Cloud Robotics and Interoperability: Enhancing Data Security Regulations in an Automated Age

KEHINDE OJADAMOLA TAKURO

Abstract- ***The interoperability of cloud robotics systems, as a backdrop for this paper, highlights the gaps in the current data security regulatory framework of the United States (US). While there is a wealth of scholarly works on privacy rights as it relates to cloud-based services and some research materials that address legal issues in the adoption of robots, detailed research assessing the effectiveness of the data security framework in the US regarding the convergence of robotic systems and cloud services, seems to be lacking. Such research is crucial in shaping policies that impact cloud robotics development. Through an examination of cloud robotics systems juxtaposed with the US data security regulatory framework, this paper advocates for an enhanced data security regulatory framework that takes into consideration the nuances of cyber-physical systems like cloud robots. This paper aims to contribute to policy developments that can spur regulatory reforms and ultimately enhance data protection for users of cloud robotics systems in the US.***

I. INTRODUCTION

By connecting to the cloud, robots can access extensive computational, storage, and communication resources housed in modern data centers, enabling them to share and process information with other robots or agents, including humans, across networks.[1] Although the term "cloud robotics" may be considered to have become more popular in recent years,[2] the use of cloud resources to enhance the functionalities of robot systems has been in existence for more than a decade.[3]

Twenty-first-century practical research in this field includes the RoboEarth Project[4] which developed a comprehensive "Cloud Robotics Infrastructure" to facilitate the seamless integration of robots with cloud infrastructure.[5] An underlying drive for this project could be linked to a conviction that future robots would need to perform tasks more quickly with a higher level of "intelligence" as well as adapt better to their environments, and such enhancements would not be possible without applicable cloud infrastructure.[6] Such convergence would allow the expansion of the concept of cloud robots to include better sensory and memory capabilities beyond their standalone systems.[7]

With technological advancements, cloud robotics systems have evolved considerably and are becoming more common in various industries.[8] Cloud robotics spans sectors such as medicine, telecommunications, media, law enforcement, automotive, and domestic activities. Specific applications include deployments of robots for performing surgeries,[9] self-driving vehicles,[10] elder care,[11] and Search and Rescue operations robots,[12] which push the boundaries of human-machine interaction by performing a wide range of tasks.[13]

As a new generation of these cyber-physical applications emerges, the potential for incessant data collection and perceived loss of control over personal information becomes apparent.[14] Put simply, the peculiar features of cloud robots increase their data security risks. While technical improvements play a crucial role in addressing these data security concerns, tailored regulations are also important in setting enforceable and effective standards to mitigate the risks. To provide context for how such regulatory standards are likely to be more effective, Part II of this paper describes cloud robots and highlights peculiar characteristics of cloud robotics systems. Part II also highlights the data security risks associated with these systems and sets forth some standards that may be effective in addressing such risks. Part III provides an overview of the US data security regulatory framework, and offers additional justification for enhanced data security regulations by highlighting key gaps in specified statutes and the implication of the patched regulatory framework. Part IV recommends

the promulgation of a federal data security law that includes addressable guidelines for the data security of cloud robots, as well as the establishment of a National Robotics Department for the development of tailored policies for data security in cloud robotics and similar systems.

II. CLOUD ROBOTS

A. Description and Application

Cloud robots have been defined as "any robot or automation system that relies on either data or code from a network to support its operation, where not all sensing, computation, and memory are integrated into a single standalone system."[15] They have also been regarded as modern robotics that use cloud computing and cloud storage.[16]

Tasks such as image processing, direction navigation, scanning, and voice recognition are some of the features that have become more efficiently possible(i) with many robots as a result of access to cloud resources which allow them to access updated image(ii) libraries, product data, and similar features.[17] Some(iii) unmanned aerial vehicles, sometimes called drones, can fly around capturing bird's-eye view pictures and(iv) directly upload those pictures to cloud storage services.[18] Other cloud robotics systems are designed to expedite air boarding procedures,[19] serve as intelligent household gadgets, or as automated human-like toys.[20] Additionally, cloud robots can be very valuable in handling big data, parallel grid computing, crowd-sourcing, and other activities.[21] Notably, certain scholars like Bekey have indicated that robots are machines built upon today's "sense-think-act" paradigm in artificial intelligence research.[22] Others acknowledge the ability of robots to perceive complexity and make appropriate decisions,[23] while some focus on robots' adaptability to environmental changes.[24]

The illustration below provides an overview of the architecture of cloud robotics systems.[25]

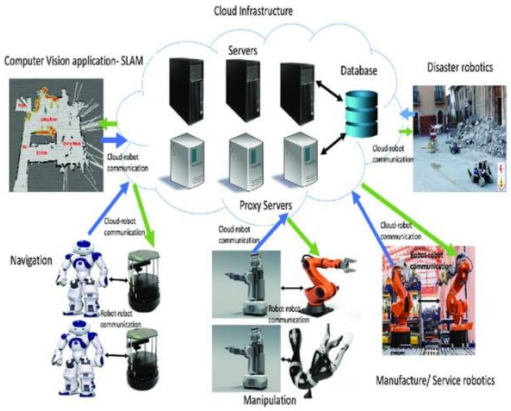

Figure 1: High-level overview of cloud robotics system architecture and applications.

