from Artificial Intelligence, Finds New Genpact Research." PR Newswire. December 06, 2017.
https://www.prnewswire.com/news-releases/consumers-want-privacy-better-data-protection-from-artificial-intelligence-finds-new-genpact-research-300567120.html.

124 Ibid.

125 "Big Data: Seizing Opportunities, Preserving Values." The White House: President Barack Obama. May 2014.
https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

126 Stephen Gardner, "Artificial Intelligence Poses Data Privacy Challenges," Bloomberg Law, October 26, 2016, https://www.bna.com/artificial-intelligence-poses-n57982079158/.

127 Ibid.

128 Jack Neff and Jack Neff, "Macy's: Marketers Should Defend Data Use But Show Restraint," Ad Age, September 12, 2013, http://adage.com/article/datadriven-marketing/macy-s-marketers-speak-data-benefits/244107/.

129 "Big Data: Seizing Opportunities, Preserving Values." The White House: President Barack Obama. May 2014.
https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

130 Gardner, "Artificial Intelligence Poses Data Privacy Challenges."

131 Ibid.

132 Frank Buytendijk, “Confronting the privacy and ethical risks of Big Data,” Financial Times, https://www.ft.com/content/105e30a4-2549-11e3-b349-00144feab7de.

133 “IBM Cybersecurity and Privacy Research,” The Harris Poll, http://newsroom.ibm.com/download/IBM+Cybersecurity+PR+Research+-+Final.pdf.

134 Ibid.

135 Ibid.

136 "IBM Security: Future of Identity Report," IBM, January 2018, https://www-03.ibm.com/press/us/en/pressrelease/53646.wss#_ftn1.

137 Ibid.

138 Frank Buytendijk and Jay Heiser, "Confronting the Privacy and Ethical Risks of Big Data," Financial Times, accessed February 13, 2018, https://www.ft.com/content/105e30a4-2549-11e3-b349-00144feab7de.

139 "Artificial intelligence: Touchpoints with consumers."

140 Jess Nelson, "Too Much Personalization Turns Off Consumers, Study Finds," Media Post, September 23, 2017, https://www.mediapost.com/publications/article/307730/too-much-personalization-turns-off-consumers-stud.html.

141 Anita Ramasastry, "Web Sites Change Prices Based on Customers' Habits," CNN, June 24, 2005, http://edition.cnn.com/2005/LAW/06/24/ramasastry.website.prices/.

142 "Bezos Calls Amazon Experiment 'a Mistake'," Business Journals, September 28, 2000, https://www.bizjournals.com/seattle/stories/2000/09/25/daily21.html.

143 Ibid.

144 Adam Tanner, "Different Customers, Different Prices, Thanks To Big Data," Forbes, June 27, 2014, https://www.forbes.com/sites/adamtanner/2014/03/26/different-customers-different-prices-thanks-to-big-data/#23c3ab165730.

[145] Matt Pierce, "OfficeMax Executive Apologizes over 'daughter Killed' Mailer," Los Angeles Times, January 20, 2014, http://www.latimes.com/nation/la-na-officemax-mess-20140121-story.html.

[146] Ibid.

[147] Ibid.

[148] Robin Roberts, "US and EU Retailers Agree on Common Approach to New Data Regulations," National Retail Federation, October 09, 2017, , accessed April 13, 2018, https://nrf.com/media/press-releases/us-and-eu-retailers-agree-common-approach-new-data-regulations.

[149] Ben Sillitoe, "GDPR: The Threats and Opportunities for Retailers," Essential Retail, July 20, 2017, https://www.essentialretail.com/analysis/gdpr-threats-and-opportunities.

[150] "Law in the United States," DLA Piper Global Data Protection Laws of the World, July 25, 2017, https://www.dlapiperdataprotection.com/index.html?t=law&c=US.

[151] Ibid.

[152] "Law in the Japan," DLA Piper Global Data Protection Laws of the World, July 25, 2017 ,https://www.dlapiperdataprotection.com/index.html?t=law&c=J.

