Can Patient Information Held by an AI Robot Be Protected by the Duty of Confidentiality?

Lupton, Michael

Published in:
International Journal of Medical Science and Health Research

International Journal of Medical Science and Health Research

Vol. 4, No. 04; 2020

ISSN: 2581-3366

Can Patient Information Held by an AI Robot Be Protected by the Duty of Confidentiality?

Professor Michael Lupton
Faculty of Law
Bond University
Gold Coast Australia

Abstract

Modern Medicine is today driven by scientific discoveries in fields such as genetics, stem cells and CRISPR Cas 9. The implementation of this technology, in the form of therapeutic treatment, is still carried out by doctors in accordance with the moral rules they swear to uphold in the Hippocratic Oath.

The doctor-patient relationship remains a contractual one, based on the moral precepts of the Oath, one of which is the duty of confidentiality e.g.

What I may see or hear in the course of treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself'.

However, modern technology in the shape of AI robots has impacted on this field of medicine as well. AI platforms run by algorithms, such as IBM's Watson, are now being used in medical practices to assist doctors in diagnoses and to drive down costs. Examples are the use of automated diagnoses to pinpoint diabetic retinopathy by the use of retinal Images. A similar process is used to diagnose skin cancer. Diagnosis of cancer in a patient's lymph nodes was significantly advanced by the 2016 Challenge Competition known as 'CAMELYON' 16 which was arranged to study algorithms used to detect metastases in lymph nodes. The published outcomes of the competition proved that the algorithm was more accurate than human doctors in their diagnoses.

From a legal and ethical point of view it is important to note that the patient's symptoms were obtained by the AI robot 'interviewing' the patient or by a human doctor feeding the patient's data into the AI robot. The net effect is that the robot is now in possession of sensitive patient information.

Because the robot is not a 'person' in the legal sense of the word, it does not have 'moral' instincts to guide it to treat the information in terms of the confidentiality imprimatur of a human doctor who is bound by the Hippocratic Oath.

This paper will examine other provisions which can be taken to protect the patient's confidential information, given that the robot is not a moral being which is capable of being bound by an oath.

Fundamental to the achievement of this end, we will distinguish between rights of privacy as opposed to the duty of confidentiality. Very briefly privacy relates to a person whereas

Vol. 4, No. 04; 2020

ISSN: 2581-3366

confidentiality is about information. We will also examine how to determine damages in the event of a breach of confidentiality by an AI robot.

AI Confidentiality.

1.Introduction

The doctor-patient relationship is usually based on a contract for services.[1] In order for the doctor to diagnose the patient's illness, the patient must disclose often sensitive personal details to the doctor. The patient is usually prepared to disclose these details because the patient knows this information is protected by the doctor's duty of confidentiality which arises out of the Hippocratic Oath, or a similar oath, in which the doctor has sworn not to reveal such information to anyone.[2]

A breach of this confidentiality, outside of justifications such as 'public interest'[3] or statutory obligation,[4] can result in a claim for damages by the grieved patient against the doctor.[5]

AI robots, the best known of which is IBM's Watson, are already actively employed in medical practicee.g.they are increasingly being used to make diagnoses of X-Rays and of the symptoms of cancer patients. The algorithms which drive these robots thus end up being in possession of the patient's information in the same way as a human doctor is after a consultation with a patient. The difference is that the algorithm is not a person and does not swear a Hippocratic Oath. The question to be decided is therefore how the confidentiality of the patient's information is to be protected?[6]

2. Difference between Privacy & Confidentiality.

This article focuses on a doctor's duty to protect a patient's confidential information. A patient also has a legal right to privacy. These concepts are often confused or used interchangeably. They are distinct in a legal sense and it would thus be advisable to draw a clear distinction between them.[7]

2.1 Definition of Privacy

Privacy is the state in which an individual is free from the intrusion or interruption of third parties. The word privacy refers to a condition in which a person is sheltered from public attention and observation. Every person has a right to be left undisturbed regarding his personal

[1] J A Devereux'Australian Medical Law' 3rd, 2007,p139. The Hippocratic Corpus (Books 1 & 2 of Epidemics)
[2] L. Lasagna, Hippocratic Oath – A Modern Version. 1964; Declaration of Geneva, Switzerland 1948.
[3] *W v Edgell* [1990] All ER 835
[4] Health Act 1937 (QLD) s 29, s 60.
[5] Royal Women's Hospital and Medical Practitioners Board of Victoria [2006] 15Y R at para 134, *Breen v Williams* (1996) 186 CLR 74.
[6] E AckerknechtA Short History of Medicine 1982,p55 (John Hopkins Press)
[7] Key Differences between Privacy and Confidentiality at https://keydifferences.com/difference-between-privacy-and-confidentiality.html