In the context of this paper, robots are regarded as automated movable machines engineered to perform tasks with varying degrees of self-sufficiency. To expatiate:

"automated movable" entails the ability to move autonomously or within their surroundings

"machine" refers to their mechanical structure

"to perform tasks" highlights their functions as designed by the manufacturers

"varying degrees of sufficiency" emphasizes their ability to function independently or with varying levels of human intervention.[26]

Typically, robots have a structure composed of interconnected links, allowing for movement. The environment-interaction function that these robots are required to possess, leads to the incorporation of multiple sensors in the makeup of these robots. The primary aims of these sensors include proprioception, which entails the tracking of the robot's position and movement to monitor the robot's internal state, and exteroception which entails external stimuli detection. Exteroceptive sensors may include sensors that are sensitive to acceleration, pressure, light, touch, proximity, and sound.[27] The illustration below is a description of a type of robot referred to as the NAO robot.[28] The NAO is a small humanoid robot designed by French company Aldebaran for educational research centers, The NAO also has sensory capabilities that can be used in museums and dance performances.[29]

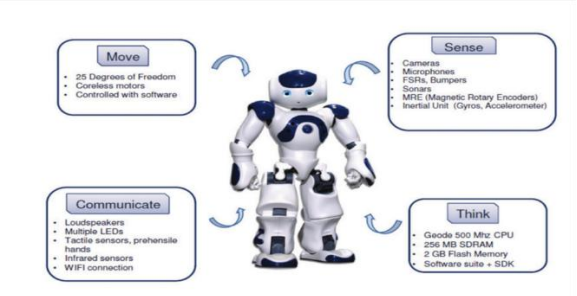

Figure 2: NAO's primary capabilities and sensors.

As a back-end representation of mergers of cloud services and robots, consider the custom robot solutions called Roomie, deployed by a fast-growing Mexican startup across Mexico and Latin America.[30] Roomie leveraged Amazon Web Services cloud infrastructure, including Amazon CloudWatch,[31] for developmental solutions, including storage, analysis, and insight-gathering of data to understand robot performance, identify trends, and develop better perception systems to understand the robot's surroundings in real-world environments. Overall, this enhances Roomie's robots' functionality, enabling them to interact and communicate with users more effectively.

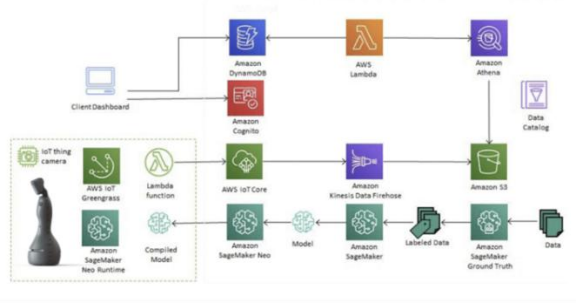

Figure 3: Roomie's adaptable setup for deploying and engaging with robots.[32]

The practical application of various cloud robots in society highlights their benefits, yet it also brings data security concerns associated with these systems closer to home, necessitating customized mechanisms to reduce such risks.

B. Data Security Concerns and Possible Regulatory Standards

Data security risks are not peculiar to cloud robots; they are also associated with independent cloud servers, mobile devices, network infrastructures, and several types of computer systems. However, the sensory and perception abilities, real-time communication protocols, edge computing features, complex data control and processing structure typical in cloud-enabled robots, as well as the embedding of the aforementioned features in artificially "intelligent"[33] machines that can interact with humans, exacerbate the data security risks in cloud robots when compared to conventional computer systems or stand-alone cloud servers.

Petit and Shladover[34] and Yaacoub et al.[35] in their research on potential cyber assaults targeting unmanned aerial vehicles and cooperative automated vehicles, detail specific threats such as malware, de-authentication, denial of service, ARP cache poison, and backdoor access, which can culminate into risks to the safety of human lives.[36] From an empirical perspective, Future Markets Insights, in its 2022 report on Cyber Security in Robotics Market Outlook, listed distributed denial of services, spoofing, man-in-the-middle, tampering, and reply attacks as some of the common cyber-attacks associated with robotics systems. Ultimately, these cybersecurity risks can have negative implications on the functionality of the robots and their interactions with humans,[37] highlighting the need for data security requirements that extend beyond the general requirements.

To provide context on the role of enforceable standards in mitigating such risks, an analysis of relevant features typical in cloud robots, and their data security concerns have been set out in the succeeding paragraphs of this section.

1. Sensory Abilities

Cloud robots typically have sensors such as inertial measurement units for navigation,[38] encoders for accurate measurement of displacements and velocities,[39] and lidars for three-dimensional environmental mapping, aimed at obtaining data from the environment to perform specified functions.[40] These sensors are highly vulnerable to cybersecurity risks such as jamming, falsified data, denial of service, data leakage, and spoofing attacks, which can negatively impact the perception of the robots and even cause them to malfunction when actuators[41] in these systems carry out the interpretation of instructions.[42] For example, the remote control of an unmanned aerial vehicle will entail the vehicle using

sensors and actuators to obtain data and ensure the transfer of such data for processing on a networked system.[43] Such transfer could also involve the exchange of telemetry data across jurisdictions or between two cloud robot systems. Where these cloud robot sensors are vulnerable, the data obtained can be maliciously used by bad actors to achieve end goals not intended by the developers of these systems.

The foregoing implies that it is beneficial for data security regulations and policies to require the inclusion of mechanisms at the sensor-design stage that enable cloud robot sensors to autonomously detect attacks and communicate such detection promptly in a way that both the user and manufacturers can address promptly. Such detection designs are feasible as demonstrated by the works of certain scholars like Bezemskij et al.[44] who detail the implementation of an automated threat detection system using a classification algorithm and tested the system on an actual robot to validate its efficacy.[45]

Further, the existence of standardized data minimization principles in applicable regulations can be effective in data security regulations as they would require such robots' sensors to only gather information essential to its operations, and unessential data must be deleted promptly to the extent reasonably possible. Further, express regulations and standards for end-to-end encryption and authentication protocols are particularly important for enhancing the data security processes of sensors used in cloud robotics systems. For instance, if proper encryption protocols are implemented in a humanoid robot and data interception by third parties occurs, the encryption algorithms will make such information unreadable to unauthorized individuals, and such information can therefore not be used to manipulate the humanoid robot. These comprehensive and practical regulatory standards will help protect data obtained by these sensory features of cloud robotics systems.