[153] Ibid.

[154] "Law in China," DLA Piper Global Data Protection Laws of the World, July 25, 2017, https://www.dlapiperdataprotection.com/index.html?t=law&c=CN.

[155] Ibid.

[156] “Ghosts in the machine: Artificial intelligence, risks and regulation in financial markets,” Euromoney, http://www.euromoneythoughtleadership.com/ghostsinthemachine/

[157] “Data Point: Credit Invisibles,” Consumer Financial Protection Bureu, 2015, https://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf

[158] “How to Build Credit Risk Models Using AI and Machine Learning,” FICO, http://www.fico.com/en/blogs/analytics-optimization/how-to-build-credit-risk-models-using-ai-and-machine-learning/

[159] “Safely grow your lending business,” ZestFinance, https://www.zestfinance.com/hubfs/Site%20updates%20Apr_2017/increase_approval_rates_case_study_2017.03.04.pdf?t=1522954270346

[160] Rebecca Feng, “Chinese Fintechs Use Big Data To Give Credit Scores To The 'Unscorable',” Forbes, 2017, https://www.forbes.com/sites/rebeccafeng/2017/07/25/chinese-fintechs-use-big-data-to-give-credit-scores-to-the-unscorable/#1e704dfd410a

[161] Chi Chi Wu, “Credit Invisibility and Alternative Data: The Devil is in the Details,” National Consumer Law Center, 2015, https://www.nclc.org/images/pdf/credit_reports/ib-credit-invisible-june2015.pdf

[162] “Technology and innovation in the insurance sector,” OECD, 2017, https://www.oecd.org/finance/Technology-and-innovation-in-the-insurance-sector.pdf

[163] Algorithm Watch, https://algorithmwatch.org/en/openschufa-shedding-light-on-germanys-opaque-credit-scoring/

[164] “How does scoring work at SCHUFA?,” Schufa, https://www.schufa.de/de/ueber-uns/daten-scoring/scoring/scoring-schufa/

[165] Spiegel Online, “German Agency to Mine Facebook to Assess Creditworthiness,” 2017, http://www.spiegel.de/international/germany/german-credit-agency-plans-to-analyze-individual-facebook-pages-a-837539.html

[166] Sophie Duvernoy, “German credit agency plan stirs ‘Big Brother’ fear,” Reuters, 2012, https://www.reuters.com/article/germany-privacy/german-credit-agency-plan-stirs-big-brother-fear-idUSL5E8H75CP20120607

[167] Pam Dixon, and Bob Gellman, “The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future,” World Privacy Forum, 2014, https://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/

[168] “Ghosts in the machine: Artificial intelligence, risks and regulation in financial markets,” Euromoney, http://www.euromoneythoughtleadership.com/ghostsinthemachine/

[169] Danielle Keats Citron, and Frank Pasquale, “The Scored Society: Due Process for Automated Predictions,” Washington Law Review, Vol. 89:1 (2014), https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1318/89WLR0001.pdf?sequence=1

[170] “Safely grow your lending business,” ZestFinance, https://www.zestfinance.com/hubfs/Site%20updates%20Apr_2017/increase_approval_rates_case_study_2017.03.04.pdf?t=1522954270346

[171] “Transparent scoring method,” Schufa, https://www.schufa.de/de/ueber-uns/daten-scoring/scoring/transparente-scoreverfahren/

[172] “The Truth About Car Insurance,” Consumer Report, https://www.consumerreports.org/cro/car-insurance/auto-insurance-special-report1/index.htm

[173] Jay Budzik, “Explainable Machine Learning in Credit,” ZestFinance, https://www.zestfinance.com/hubfs/Underwriting/Explainable-Machine-Learning-in-Credit.pdf

[174] “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” OECD, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[175] “Directive 95/46/EC of The European Parliament and of The Council,” EUR-Lex, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046