Vol. 4, No. 04; 2020

ISSN: 2581-3366

life and the private matters which constitute that life. In other words, an individual can create a boundary preventing third parties from accessing his private information for general use which in turn may impact unfavourably against him.[8]

2.2 Definition of Confidentiality

Confidentiality of information exists when it is intended or expected of a person to keep information which has been imparted to him or her in confidence.

Confidentiality implies the existence of trust between two parties. In other words, if party A confides information to party B on the basis of trust, it is thus expected of B, to hold the information in trust or confidence until A agrees that he may release the information.[9]

Information that is shared between a doctor and a patient and a client and a solicitor are held in trust and protected as being confidential.[10]

3. Other distinctions between Privacy & Confidentiality

3.1 Privacy is a right. Confidentiality is an agreement.

3.2 Privacy relates to a person, confidentiality to information.

3.3 Privacy places restrictions on third parties accessing the personal details of a person. Confidentiality protects an individual's information from a range of unauthorised persons.

3.4 If confidentiality is compulsory two parties have a fiduciary or trust relationship. Observing a person's privacy is voluntary, but breaking privacy can lead to claims for damages.[11]

The information which a medical robot, like IBM Watson, would glean from a patient would thus fall into the category of information protected against disclosure by the duty of confidentiality. Can a robot make such a moral judgement? How will liability be calculated for any damages occasioned by such a breach of confidentiality? I will attempt to answer these questions in the course of this article. AI robots are going to become an ever-increasing presence in the field of medicine and regulation of their activities is going to become ever more important.[12]

[8]ibid
[9]ibid
[10]ibid
[11]ibid
[12]E Ackerman 'Hoaloha Robotics Developing Socially Assistive Hardware Platform' (2013) 4 *Sept IEEE Spectrum* 'Our Robot has the benefit of knowing a user is nearby and if the user is currently looking at the robot… It also tracks the last conversation…and the history of other conversations with this user…'

Vol. 4, No. 04; 2020

ISSN: 2581-3366

4. Some existing AI health robots and their functions.

The following AI health platforms currently help physicians to be better doctors:-

4.1 IBM's Watson Health

Watson's algorithms are being trained to efficiently and quickly identify symptoms like heart disease and cancer.[13]

4.2 P.A.C.- programme assisted care.

Stanford University has been developing an AI assisted care programme, which provides an intelligent senior's wellbeing support system which will sense any behavioural changes in elderly people living alone. Their smart I.C.O 's use multiple sensors to monitor every aspect of the patient.[14]

Siri, Google Now and Cortana.

Mobile phone users can call on the above robots to respond to mental and physical health issues, thereby allowing patients to access at least a form of medical care at an early stage.[15]

4.4 'Molly' is a virtual nurse that is being developed to provide follow-up care to discharged patients, thus allowing doctors to focus on more urgent cases.

A study conducted in 2016/17 found that physicians only spent 27% of their office day on direct clinical face time with their patients, while they spent 49.2% of their office day on electronic hospital records and desk work. Eliminating record updating by using algorithms will free up much more precious time to interact with patients. Another example of time saving by AI systems is a study which proved that an AI system was able to outperform dermatologists in correctly classifying suspicious skin lesions.[16]

What we can learn from the new era of AI augmented medical practice is that analytically and logically algorithm driven robots may be able to use their skills to monitor and analyse human behaviour. However, there are certain human traits such as critical thinking, interpersonal and

[13]B. Monegain 'Florida's Jupiter Centre Becomes First US Hospital to use IBM's Watson for Oncology' *Mobile Health News* 1 Feb 2017. AL Samuel 'Some Studies in Machine Learning Using the Game of Checkers', (2000) 3 *IBM Journal of Research and Development* 210
C Ross and I Swetlitz 'IBM Pitched its Watson Supercomputer as a Revolution in Cancer Care. It is nowhere close' *STAT 5* September 2017.