2. Complex Data Processing Structure

Unlike in stand-alone cloud computing systems, where the transfer and exchange of data generally seem more straightforward, the movement of data across machines and cloud environments (sometimes in different jurisdictions) and the importance of data portability to the enhanced functionality of cloud robotics systems, make data security more nuanced in the cloud robotics ecosystem.[46]

For instance, the concept of data breach (as well as incidence response and reporting requirements) will need to be construed very broadly for cloud robotics systems because of the multiple data entry points, layered architectural systems, and the high likelihood of involvement of multiple service layers and sub-providers in the development and operation of cloud robots.[47] This multiplicity factor increases the chances of vulnerabilities on both the side of the physical system and the cloud servers relying on these robots. Additionally, even authorized access can amount to data breaches. Some of these cloud environments are used by multiple organizations,[48] which then demands a regulatory framework that promotes safe and seamless data portability, and expressly requires data isolation and management of digital identities in cloud ecosystems.

3. Remote Access

The ability to access a cloud robot remotely makes it highly vulnerable to data security risks. There is the potential for bad actors to manipulate the physical structures of the robot, either remotely even from a jurisdiction different from the location of the robot, or in person, thereby controlling the robot or tampering with data that the robot has access to. Remote access also introduces additional entry points for exploitation such as unsecured communication protocols, or vulnerabilities within the physical systems or cloud servers.[49] These risks demand stricter data security regulations. Specifically, monitoring obligations and access limitations, such as requiring a digital signature or biometric access should be expressly imposed on manufacturers and authorized persons who interact with and have access to the physical structure of the robots as well as the cloud servers used by such robots.[50] Also, standardized regulations can help address the potential cross-jurisdictional nature of data processing, control, and access to cloud robotics systems.

4. Communication Protocols and Network Infrastructure

Seamless interaction between physical robots and cloud servers is significantly facilitated by communication protocols and their network

infrastructure. These protocols, such as the Robot Operating System (ROS) and Message Queuing Telemetry Transport (MQTT), are generally regarded as procedures and rules that dictate how robots, networks, and other devices communicate with each other.[51]

Since communication protocols entail the transfer of data across networks and physical devices, there are more susceptible to breach in the event of vulnerabilities or where there is a lack of adequate layered security systems. For example, health monitoring systems, which have communication protocols, usually involve the transfer of data to a database server or other electronic devices via Wi-Fi or radio frequency,[52] and research studies have demonstrated that these channels are usually vulnerable and can cause the leak of patients' information.[53] If such transmitted data are not properly encrypted, it could be especially harmful since such data can be directly interpreted.[54]

Consequently, the communication infrastructure of cloud robots highlights that express and customized requirements for access control mechanisms such as Transport Layer Security (to restrict unauthorized application programming interface calls) and cryptographic protocols for cloud robotics systems, are particularly important in enhancing the security of data accessed or transferred via their communication infrastructure. [55]

5. Edge Computing

As a result of certain limitations of cloud computing (based on its centralized data center), which leads to heavy bandwidth costs and lengthy time delays, many cloud robot systems adopt edge computing. In other words, such cloud robots feature a three-layer architecture comprising the cloud, edge computing, and the physical aspects of the system.[56]

In edge computing, data processing occurs along the path between data sources and the cloud, that is, the "edge".[57] The advantage of the edge computing incorporation to cloud robots is that it "offloads some computationally extensive tasks to the edge node rather than a distant cloud".[58] Also, edge nodes can harmonize the interface of homogenous devices, and perform caching and processing, as well as distribute request and delivery service from cloud to user.[59] For example, edge computing enables autonomous vehicles to rapidly assess sensor data and make split-second decisions while driving.

The vulnerabilities of these data processing activities close to the "edge" include that where adequate security mechanisms are not in existence, there is an increased risk of data exposure and cybersecurity attacks.[60] Also, the distribution of request and delivery service from the cloud to the user via edge nodes indicates the risks to data security during such request distribution as it can entail the transmission of raw sensor data.[61]

Aligning with scholarly recommendations,[62] local data anonymization or aggregation to the extent reasonably possible can be required in data security regulations as a pre-requisite for the transmission of sensitive data in robotics systems to help minimize the chances of compromise of sensitive information. Further, the importance of sophisticated security protocols for cloud robotics systems comes to the fore especially for cloud robots adopting edge computing, considering the dynamic nature of these edge network systems and their interaction with cloud servers and users.[63]

III. US DATA SECURITY REGULATORY FRAMEWORK

A.

B. Overview of Regulatory Framework

The US has federal and state laws, as well as sector-specific laws or regulations, that impose data protection obligations and impact the data security processes of businesses.[64] Examples of state laws that can impact the data security processes in the US cloud robotics industry include the New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act,[65] and the California Consumer Privacy Act (CCPA).[66] Furthermore, according to the National Conference of State Legislatures, each of the 50 states, as well as Puerto Rico, Guam, the District of Columbia, and the Virgin Islands have legislation requiring private businesses to report breaches as required under such statutes.[67] The current state laws may be considered to be robust laws — at least from an intrastate commerce perspective — designed to enhance the protection of consumer data privacy rights for businesses operating within these states.

Additionally, at the federal level, the Federal Trade Commission (FTC) Act is often interpreted to prevent deceptive data security practices by businesses. Also, privacy and security rules regulations under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act),[68] generally regulate the handling of applicable personal health information (PHI) within the healthcare industry which may impact health care robots.[69] In the event of a data breach, covered entities and their business associates are required to notify specified persons and institutions, including affected individuals and the U.S. Department of Health and Human Services, within the mandated timeline.[70]

C. Enhancing Data Security Regulations for Cloud Robotics: Further Justifications

This multiplicity of statutes indicates the compliance gaps that may be associated with interpreting a myriad of laws to enhance the data security of multifaceted systems like cloud robots. In other words, a unified data security framework is likely to be more effective and enforceable for complex cyber-physical systems. To complement the analysis in section B of Part II of this paper, an evaluation of the concept of data breach in the HITECH Act, California's breach notification law, New York Information Security Breach and Notification Act,[71] and Massachusetts' breach notification law, as well as certain data protection obligations in the SHIELD Act, is conducted in the succeeding paragraphs of this section to highlight the need for enhanced data security regulatory standards, especially for cloud robotics systems.