[176] “Regulation (EU) 2016/679 of The European Parliament and of The Council,” EUR-Lex http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[177] “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,” Article 29 Data Protection Working Party

[178] “How to comply with GDPR Article 22? Automated credit decisions,” http://www.reubenbinns.com/blog/how-to-comply-with-gdpr-article-22-automated-credit-decisions/

[179] “Act on the Protection of Personal Information,” http://www.japaneselawtranslation.go.jp/law/detail_main?id=130

[180] “Mizuho, SoftBank tap AI for consumer loan screening,” Nikkei Asian Review, 2017, https://asia.nikkei.com/Business/Mizuho-SoftBank-tap-AI-for-consumer-loan-screening

[181] Sara Xia, “China’s Personal Information Security Specification: Get Ready for May 1,” 2018 ,https://www.chinalawblog.com/2018/02/chinas-personal-information-security-specification-get-ready-for-may-1.html

[182] Samm Sacks, “China’s Emerging Data Privacy System and GDPR,” Center for Strategic & International Studies, 2018 ,https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr

[183] Lea Nonninger, “Here's why China is concerned about Tencent and Alibaba's credit scoring efforts,” Business Insider, 2018, http://www.businessinsider.com/china-tencent-and-alibabas-new-credit-scoring-solution-2018-2

[184] “Fair Credit Reporting Act,” https://www.ftc.gov/system/files/fcra_2016.pdf

[185] “Big Data: A Tool for Inclusion or Exclusion?,” Federal Trade Commision, 2016, https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

[186] Mikella Hurley, and Julius Adebayo, “Credit Scoring in The Era of Big Data,” Yale Journal of Law and Technology, Vol. 18:1 (2016), http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1122&context=yjolt

[187] Mikella Hurley, and Julius Adebayo, “Credit Scoring in The Era of Big Data,” Yale Journal of Law and Technology, Vol. 18:1 (2016), http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1122&context=yjolt

[188] Matthew Collier et al., “Artificial Intelligence (AI): Healthcare’s New Nervous System.” Accenture, 2017, https://www.accenture.com/us-en/insight-artificial-intelligence-healthcare.

[189] Nicole Kobie, “AI Has No Place in the NHS if Patient Privacy Isn’t Assured,” Wired UK, 28 Sep. 2017, http://www.wired.co.uk/article/ai-healthcare-gp-deepmind-privacy-problems.

[190] Ibid.

[191] Ibid.

[192] Shailin Thomas, “Artificial Intelligence and Medical Liability,” Harvard Law Petrie-Flom Center, 10 Feb. 2017, http://blogs.harvard.edu/billofhealth/2017/02/10/artificial-intelligence-and-medical-liability-part-ii/.

[193] Matthew Collier et al., “Artificial Intelligence (AI): Healthcare’s New Nervous System.” Accenture, 2017, https://www.accenture.com/us-en/insight-artificial-intelligence-healthcare.

[194] Peter Blackburn, “Artificial Intelligence Will Be Adopted, Says NHS England.” British Medical Association, 14 Sep. 2017, https://www.bma.org.uk/news/2017/september/artificial-intelligence-will-be-adopted-says-nhs-england.

[195] Hadley Gamble and Matt Clinch, “Bill Gates Says Technology Could ‘Accentuate’ The Gap Between The Rich and Poor.” CNBC News, 14 Nov. 2017, https://www.cnbc.com/2017/11/14/bill-gates-defends-the-rise-of-the-robots.html.

[196] Jon Sharman, “AI Could Have ‘Immense’ Benefits for NHS, Says Tech Committee Chair.” The Independent, 11 Jan. 2018, http://www.independent.co.uk/news/health/ai-nhs-benefits-artificial-intelligence-chair-norman-lamb-reform-a8152651.html

[197] Mariya Yao, “US Falls Behind China & Canada In Advancing Healthcare With A.I.” Forbes, 1 June 2017, https://www.forbes.com/sites/mariyayao/2017/06/01/u-s-falls-behind-china-canada-in-advancing-healthcare-with-a-i/#7780d000206a

[198] Dean Arnold and Tim Wilson, “ What Doctor?: Why AI and Robotics will Define New Health.” PWC, 2017, https://www.pwc.com/gx/en/industries/healthcare/publications/ai-robotics-new-health/data-explorer.html#!/P/29/bars?cut=Territory&Tecf=2,12.