[14]J Maderer' How Would You Like Your Assistant – Human or Robotic? 29 April (2013) *Georgia Tech News Centre*
Barbara Peters-Smith *'Robots and More: Technology and the Future of Elder Care'* May 27, 2013
B.Peters-Smith 'Nation at Crossroads in home care for Elders' 25 May 2013 Herald Tribune

[15] Herald Tribune Biplab Das 'A Survey on Question Answering Systems, Institute of Technology, 54-58. Barber and Molteni. *Wired*,11 November 2019, p5.

[16]K J Dreyer and J R Geis 'When Machines Think: Radiology's Next Frontier', (2017) 285 *Radiology* 713-715.

Vol. 4, No. 04; 2020

ISSN: 2581-3366

communication skills, emotional intelligence, and creativity which cannot as yet be learned by algorithms. We can thus submit that in the current phase of the evolution of AI robots their function in a medical practice or laboratory is that of an associate, rather than as a substitute for a medical practitioner.[17]

As health professionals seek to intelligently incorporate AI systems into the art of medicine, medical schools and health administration systems will have to develop and foster, in parallel, a more robust culture of statistical literacy and especially effective control and supervision of the AI robots so that the human doctor always retains ultimate control and hence fulfills the duty of confidentiality.[18]

The Australian Therapeutic Goods Administration (TGA) is aware of the current, and especially the future challenges, posed by the use of software as a medical device in its own right. The TGA has recently issued a consultation paper titled 'Software as a Medical Device' or SaMD.

A SaMD can be operated on a general computing platform which can include a mobile device. When used in this fashion it is consistent with the definition of a 'medical device' in the TPA 1989. An example of a SaMD could be an 'app' which is used to analyse medical images, or which analyses a database of medical records to assist in the diagnosis and/or treatment of a disease. A SaMD can be distinguished from software which is embedded in, and which controls a physical medical device.

Proposed Reform

The envisaged reforms proposed to address the above problems are:

Classifying SaMD Products

Medical devices are currently classified on the basis of any potential harm which they may cause to a patient where there is any interaction between a physical device and a patient. The only existing regulation of medical device software concerns software which is associated with physical devices. The regulation reads as follows:-

'If a medical device is driven or is influenced, by an item of software, the software has the same classification as the medical device'.

The problem with this regulation is that it does not capture software which is not associated with a physical device such as a SaMD where there is no interaction between a patient and a physical device because the software is actually the device.

Under the current regulatory framework SaMD products can only be classified in Class 1. This in turn means that SaMD products are not currently scrutinised for supporting evidence by the

[17] S C Shapiro 'Artificial Intelligence,' in *Encyclopedia of Artificial Intelligence* ed S C Shapiro, Vol 1, 2nd ed, 1992

[18] A Kirsch et al 'Plan Based Control of Joint Human-robot Activities' (2010) 24 *J KünstlicheIntelligenze*, 223-231

Vol. 4, No. 04; 2020

ISSN: 2581-3366

TGA. Under the proposed new classifications all SaMD products will require regulatory oversight. It is submitted that the oversight should also extend to the protection of the confidentiality of all patient information.

5. AI will provide a useful function.

In 2016 the world Economic Forum named open AI ecosystems as one of the 10 most important emerging technologies. There is already an unprecedented amount of data available which will be better analysed due to the ever-improving natural language processing abilities of algorithms. This adds up to the fact that AI will become increasingly indispensable to consumers. This is nowhere better illustrated than in the medical and health care field where there is a treasure trove of information to be extracted and utilised from the millions of potential medical records held in thousands of hospitals. If these patient medical records are deep mined by algorithms, they have the ability to generate masses of information aimed at improving the diagnosis of many little-known illnesses.[19]

The principles of genetic algorithms have already been used to predict the outcome for critically ill patients with lung cancer and melanoma. They have also been used in the computerised analysis of mammographic microcalcification, and MRI segmentation of brain tumours.[20]

There is no question regarding the useful contribution which AI robots can make. However when these robots are loaded with masses of information they pose an enormous risk for breaching the rights to privacy and the duty of confidentiality owed to the patients whose medical records are now in their databases. How is the legal system going to respond to breaches of this information?[21]

6. Robots, Data Collection, and the Circle of Confidentiality.

The collection and recording of a patient's data in medical files is a prerequisite for assuring the quality, sufficiency and continuity of proper medical treatment. The treatment in turn may not be confined to one doctor or one hospital and it may be necessary for other healthcare professionals to have access to the records which chronicle his treatment. This information enables those involved with the current phase of treatment to exchange information, opinions and knowledge to conclude the current therapy.[22] When consent is given by the patient to provide the requested

[19] Ed Pilkington 'Googles secret cache of medical data includes names and full details of millions- whistleblower' 13 Nov 2019 *The Guardian.*

Google's Project Nightingale involves the secret transfer of the personal medical data of up to 50 million Americans held by Healthcare providers Ascension to Googles cloud. The data includes full personal details including name and medical history.