1. Construing Data Breach

Cloud robotics systems merge networked systems, cloud services, third-party systems, processing units, physical data servers, and the physical robots themselves. As a result, the issue of data breach can arise from different (and possibly authorized) endpoints, exacerbating the complexity. In addition, for cloud robotics systems connected with or sharing data with other robotics systems, a breach in one component could lead to a data breach in another associated robotic system. While this scenario may seem like the imagination of a writer of a science fiction movie, such instances are a possibility with current and future innovations in cloud robotics. In addition, with these systems processing information in real-time and sometimes relying on services from third-party providers, tracing the source of a data breach can be challenging.

Notably, the HITECH Act defines a breach as the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information, subject to certain exceptions.[72] It is posited that in addition to the sectoral limitation of these health data rules, the definition of data breach highlights a gap in the current health data security regulations framework. Particularly, the word "unauthorized" in the aforementioned definition of a data breach could suggest that technical vulnerabilities leading to unintended data breaches, which are very possible in cloud robotics systems, may not necessarily constitute a data breach under the relevant rules. Moreover, authorized uses or access to PHI that are unnecessary, may not be classified as data breaches especially in the cloud robotics ecosystem, if the rules are interpreted literally by the courts.

Furthermore, the direct and indirect involvement of third-party suppliers in these cloud robotics systems, coupled with the limitation of obligations in these health data privacy and security rules to "covered entities" and "business associates" as defined in the HIPAA rules, potentially means that many third party suppliers providing indirect services in the cloud robotics ecosystem for health purposes may have strong arguments suggesting that the data security compliance obligations do not apply to them, even when they have access to consumers' PHI.

With regards to state law, California's breach notification law defines a breach as the "*unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of integrity of personal information maintained by the person or business*".[73] New York Information Security Breach and Notification Act,[74] and Massachusetts' breach notification law have similar definitions which in effect posit that a breach of security is an unauthorized acquisition or unauthorized use of personal information that compromises the security or confidentiality of the information protected by the applicable law.[75] These definitions, similar to HIPAA

security rules, limit breaches to unauthorized use or acquisition, overlooking the possibility of technical vulnerabilities leading to unintended breaches. This highlights the inadequacy and gaps in these fragmented regulations, particularly when dealingIV. with complex cloud robotics systems with multiple endpoints in different states or controlled by different operators, making them vulnerable to breaches even where there is no unauthorized access.

2. Obligations in a Multi-Party Ecosystem

Another statute that highlights the current regulatory gap as it relates to data security obligations of cloud robotics market players is the SHIELD Act. This Act generally imposes commendable data security obligations on covered businesses that own or license computerized data which includes private information of NY residents.[76] In situations where a cloud service provider does not "own" or "license" such data, it appears that the aforementioned obligation would not apply to them, even though they may play a relevant role in the processing of such data. It can be argued that the SHIELD Act, by referencing other statutes like Title V of the federal Gramm-Leach-Bliley Act, implies that processors who do not own or license computerized data are still subject to the applicable provisions of the SHIELD Act. However, such an argument further affirms the ambiguity that arises from the current data security regulatory framework. While it is important to avoid regulations that may stifle innovation, it is also important to ensure that relevant parties are expressly subject to data security obligations.

Commendably, the SHIELD Act mandates covered entities to require their third-party service providers to implement security measures equivalent to the standards by contract.[77] However, this approach might still not suffice especially where there is no direct partnership between the entity regulated under the SHIELD Act and the "unregulated" third-party service provider. Amending such a provision of the SHIELD Act to expressly extend data security obligations to entities involved in the development of systems that would have access to computerized data, appears to be a good way to address the current gap.

It is opined that expanding stipulated obligations to cover all relevant entities will not hinder innovation but rather improve interoperability by establishing clearer standards, rather than relying on contract terms among various entities.

Recommendations

While the sector-specific and state data protection regulations impacting cloud robotics systems operating in the US have laid a commendable groundwork for data security, there's still room for improvement. It is time to 'get the ducks in a row' by adopting a harmonized and tailored regulatory framework in the US that anticipates the convergence and borderless nature of technologies, especially in the realm of cloud robotics systems. This regulatory framework should include the promulgation of a federal data security regulatory law with a section containing addressable cybersecurity guidelines[78] for cloud robotics and similar cyber-physical systems. Notably, a harmonized data security regulatory framework exists in jurisdictions with enhanced data security regulations like South Korea,[79] the European Union,[80] and China[81] which are key market players in the use and development of robotics, artificial intelligence, and cloud computing.

Further to the potential regulatory standards in Part II of this paper, specific provisions that should be reflected in the proposed national regulatory framework for the US include robust encryption requirements, data processing principles and data protection obligation that cover businesses that own and license data as well as other businesses involved directly or indirectly in the processing of or have access to such data, a broad definition of data breach to cover unauthorized access to data as well as authorized access that culminates in united violation of expected standards or technical vulnerabilities, harmonized reporting requirements, stringent access control mechanisms, clear guidelines on data ownership rights and data residency rights including as it relates to data generated by robots and data stored in the clouds, practical data security guidelines for partnerships that will entail transfer or processing of data with entities outside the US, regular independent cybersecurity audits for cloud robotics providers and other third party service providers, as well as the empowerment of an appropriate agency such as National Institute of Standards and Technology (NIST) with clear broad authority to provide

enforceable and addressable guidelines for such cyber-physical systems.

It is pertinent to mention that a proposed federal data protection legislation titled the American Data Privacy and Protection Act (ADPPA),[82] (which with appropriate updates to the draft Bill, may have been a step in the right direction) has failed to advance before Congress.[83] Agency leaders maintained that it would not hold enforcement power under state legislation, even though the ADPPA's preemption provision preserved components of state privacy laws. It is posited that a federal tailored data security regulatory framework is still feasible, considering that the cross-border nature of many technology processes is culminating in increased interstate transfer of data in activities involving data. Since there is a thriving tech industry in California and the CCPA can be regarded to be a robust regulation, federal law could be modeled with provisions similar to the CCPA, with relevant updates such as the recommendations in this paper, included in the federal law, and then other states can be lobbied to amend their state laws to reflect this. Then, state laws could affect just specified intrastate data security matters that are not preempted by federal law.