[199] PWC Germany, “Sherlock in Health: How Artificial Intelligence May Improve Quality and Efficiency, Whilst Reducing Healthcare Costs in Europe.” PWC, 17 June 2017, https://www.pwc.de/de/gesundheitswesen-und-pharma/studie-sherlock-in-health.pdf.

[200] Christina Farr, “Eric Schmidt Says A.I. Won’t Replace Your Doctor.” CNBC News, 6 March 2018, https://www.cnbc.com/2018/03/06/eric-schmidt-says-ai-wont-replace-your-doctor.html.

[201] Cai Yewen, “Could AI Be the Cure for China’s Medical Crisis?” Sixth Tone, 26 Dec. 2017, http://www.sixthtone.com/news/1001462/could-ai-be-the-cure-for-chinas-medical-crisis%3F.

[202] Angus Chen, “Like It Or Not, Personal Health Technology Is Getting Smarter Listen· 3:05 .” NPR, 5 March 2018, https://www.npr.org/sections/health-shots/2018/03/05/588914818/personal-tech-devices-are-still-learning-how-to-improve-health.

[203] Ibid.

[204] Ibid.

[205] Luke Oakden-Raynor, “Artificial Intelligence Won’t Replace Doctors Soon but it can Help with Diagnosis.” ABC Australia, 19 Sep. 2017, http://www.abc.net.au/news/2017-09- 19/ai-wont-replace-doctors- soon-but- it-can- help-diagnosis/8960530.

[206]Matt O’Connor, “AI Expert: Marriage of Machine Learning, Radiology May Turn Out Different Than You Think.” Health Imaging, 23 Feb. 2018, http://www.healthimaging.com/topics/artificial-intelligence/ai-expert-marriage-machine-learning-radiology-may-turn-out-different.

[207] Ibid.

[208] Jonathan Bush, “How AI is Taking the Scut Work out of Health Care.” Harvard Business School, 5 March 2018, https://hbr.org/2018/03/how-ai-is-taking-the-scut-work-out-of-health-care.

Review, 5 March 2018

care.

[209] Robert Hart, “If You’re Not a White Male, Artificial Intelligence’s Use in Healthcare Could beDangerous.” Quartz, 10 July 2017, https://qz.com/1023448/if-youre- not-a- white-male- artificial-intelligences-use- in-healthcare- could-be- dangerous/.

[210] Reed Abelson and Matthew Goldstein, “Millions of Anthem Customers Targeted in Cyberattack,” The New York Times, 5 February 2015, https://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html

[211] James Vincent, “ Google’s DeepMind made ‘inexcusable’ errors handling UK health data, says report,” The Verge, 16 May 2017 https://www.theverge.com/2017/3/16/14932764/deepmind-google-uk-nhs-health-data-analysis

[212] Elizabeth Denham,"Undertaking Cover Letter," Information Commissioner's Office, 3 July 2017, https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf

[213] Elizabeth Denham,"Undertaking Cover Letter," Information Commissioner's Office, 3 July 2017, https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf; and Dominic King, "Why doesn't Streams use AI?," DeepMind Health, https://deepmind.com/blog/streams-and-ai/. Importantly, the Streams app does not contain any AI components (yet).