[20] S E Dilsizian and E L Siegel 'Artificial intelligence in medicine and cardiac imaging: harnassing big data and advanced computing to provide personalized medical diagnosis and treatment' (2014) *Current Cardiology Reports,* Springer,

[21] R Poplin 'Prediction of Cardiovascular Risk factors from Retinal Fundus photographs Using Deep Learning' (2018) 2 *Nature Biomedical Engineering,* 158

[22] S H Park and K Han, 'Methodologic guide for evaluating clinical performance and effect of artificial intelligence technology for medical diagnosis and prediction' (2018) *Radiology.pubs.rsna.org and web of Science:45*

Vol. 4, No. 04; 2020

ISSN: 2581-3366

information it is presumed that all personal information provided for the initial diagnosis will also be available to other doctors, to whom he subsequently gives consent to treat him, without such access constituting a breach of confidentiality. However, such access is subject to a proviso that the sensitive information in that patient's record remains within the 'circle of confidentiality' and that reckless revelation of any aspect of the patient's data will be prevented by the imposition of the obligation of professional secrecy or confidentiality.[23]

The same situation can and probably will arise where an AI platform is part of the team of doctors which is gathering or using patient data in that 'circle of confidentiality'. The information locked into the robot's database would be under the supervision of the clinic which owns the robot and access could only be obtained via the clinic manager. This protocol is probably best suited to secure the confidentiality of the information held by the AI robot.[24]

7. <u>Patient information in the Robot world.</u>

Robots will not necessarily be isolated from contact with other robots in the general field of medicine. Where a patient is subject to multidisciplinary treatment and therapies, robots in Hospital A will more than likely be in contact with robots at Hospital B or Medical Clinic C to exchange information in order to best serve the interests of patient X. Where such inter-robot contact takes place, confidential patient information can be exposed to the risk of disclosure. Article 7 of the EU Charter of Fundamental Rights offers protection to rights of self-determination via the General Data Protection Regulation (GDPR) which applies to the processing of personal data in parallel to medical law and ethics. Personal data means 'any information relating to an identified or identifiable natural person.' Patient data which is not only shared with health care professionals (HCP) but also new data which is processed by AI providers, such as a birth control app used by a patient, will normally qualify as 'special category personal data'. For this reason, the processing of health data will require 'explicit consent' from the data subject provider.[25]

The GDPR in turn defines ‘regular’ consent as any freely given, specific, informed and unambiguous expression of agreement with the respective data processing. Where a robot is in a position to make automated decisions, regulations in the form of Articles 13(i) (f), 14 (1) (9) and 15 (1) (12) in conjunction with Article 22 GDPR are applicable.[26] This means that the patient who has been subject to an AI diagnosis can ask to be provided with ‘meaningful information’ about the logic

[23]E J Topol ‘High Performance Medicine: The Convergence of Human and Artificial Intelligence’ (2019) 24 *Nature Medicine* 44

[24]ibid

[25]GDPR Portal: *Site Overview,* EU GDPR, https://www.eugdpr.org

[26]B Goodman and S Flaxman ‘EU Regulations on Algorithmic Decision Making and a Right to Expression’ at ar XIV: 1606. 08813 [stat. ML] 28June,2016.

Vol. 4, No. 04; 2020

ISSN: 2581-3366

involved in the robot's diagnosis. Given the complexity involved in the making of an algorithmic decision, providing an understandable explanation would be challenging.[27] The process of robotic diagnosis and the dispensing of meaningful information again emphasises that the confidentiality of patient information, which may breach this situation, should be managed by a human doctor exercising control over the AI robot.