Also, there is merit in considering the establishment of a National Robotics Department (NRD) as a department of a relevant agency, preferably the NIST, to contribute, among other things, to the development of tailored policies and standards for data security in cloud robotics and similar systems. This recommendation differs slightly from Ryan Calo's[84] recommendation that a Federal Robotics Commission (FRC) should be established. While the benefits of such a commission, such as independence and focused attention on robotics matters, are recognized, it is maintained that the establishment of an NRD as a department of the NIST has overriding advantages such as cost-efficiency, ease of collaboration with other departments of the NIST, creation of policies that take into consideration different sectors of the economy, ease of leveraging expertise and resources of NIST, and the likelihood of speed in the establishment and operation of such a department.

CONCLUSION

With the US being a key player in the global market for cloud robotics and the cross-jurisdictional nature of cloud robotics use and development,[85] the potential and existing adverse effects of inadequate data security standards for cloud robotics on individuals, businesses, and state governments cannot be overemphasized.[86]

From a national security standpoint, inadequate data security standards for robotics systems such as drones or combat robots with remote capabilities could inadvertently cause harm or could be exploited by malicious actors to target civilians, obtain sensitive national information, or destroy properties.[87] Further, the use of cloud robots for healthcare purposes has numerous benefits such as effective surgery assistance. However, where health data stored in the cloud is altered maliciously or there are data security weaknesses that impact the function of these cloud robots, or health care information of patients on cloud servers connected to health care robots used for surgeries are leaked or tampered with, it could cause emotional harm, and even endanger the lives of patients.[88] Safety concerns also arise from security vulnerabilities of autonomous driving cars, with reports of fatal incidents raising questions about their reliability.[89] With regards to the economy, while cloud robots have evident manufacturing, business and social benefits, vulnerabilities in their data security structures can have a negative impact on consumer trust, innovation, and ultimately the economy.

These adverse effects underscore the importance of a proactive reassessment of current data security regulatory frameworks in the US. Without tailored actions to better secure these cloud robotics systems, cyberattacks could escalate in size and frequency.[90] The implementation of a harmonized and tailored framework may seem daunting at first glance. However, given that the concept of cloud robots itself was considered impossible at some time, it demonstrates that with the necessary willpower and recognition of the benefits to legislative reputation and the US economy, the regulatory proposal is feasible. A harmonized framework would not only enhance data security but would streamline compliance operations,

promote secure data portability, and ultimately foster innovation on a national level.

REFERENCES

[1] Wuhui Chen, Yuichi Yaguchi, Keitaro Naruse, Yutaka Watanobe, and Keita Nakamura, *A Study of Robotic Cooperation in Cloud Robotics: Architecture and Challenges*, IEEE ACCESS. (2018) pp. 1-1. 10.1109/access.2018.2852295. https://www.researchgate.net/publication/326193277_A_Study_of_Robotic_Cooperation_in_Cloud_Robotics_Architecture_and_Challenges/citations. (Accessed April 20, 2024).

[2] See Ragab, Ahmed & Khalil, Abeer & Elfaham, Mohamed & Hashad, Atalla, (2018), *Cloud Robotics: A Survey*, pp. 46-52. https://www.researchgate.net/publication/334726380_Cloud_Robotics_A_Survey, which cited James J. Kuner. *Cloud-Enabled Robots*. In IEEE-RAS INTERNATIONAL CONFERENCE ON HUMANOID ROBOTS, Nashville, TN, 2010.

[3] [1] *See generally Masayuki Inaba et al., A Platform for Robotics Research Based on the Remote-Brained Robot Approach, 19* INT'L J. ROBOTICS RES. *933, 933–39 (2000) (proposing a framework for "the remote-brained robot approach"). 7. See, e.*

[4] (2010-2014).

[5] Markus Waibel et al, *A World Wide Web For Robots, 18* IEEE ROBOTICS & AUTOMATION MAGAZINE, No. 2 (2011), pp. 69-82.

[6] Ugo Pagallo, *Robots In The Cloud With Privacy: A New Threat To Data Protection?*, 29 COMPUTER LAW & SECURITY REVIEW, Issue 5, (2013), pp. 501-508.

[7] *Id.*

[8] Andrew Proia and Drew Simshaw, *Consumer Cloud Robotics and the Fair Information Practice Principles: Recognizing the Challenges and Opportunities Ahead, 16* MINNESOTA JOURNAL OF LAW, SCIENCE & TECHNOLOGY, (2015), Issue 1, pp. 149.

[9] Daniele Giansanti, and Rosario Alfio Gulino, *The Cybersecurity and the Care Robots: A Viewpoint on the Open Problems and the Perspectives*, HEALTHCARE (BASEL) (2021), 1653, doi: 10.3390/healthcare9121653 (Accessed April 20, 2024).

[10] Yang Yu and Sanghwan Lee, *Remote Driving Control With Real-Time Video Streaming Over Wireless Networks: Design and Evaluation,* 10 IEEE ACCESS, (2022), pp. 64920-64932, 2022, doi: 10.1109/ACCESS.2022.3183758.

[11] Adriana Tapus, Juan Fasola, and Maja J. Mataric, *Socially Assistive Robots for Individuals suffering From Dementia*, (2008), RESEARCHGATE, https://www.researchgate.net/publication/228968582_Socially_assistive_robots_for_individuals_suffering_from_dementia. (Accessed April 22, 2024).

[12] Tuan Vuong, Avgoustinos Filippoupolitis, George Loukas, and Diane Gan, *Physical Indicators of Cyber Attacks Against a Rescue Robot,* (2014) IEEE INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING AND COMMUNICATION WORKSHOPS, PERCOM WORKSHOPS 2014. 338-343. 10.1109/PerComW.2014.6815228.