[214] Julia Powles and Hal Hodson, "Google DeepMind and healthcare an age of alogorithms," Health and Technology, 16 March 2017, https://link.springer.com/content/pdf/10.1007%2Fs12553-017-0179-1.pdf and Elizabeth Denham,"Undertaking Cover Letter," Information Commissioner's Office, 3 July 2017, https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf

[215] Elizabeth Denham,"Undertaking Cover Letter," Information Commissioner's Office, 3 July 2017, https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf

[216] Dr. Margaret Chan, "Opening Remarks at the Artificial Intelligence for Good Global Summit," The World Health Organization, 7 June 2017, http://www.who.int/dg/speeches/2017/artificial-intelligence-summit/en/.

[217] Cécile Huet, "European Commission's Initiatives in Artificial Intelligence," European Commission, 2017, http://www.oecd.org/going-digital/ai-intelligent-machines-smart-policies/conference-agenda/ai-intelligent-machines-smart-policies-huet.pdf.

[218] Ibid.

[219] Ibid.

[220] Rand Hindi, "Will Artificial Intelligence Be Illegal In Europe Next Year," Entrepreneur, 9 Aug. 2017, https://www.entrepreneur.com/article/298394.

[221] Megan Molteni, "Medicine is Going Digital. The FDA is Racing to Catch Up," Wired, 22 May 2017, https://www.wired.com/2017/05/medicine-going-digital-fda-racing-catch/.

[222] Ibid.

[223] Columbia Lab Interview

[224] Teresa Zayas Caban et al., "Hype to Reality: How Artificial Intelligence (AI) Can Transform Health and Healthcare," Office of the National Coordinator for Health Information Technology, 17 Jan. 2018, https://www.healthit.gov/buzz-blog/interoperability/hype-reality-artificial-intelligence-ai-transform-health-healthcare/.

[225] Jonathan Kay, "How do you Regulate a Self-Improving Algorithm," the Atlantic, 25 Oct. 2017, https://www.theatlantic.com/technology/archive/2017/10/algorithms-future-of-health-care/543825/.

[226] John Sotos, "How the FDA Should Regulate Medical AI Systems," 15 Sep. 2017, https://blogs.wsj.com/experts/2017/09/15/how-the-fda-should-regulate-medical-ai-systems/

[227] Ibid.

[228]Ministry of Health, Labor and Welfare (MHLW), "Summary of Report of Round Table Conference on Promotion of Utilization of AI in the Field of Health and Medical Care," 27 Jun. 2017, https://drive.google.com/file/d/1qj69G2Ge13LWSE9_pdz2HEBh3mfbjgMn/view

The six areas include 1) Genomic medicine, 2) Diagnostic imaging support, 3) Diagnostic/treatment support, 4) Pharmaceutical product development, 5) Nursing care/dementia, and 6) Surgical support.

[229] Interview with Healthcare Science Division, Ministry of Health, Labour and Welfare (MHLW), Japan conducted on March 1, 2018.

[230] Wang Xiaodong, "Use of AI to Grow in China's Medical Sector," The Phnom Penh Post, 11 Oct. 2017, https://www.phnompenhpost.com/international/use-ai-grow-chinas-medical-sector.

[231] Ibid.

[232] Ibid.

[233] Ibid.

[234] Megan Molteni, "Health Care is Hemorrhaging Data. AI Is Here to Help," WIRED, 30 Dec. 2017, https://www.wired.com/story/health-care-is-hemorrhaging-data-ai-is-here-to-help/?mbid=BottomRelatedStories.

[235] Nick Stockton, "Veritas Genetics Scoops Up an AI Company to Sort Out Its DNA," WIRED, 07 Aug. 2017, https://www.wired.com/story/veritas-genomics-scoops-up-an-ai-company-to-sort-out-its-dna/.

[236] Emily Singer, "AI Could Help Predict Which Flu Virus Will Cause the Next Deadly Human Outbreak," 03 Sep. 2013, https://www.wired.com/2013/09/artificial-intelligence-flu-outbreak/.

[237] This methodology is given by Prof. Anya Maria Schiffrin's Media Campaigning and Social Change course at SIPA.

[238] This report conducted key entity scraping only on AV and Healthcare applications as examples.