8. Protection of patient confidentiality against the negligence of robots.

There is no comprehensive protection regime as yet applicable to AI robots functioning in medical practice. The regulation of medical devices is vital to ensure that safe and efficient controls exist over AI systems within healthcare. A practical workable system for allocating liability to robots is also vital for robotics to be accepted as useful assistants in health care.[28]

8.1 Strict Liability

Considerable doubt can be raised whether the overall risk profile (including protection of confidentiality) justifies opening the Product Liability Directive to encompass non-embedded software across the health care industry *in general*. An alternative basis in terms of which to ground liability could thus be achieved by applying the doctrine of *strict liability* within the sector. This would apply mainly in those areas of medical practice in which AI platforms are being tested,thus exposing patients to a breach of their confidential information.[29]

8.2 Negligence

The E.C. is currently evaluating whether its existing product liability frame-work is competent to deal with the so-called 'emerging digital technologies', as for example AI and advanced robotics.[30] The main concern around AI centres on the unpredictability of the self – learning capabilities of certain AIalgorithms. It is feared that these systems could develop unethical traits and even illegal behaviours which were not foreseeable by their human developers, a fact which could absolve them of their liability. An oft cited example is Microsoft's chatbox 'Tay' which learned racist and sexist language. This forced its withdrawal on launch day. Under a negligence

[27]S Wachter et al 'Why a Right to Explanation of Automated Decision Making Does Not Exist in the General Data Protection Regulation' *(2017) 7 (2) Int's Data Priv L p.76-99*

[28]G Barber and M Molteni 'Google is slurping Up Health Data – and it Looks Totally Legal 11 Nov 2019, *'Wired'* Under the Health Insurance Portability and Accountability Act, better known as HIPAA, patient records and other medical details can be used only to help the covered entity carry out its healthcare functions; The Federal health care privacy law allows hospitals access to share information with its business associates (Google) without obtaining patient consent. Thus, Google's services could be regarded as 'quality improvement' which is one of HIPAA's sanctioned uses for business associates. Google would however have anonymized the information before it could use it to develop and train machine learning models for commercial sale.

[29]A. D. Selbst and J Powles 'Meaningful Information and the Right to Explanation' (2017) 7 *International Data Privacy Law*, 233, 234.

[30]T Simonite 'When Bots Teach Themselves to Cheat' 8 Aug 2018 *Wired*

Vol. 4, No. 04; 2020

ISSN: 2581-3366

regime there might be limited space for a developer to argue that such 'self-learning' would be beyond what they could reasonably control.[31]

It is however possible to avoid a 'Tay-like disaster' by rigorous testing, by 'freezing' the algorithm and by disabling its 'online learning' capacity. It is only where the above measures are omitted by the developers of the algorithm that a strong indication for negligence could exist.[32]

Under the existing product liability law, AI platforms which develop such unpredictable traits would not shelter the AI developer from liability, if over time their algorithms deviated from the safety standards which may reasonably be expected by a user of the platform. This would of course also be true, if by a process of deep learning, the AI robot learned to communicate confidential patient information to other AI platforms on an unauthorised basis.[33]

With the problems AI robots present it might be tempting to decide to solve the problem by declining to use the technology. However, with the rapid strides the technology is making, especially via apps and cloud computing services, these robots are demonstrating that they can and do exceed the performances of human health care providers. As a result, doctors could find themselves in the analogous position that they could incur liability via their omission to use available robot diagnosis.[34]

The transitional phase of the technology, which is where we now find ourselves, is probably the period in which to expect the greatest potential for negligence claims to be brought i.e. when the technologies are gaining traction, but all the gremlins have not yet been eliminated. [35]

[31]E Steven et al. 'Artificial Intelligence in Medicine and Cardiac Imaging: Harnessing Big Data and Advanced Computing to Provide Personalised Medical Diagnosis and Treatment' (2014) *Current Cardiological Report* 16: 441

[32]J Vincent 'Twitter taught Microsoft's AI Chatbox to be a racist Asshole in less than a day',24 May. *The Verge*

[33] A B Laakmann 'When should Physicians be Liable for Innovation' (2015) 38*Cardozo Law Review*, 913

[34]T. Yang and R Silverman, 'Mobile Health Applications: The Patchwork of Legal and Liability Issues Suggests Strategies to Improve Overnight' (2014) 33 (2) *Health Affairs* 222-27

[35]House of Lords, Select Committee on Artificial Intelligence, Report of Session 2017-19, AI in the UK: ready, willing and able? 16 April 2018 (House of Lords, 2018)

House of Commons Science and Technology Committee, Algorithms in Decision Making. Fourth Report of Session 2017-19, 13 September 2016, House of Commons (2016)

European Commission, A Staff Working Document, Liability for emerging digital technologies, Brussels, 25.4.2018 SWD (2018) 137 Final (EC Staff Working Document on Liability, 2018.