[13] Laura Romeo, Antonio Petitti, Roberto Marani, and Annalisa Milella, *Internet of Robotic Things in Smart Domains: Applications and Challenges*, SENSORS (BASEL), 3355, (2020). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349752/. (Accessed April 22, 2024).

[14] Pagallo, *supra* note 6.

[15] Ben Kehoe, Sachin Patil, Pieter Abbeel, Ken Goldberg, *A Survey of Research on Cloud Robotics and Automation*, 12 IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING, (2015), pp. 398–409. https://ieeexplore.ieee.org/document/7006734 (Accessed May 7, 2024).

[16] Chen, *supra* note 1.

[17] Olimpiya Saha, and Prithviraj Dasgupt, *A Comprehensive Survey of Recent Trends in Cloud Robotics Architectures and Applications*, (2015), 7 ROBOTICS, (3):47. https://cir.nii.ac.jp/crid/1360861712188306560, (Accessed April 20, 2024).

[18] Jerico Moeyersons, Martijn Gevaert, Karl-Erik Réculé, Bruno Volckaert, and Filip De Turck, *UAVs-as-a-Service: Cloud-based Remote Application Management for Drones*, *(*IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, 2021), pp. 926-931.

[19] *Emirates Introduces Revolutionary Robotic Check-in System at Dubai International Airport*, Emirates Times, (March 10, 2023), https://theemiratestimes.com/emirates-introduces-robotic-check-in-system/ .

[20] As an example, see the Robopal toy: Dylan F. Glas, Takahiro Miyashita, Hiroshi Ishiguro, Norihiro Hagita, *Robopal: Modeling Role Transitions in Human-Robot Interaction, (*Proceedings 2007 IEEE International Conference on Robotics and Automation, Rome, Italy, 2007), pp. 2130-2137, doi: 10.1109/ROBOT.2007.363636.

[21] Saha, *supr*a note 18.

[22] GEORGE A. BEKEY, AUTONOMOUS ROBOTS: FROM BIOLOGICAL INSPIRATION TO IMPLEMENTATION AND CONTROL, The MIT Press, Cambridge, Mass. & London (2005)

[23] PETER SINGER, WIRED FOR WAR: THE ROBOTICS REVOLUTION AND CONFLICT IN THE 21ST CENTURY, Penguin, London (2009).

[24] Pagallo, *supra* note 6.

[25] Saha, *supra* note 18.

[26] See the definition of Neil Richards, and William Smart, *How Should the Law Think About Robots*?, (2013) https://ssrn.com/abstract=2263363 (Accessed April 22, 2024).

[27] JIEFEI WANG AND DAMITH HERATH, FOUNDATIONS OF ROBOTICS: A MULTIDISCIPLINARY APPROACH WITH PYTHON AND ROS, Springer, and Kinova (2022), Chapter 7, pp. 180, *https://doi.org/10.1007/978-981-19-1983-1* (Accessed April 22, 2024).

[28] Aldabarn Robotics. NAO Software Documentation. 2019, http://doc.aldebaran.com/index.html (Accessed April 19, 2024).

[29] Elfituri Lahemer, and Ahmad Rad, An *Adaptive Augmented Vision-Based Ellipsoidal SLAM for Indoor Environments*, SENSORS, (2019), https://www.researchgate.net/publication/333939201_An_Adaptive_Augmented_Vision-Based_Ellipsoidal_SLAM_for_Indoor_Environments (Accessed May 7, 2024).

[30] Alfredo Polito, Camilo Buscaron, and Grace Reed, *Roomie Uses AWS Robomaker to Scale Custom Robotics Development*, Amazon Robotics Blog (April 1, 2021), https://aws.amazon.com/blogs/robotics/roomie-uses-aws-robomaker-to-scale-custom-robotics-development/ (Accessed April 21, 2024).

[31] As well as Amazon Lex, Amazon Kinesis, Amazon S3, and Amazon Recognition via the AWS RoboMaker cloud Extensions for ROS.

[32] Polito, *supra* note 30.

[33] Angelica Lima, *Robots Aren't as Smart as You Think*, https://www.technologyreview.com/2017/11/02/147995/robots-arent-as-smart-as-you-think/, MIT Technology Review (2017) (Accessed May 6, 2024).

[34] Jonathan Petit, and Steven E. Shladover, *Potential Cyberattacks on Automated Vehicles,* 16 IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS (2015).

[35] Jean-Paul Yaacoub, Hassan Noura, Ola Salman, and Ali Chehab, *Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations,* 21 INTERNATIONAL JOURNAL FOR INFORMATION SECURITY *(2021).*

[36] Gledre Sabaliauskaite, Geok Ng, Justin Ruths, Aditya Mathur, *A Comprehensive Approach, and a Case Study for Conducting Attack Detection Experiments in Cyber–Physical Systems*, 98 ROBOTICS AND AUTONOMOUS SYSTEMS (2017).

[37] Future Market Insights, Cyber Security in Robotics Market Outlook (Forecast 2023 to 2033). (February 2022).

[38] Gerasimos Samatas, and Theodore Pachidis, *Inertial Measurement Units (IMUs) in Mobile Robots over the Last Five Years: A Review*, 6 Designs, (2022) pp. 17. https://www.mdpi.com/2411-9660/6/1/17 (Accessed May 6, 2024).

[39] Ferran Paredes, Cristian Herrojo, and Ferran Martín, *Position Sensors for Industrial Applications Based on Electromagnetic Encoders, Sensors*, 8 BASEL, (2021), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8069193/ (Accessed May 7, 2024).

[40] Madhushanka Padmal, Dileepa Marasinghe, Vijitha Isuru, Nalin Jayaweera, Samad Ali, and Nandana Rajatheva, *Elevated LiDAR Based Sensing for 6G - 3D Maps with cm Level Accuracy*, 2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring), Helsinki, Finland, 2022, pp. 1-5, https://ieeexplore.ieee.org/document/9860788 (Accessed May 7, 2024).