High-Level Expert Group on Artificial Intelligence, Draft Ethics Guidelines for Trustworthy AI, Brussels 18 December 2018.

European Parliament, Committee on Legal Affairs, Report with recommendations to the Commission on Civil Law Rules on Robotics, Brussels, 27 January 2017. (European Parliament, 2017)

Executive Office of The President, National Science and Technology Council Committee on Technology.

See *Wired* Supra, Google has also contracted with The Mayo Clinic to move its vast collection of patient records onto the Google Cloud. From this secure location Google has been granted limited access to anonymised patient information with which to train its algorithms.

Vol. 4, No. 04; 2020

ISSN: 2581-3366

For the AI development industry to negotiate this period safely, doctors and the patient public require unambiguous guidance to be asserted over the industry by regulation.[36]AI robots require final approval from the HCP and they in turn bear responsibility for their decision. On the other hand, AI producers bear the liability for the safe and efficient functioning of their technologies.[37] Doctors and hospitals who purchase and use AI robots should limit the use of the devise within the risk, design and label constraints. Exceeding their limits would amount to negligence. The risk standard which an AI robot should conform to, prior to release in practice by its producers, is that the devise should be proved to be at least as safe and effective as conventional human decision making. Examples of such decisions would be the interpretation of X-Rays or a cancer diagnosis. An AI robot should be programmed in such a way that it is barred from releasing

patient information without an overriding function by a supervising doctor. Such a move would ensure confidentiality by the protection of patient information.[38]

8.3 Personhood.

Both Civil and Common Law have conferred a form of personhood on non-persons e.g. the recognition of Companies as persons. This allows the company to operate within the confines of the law as a legal person capable of suing and being sued. This concept, which was devised by Roman Law, is now entrenched in the legal systems of most countries by way of company legislation. This concept differs from the actions of robots, in that companies act via their officers, whereas AI robots act of their own volition. The action of a company director which infringes the law can therefore be judged by the same criteria applicable to ordinary humans. For example, were the director's actions reasonable[39] or were they unlawful? The same criteria cannot be applied to the unilateral actions of robots.

The law is still grappling with the concept of how to regulate advanced robots and more especially how to legally evaluate their actions and interactions with patients in the field of law, so as to compensate for injuries caused, or to prevent potential harms arising from their actions.[40]

A proposal that has been advanced is whether it would be feasible to grant legal personhood to AI robots, on the basis that AI shares comparable intellectual capacities with humans more so than do other natural beings, albeit that AI has reduced capabilities by comparison to humans. The logic and impulses displayed by AI are alien to those of humans,[41] resulting in their actions often being too random and unpredictable by comparison to our own. This is therefore one

[36] Royal Society, 'Machine Learning: The Power and Promise of Computers that learn by Example' *2017 Royal Society*

[37]S Wachter et al 'Transparent, Explainable and Accountable AI for Robotics' (2017) 2 (6) *Science Robotics* 6080

[38]L F Friedman and Reuters, 'IBM's Watson Computer Can Now Do in a Matter of Minutes What it takes Cancer Doctors Weeks to Perform' *Business Insides* 5 May, 2015.

[39] J Chung and A Zink "Hey Watson – Can I Sue you for Malpractice? Examining the liability of Artificial Intelligence in Medicine'. (2018) 11/2 *Asia Pacific Journal of Health Law and Ethics* S1, 76/77

[40]ibid

[41] R Abbott, 'The Reasonable Computer: Disrupting the Paradigm of Tort Liability', *George Washington Law Review* (2018) 861, p2.

Vol. 4, No. 04; 2020

ISSN: 2581-3366

reason why AI robots should not enjoy personhood as they lack a form of intelligence which is compatible to human intelligence. The area of law which is least suitable to answering the actions of AI robots is within the branch of Torts, where one of the criteria for determining the negligence of a party's actions is based on whether their actions deviated from those of the so called 'reasonable man'. No test of the 'reasonable robot' has yet been devised and it is therefore unlikely whether either the common law or civil law of torts could be applied to judging the actions of AI robots.[42]

It is submitted that anointing an AI robot with personhood would result in a gross distortion of the law in order to accommodate the robot within the normal/natural confines of the law of torts. At the end of the day, a legal actor is always a human being who plays an acknowledged legal role, either as a physical person or as an executive member of a non-human legal entity which is treated as a person for certain legal purposes.[43] Human beings are always the final decision makers for legal persons, and they must be aware of the consequences of their actions. The entity's liability will largely be determined by the legality and/or reasonableness of the human's actions on its behalf.

The assignment of legal personhood to AI robots can thus be described as 'non-natural'. The attachment of legal personhood to robots would undermine the concept of legal personhood as it now exists in the law. A robot is capable of actions e.g. it could gather confidential information from a patient. However, it may also disclose the information without authorization. Should this happen there would not be a real person whose actions are indictable according to accepted principles of law regulating the robot's actions.

To sum up, ascribing personhood to an AI robot will not be a natural or reliable form of legal protection for a patient's confidential information.

Human beings are always the final decision makers for legal persons, and they must be aware of the consequences of their actions. The entity's liability will largely be determined by the legality and/or reasonableness of the human's actions on its behalf.[44]

The assignment of legal personhood to robots would undermine the idea of legal personhood as it now exists. Even though the robot can act e.g. it can gather confidential information from a patient, and although it may disclose the information without authorization there will not be a real person whose actions are indictable according to accepted principles of law.[45]

---

[42] George L Priest 'Satisfying the Multiple Gods of Tort Law' (1988) 22 *Valparaiso University Law Review* 643, 648.

[43]D Schŏnberger 'Artificial Intelligence in Healthcare: a critical analysis of the legal and ethical implications (2019) 27 *International Journal of Law and Information Technology* 173, 201-203

[44]P Danzon, Medical Malpractice Theory, Evidence and Public Policy, H. VP 1985 p 1

[45]R Abbott 'The Reasonable Computer: Disrupting the Paradigm of Tort Liability' (2018) 86 (1) *George Washington Law Review* 3-5

DC Vladeck 'Machines Without Principles: Liability Rules and Artificial Intelligence' (2014) 89 *Washington Law Review.*

Vol. 4, No. 04; 2020

ISSN: 2581-3366

The alternative and more radical view is that granting legal personhood to an AI robot does not foreshadow an imminent uprising of intelligent machines. Legal personhood is merely a pre-existing legal fiction used to hold natural persons, as well[46] as artificial persons, accountable. Prof Michael Dorf has expressed his view as follows: -

'Personhood is a legal status for which sentience is neither a necessary nor a sufficient condition. It is not a necessary condition because as a matter of law artificial entities like corporations can have personhood.'[47]

To sum up, ascribing personhood to an AI robot will not be a natural or reliable form of legal protection for a patient's confidential information.

8.4 Consulting Physician

Can an AI robot (e.g. Watson) be classified as a 'consulting physician'? Would such a classification provide appropriate protection for confidential information?[48]

What is the legal position of a consulting physician vis-à-vis a patient? In current legal terms a consulting physician does not incur a legal duty of care to a patient, because this category of physician does not actually interact with the patient.[49] Consulting physicians fulfil the role of providing the advice they are contracted to provide. They are provided with medical evidence gathered by the patient's doctor and they then provide a diagnosis to the patient based on an

interpretation of that evidence. The consultant never examines or talks to the patient and does not establish a physician–patient relationship which can give rise to a cognisant medical malpractice claim, like for example, breach of confidence.[50]

If we use the best known most developed AI robot, Watson, as an example then it is apparent that Watson exceeds the usual scope of a consulting physician, because it can actually 'examine'

patients via access to the patient's medical history, phenotype and more recently their genomic data.[51] In addition to this Watson is advertised on the IBM website in the following terms;

'If you are a patient interested in Watson Genomics from Quest Diagnostics [which utilizes genetic sequencing capabilities to help oncologists identify personalised treatment regimens for

[46] See in CorinFaife "When Does an Artificial Intelligence Become a Person?' *Medium* 18 October 2016.

[47] S Wachter et al 'Transparent, Explainable and Accountable AI'. in *Robotics* (2017) 2 (6) at 1062 p 1049

[48] Science Robotics 6080 J.S. Allain, 'From Jeopardy to Jaundice': The Medical Liability Implications of Dr Watson and other Artificial Intelligence Systems (2013) 73 *Louisiana Law Review.*

[49] *Goodwill and British Pregnancy Advisory Service* (1996) 2 ALL ER 161

[50] *Caparo Industries plc v Dickman* [1990] UKHL [1990] 2 AC 605.