[41] Actuators generally work with the sensors to carry out the required function. When a sensor obtains information from the environment, an algorithm can then be employed to interpret and decide on action based on such information, and a set of instructions is then sent by the algorithm to the robot's actuators based on the sensory information to carry out the relevant purpose. See Jiefei Wang and Daminth Herath, *What Makes Robots? Sensors, Actuators, and Algorithms*, Foundations of Robotics (2022). Springer, Singapore, https://link.springer.com/chapter/10.1007/978-981-19-1983-1_7 (Accessed May 6, 2024).

[42] Dimitris Gritzalis, Grammati Pantziou, and Rodrigo Román-Castro, *Sensors Cybersecurity*, SENSORS BASEL (2021), https://www.researchgate.net/publication/350679707_Sensors_Cybersecurity (Accessed May 6, 2024).

[43] Pagallo, supra note 6.

[44] Anatolij Bezemskij, George Loukas, Richard Anthony, and Diane Gan, *Behaviour-Based Anomaly Detection of Cyber-Physical Attacks on a Robotic Vehicle*. IN PROCEEDINGS OF THE 15TH INTERNATIONAL CONFERENCE ON UBIQUITOUS COMPUTING AND COMMUNICATIONS AND 2016 INTERNATIONAL SYMPOSIUM ON CYBERSPACE AND SECURITY (IUCC-CSS), Granada, Spain, 14–16 December 2016; pp. 61–68.

[45] See also Chundong Wang, Yee Ching Tok, Rohini Poolat, Sudipta Chattopadhyay, and *Mohan Elara, How to Secure Autonomous Mobile Robots? An Approach with Fuzzing, Detection and Mitigation*, 112 JOURNAL OF SYSTEMS ARCHITECTURE (2021), 101838., https://www.sciencedirect.com/science/article/abs/pii/S1383762120301302 (Accessed May 6, 2024).

[46] 35 Millard, C., Hon, W. K., and Singh, J. "Internet of Things Ecosystems: Unpacking Legal Relationships and Liabilities." In 2017 IEEE International Conference on Cloud Engineering (IC2E), (2017): 286-291.

[47] Hon, W.K., and Millard, C, *Cloud Technologies and Services*, In Millard, C. (ed) CLOUD COMPUTING LAW, Oxford University Press, 2013, pp. 3-17.

[48] Timothy Morrow, *12 Risks, Threats, & Vulnerabilities in Moving to the Cloud*, Software Engineering Institute Blog, (March 5, 2018) https://insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud/ (Accessed May 6, 2024).

[49] Pagallo, *supra* note 6.

[50] Yaacoub, *supra* note 35. See also Olga Weis, *Cloud Based Biometric Attendance System with Redirection Technology*, FlexiHub Blog (February 8, 2023) https://www.flexihub.com/biometric-device-to-the-cloud/ (Accessed May 7, 2024).

[51] Armin Mokhtarian, Alexandru Kampmann, Maximilian Lueer, Stefan Kowalewski, and Bassam Alrifaee, *A Cloud Architecture for Networked and Autonomous Vehicles*, CONFERENCE: 16TH IFAC SYMPOSIUM ON CONTROL IN TRANSPORTATION SYSTEMS CTS 2021, (June 2021), at Lille, France, https://www.researchgate.net/publication/355096282_A_Cloud_Architecture_for_Networked_a

nd_Autonomous_Vehicles (Accessed May 6, 2024).

[52] Kassem Fawaz, Kyu-Han Kim, Kang Shin, *Protecting Privacy of BLE Device Users*, IN PROCEEDINGS OF THE 25TH USENIX SECURITY SYMPOSIUM (USENIX SECURITY 16), Austin, TX, USA, 10–12 August 2016. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/fawaz (Accessed May 8, 2024).

[53] Luis Hernández-Álvarez, Juan José Bullón Pérez, Farrah Kristel Batista, and Araceli Queiruga-Dios, *Security Threats and Cryptographic Protocols for Medical Wearables*, MATHEMATICS (2022), https://www.researchgate.net/publication/359170145_Security_Threats_and_Cryptographic_Protocols_for_Medical_Wearables (Accessed May 8, 2024).

[54] *Id.*

[55] Alessandra Sorrentino, Filippo Cavallo, and Laura Fiorini, A Plug and Play Transparent Communication Layer for Cloud Robotics Architectures, ROBOTICS (2020) https://flore.unifi.it/retrieve/handle/2158/1195202/483749/IP0xx%20-%20MDPI%20robotics%20Cloud%20robotics.pdf (Accessed May 8, 2024).

[56] Weisong Shi, Jie Cao, Quan Zhang, Youhuizi Li, and Lanyu Xu, *Edge Computing: Vision and Challenges*, IEEE INTERNET OF THINGS JOURNAL, (2016) 3(5):637-646, (Accessed May 8, 2024).

[57] *Id.*

[58] *Id.*

[59] P. Jorge Escamilla-Ambrosio, Abraham Rodríguez-Mota, Eleazar Aguirre-Anaya, Raul Acosta-Bermejo, and Moises Salinas. Distributing Computing in the Internet of Things: Cloud, Fog and Edge Computing

[60] Over-view, STUDIES IN COMPUTATIONAL INTELLIGENCE JOURNAL (2018) https://www.researchgate.net/publication/319715424_Distributing_Computing_in_the_Internet_of_Things_Cloud_Fog_and_Edge_Computing_Overview (Accessed May 8, 2024).

[61] Shi, *supra* note 56.

[62] *Id.*

[63] *Id.*

[64] Francis DaCosta, *Rethinking the Internet of Things: A Scalable Approach to Connecting Everything. New York, NY, USA*: (2013), APRESSOPEN.

[65] Some of these laws are regarded as data privacy laws. Although, the concepts of data privacy, data protection, and data security overlap, data privacy generally focuses on the rights of consumers to privacy of their information.

[66] Codified under New York's General Business Law as Article 39-F sections 899-AA and 899-BB.

[67] Act of 2018 as amended by the California Privacy Rights Act of 2020 (CPRA),

[68] Security Breach Notification Laws, (January 17, 2022), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws#:~:text=All%2050%20states%2C%20the%20District,information%20involving%20personally%20identifiable%20information. (Accessed April 21, 2024).

[69] 43 USC 17932).The HITECH Act was enacted as part of the American Recovery and Reinvestment Act of 2009, and signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology - https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html (Accessed April 21, 2024).

[70] Also, the HITECH Act extended the duties of business associates under the HIPAA Security Rule, with subsequent regulations from HHS to enact and clarify these adjustments. See HHS' publication on, Summary of the HIPAA Security Rule, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html. (Accessed April 21, 2024).

[71] Section 13400(1) and 13402(a) and (b) of the HITECH Act. The Act incorporates the

definitions of ‘‘covered entity,’’ ‘‘business associate,’’ and ‘‘protected health information’’ used in the HIPAA Administrative Simplification regulations (45 CFR parts 160, 162, and 164) (HIPAA Rules) at § 160.103.

[72] 2005, which was amended by the SHIELD Act, https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act (Accessed April 22, 2024).

[73] These exceptions include “disclosures where the recipient of the information would not reasonably have been able to retain the information, certain unintentional acquisition, access, or use of information by employees or persons acting under the authority of a covered entity or business associate, as well as certain inadvertent disclosures among persons similarly authorized to access protected health information at a business associate or covered entity”. See, Department of Health and Human Services, Office of the Secretary, *Breach Notification for Unsecured Protected Health Information*, Federal Register/Vol. 74, No. 162/Monday, August 24, 2009/Rules and Regulations, 45 CFR Parts 160 and 164 RIN 0991–AB56, https://www.govinfo.gov/content/pkg/FR-2009-08-24/pdf/E9-20169.pdf (Accessed April 21, 2024).

[74] Section 1798.82 of the California Civil Code.

[75] 2005, which was amended by the SHIELD Act, https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act (Accessed April 22, 2024).

[76] Part 1, Title XV, Chapter 93H of Massachusetts General Laws, https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H (Accessed April 22, 2024).

[77] Section 899-bb of the New York General Business Law.

[78] Section 899-BB (2)(a)(5) of the New York General Business Law.

[79] Addressable guidelines in this context refer to regulations that are required to be followed, while leaving some discretion to entities. Where there is a more efficient or better procedure or process different from the stipulated guideline, entities would generally be able to implement the better option within the confines and spirit of the relevant regulation.

[80] See South Korea’s Personal Information Protection Act (PIPA), A translation of PIPA is available at https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG ,accessed on April 22, 2024; and South Korea’s Guidance on the Safe Use of Personal Information in the Age of Artificial Intelligence, https://securiti.ai/south-korea-safe-use-of-personal-information-in-ai/ (Accessed April 20, 2024).

[81] European Union’s General Data Protection Regulation (GDPR). The GDPR is enforced by independent national data protection agencies, as well as national courts. See Data protection: Commission adopts new rules to ensure stronger enforcement of the GDPR in cross-border cases, European Commission Press Release, July 4, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3609 . (Accessed April 20, 2024). See also Civil Law Rules on Robotics European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0051&rid=9#:~:text=C%20252%2F241-,Thursday%2016%20February%202017,conflict%20with%20the%20First%20Law. (Accessed April 20, 2024).

[82] China’s Cybersecurity Law whose translation is available here https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ (Accessed April 20, 2024). China’s Personal Information Protection Law available here https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/ (Accessed April 22, 2024). China’s Data Security Law whose Translation is available here https://www.chinalawtranslate.com/en/datasecuritylaw/ (Accessed April 22, 2024). China’s Regulations on Management of Network Product

Security Vulnerability Management, whose translation is available https://www.chinalawtranslate.com/en/product-security-vulnerabilites/ (Accessed April 20, 2024).

[83] This bill establishes requirements for how companies, including nonprofits and common carriers, handle personal data, which includes information that identifies or is reasonably linkable to an individual. The bill was sponsored by Rep. Pallone, Frank, Jr. [D-NJ-6] , and introduced on June 21, 2022. The latest action on the bill on the Congress website is stipulated as "Placed on the Union Calendar, Calendar No. 488, Action By: House of Representatives" on December 30, 2022. See https://www.congress.gov/bill/117th-congress/house-bill/8152 (Accessed April 22, 2024)

[84] Alan Butler and Hayley Tsukayama,, Data Protection Leaders Differ on Powers of New US Privacy Law, Bloomberg Law (October 6, 2023) https://news.bloomberglaw.com/privacy-and-data-security/data-protection-leaders-differ-on-powers-of-new-us-privacy-law (Accessed April 22, 2024).

[85] Ryan Calo, *Robotics and the New Cyberlaw*, 103 CALIFORNIA LAW REVIEW, (2015). No. 3, pp. 513-63.

[86] Rika Melissa, *Global Cloud Robotics Market to Reach USD 74.7 Billion by 2032*, Statzon (January 12, 2024), https://statzon.com/insights/global-cloud-robotics-market#:~:text=Cloud%20Robotics%20Market%20Size&text=The%20global%20cloud%20robotics%20market,34.7%25%20from%202023%20to%202032 (Accessed April 21, 2024).

[87] Cesar Cerrudo, Lucas Apa, *Hacking Robots Before Skynet*, CYBERSECURITY INSIGHT, IOACTIVE REPORT, Seattle, USA (2017) https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf (Accessed May 7, 2024).

[88] Alessio Botta, Sayna Rotbei, Stefania Zinno, and Giorgio Ventre, *Cyber Security of Robots: A Comprehensive Survey*, 18 SCIENCE DIRECT (2023), 200237.

[89] *Id.*

[90] *Id.*

[91] Wojciech Szynkiewicz, Niewiadomska-Szynkiewicz Ewa, and Kamila Lis, *Deep Learning of Sensor Data in Cybersecurity of Robotic Systems: Overview and Case Study Results*, 12 Electronics (2023), no. 19: 4146. https://doi.org/10.3390/electronics12194146 (Accessed May 8, 2024).