[51] D Murgah 'Columbia Doctors Turn to IBM's Watson for Patient Diagnosis, Clairvoyance' *ENGADGET.Com* (24 March 2011) http://www.engadget.com

Vol. 4, No. 04; 2020

ISSN: 2581-3366

their patients], speak with your oncologist to determine if this technology might be right for you'.[52]

It is easy to deduce that the wording of the above advertisement underplays the role that Watson the robot plays in treating a patient and that in fact it supersedes that of the visual 'consulting physician' and is more akin to being a member of the team of physicians treating the patient.[53]

Seeking to attach liability to Watson via the product's liability regime is likewise unsatisfactory as Watson does not fall into the category of a typical medical device which performs a monitoring function, or a treatment function like a pacemaker once it is surgically implanted in a patient. Watson's algorithmically based intelligence allows it to function at a level more akin to a human doctor by actually interpreting and analysing patient information.[54]

Trying to recover damages against Watson for medical negligence based on a product liability basis is unlikely to succeed for the following reasons:-

(a) The primary function of hospitals and other health care providers is to provide services rather than to sell goods and for this reason they have traditionally been deemed to be immune from product liability claims.[55]

(b) Even if Watson were to qualify as a medical device, its patients would not be able to sue Watson's designer or manufacturer directly because of the doctrine of the 'learned intermediary' which essentially holds physicians responsible for assessing the risks and benefits of using a specific device (Watson) on a given patient.[56]

(c) Because software has not generally been categorised as a form of product liability it would mean that any actions would be restricted to blatant hardware malfunctions e.g. where Watson shuts down while monitoring and managing life support systems, which then result in the patient's death.[57] Therefore if products liability law did expand to include software it would create difficulties regarding the onus of proof e.g.a plaintiff would be hard put to distinguish whether the damage was occasioned by a hardware or software problem.[58]

The problem outlined above might tempt the legislature to categorise Watson as a legal person in order to apply well established provisions of liability law to Watson's actions. However, as we

[52] J Fingas IBM's Watson A I saved a woman from Leukemia' 7 August,2016, *Engadget.*

[53]CEA Karnow 'The Application of Traditional Tort Theory to Embodied Machine Intelligence' (2016) *Robot Law* 51. S 2

[54]B Mesko 'What is Using IBM Watson in Everyday Medicine like?' *Medical Futurist*http://medicalfuturist.com. Chung and Zink op cit 75, 76.

[55] Allain op cit 1062

[56]W N Price 'Medical Malpractice and Black Box Medicine' in *Big Data Health Law and Bioethics* I Cohen et al eds. (CUP 2018)

[57] Jessica S. Allain 'From Jeopardy to Jaundice - The Medical Liability Implications of Dr Watson and other Artificial Intelligent Systems' (2013) 73 *Louisiana Law Review* 1052

[58]ibid

Vol. 4, No. 04; 2020

ISSN: 2581-3366

discussed supra this 'solution' creates its own problems in that it will dist or tort law in order to 'fit' Watson into its ambit.[59]

It is therefore submitted that the most practical solution for regulating Watson (and similar AI platforms) is to make their actions subject to the supervision of a human doctor. The latter will then in turn be covered by fidelity insurance which will extend to both the actions and diagnosis of Watson and its human supervisor.[60]

It is submitted that liability should be attached to Watson's actions on the same basis as that for human doctors viz under the law of medical malpractice, except that the negligence will be ascribed to the human doctor who supervises Watson and who uses his judgement to scrutinise and approve, or reject, Watson's diagnosis and treatment proposals.[61]

Such an approach will preserve the legal status quo regarding the liability of doctors for malpractice, and the law will not have to resort to elaborate devices to facilitate Watson as a legal person for purposes of litigation.[62]

A consistent human supervisory oversight of Watson's practice will also ensure that a patient's confidential information is protected by the moral judgement of a human doctor whose actions are ethically based and guided by the Hippocratic Oath or similar.[63]

Based on the discussion above I would thus submit that AI robots like Watson have a vital role to play in the future of medical care, but that their role should be confined to supplementing the role of human doctors rather than replacing human expertise. This combination of the analytical and problem-solving capabilities of machines with the moral judgments of humans will provide a formidable partnership for serving the needs of patients in the 21st Century and beyond.[64]

9. Conclusion

Regardless of the laws or regulatory systems chosen to apply to robots, they are going to have a significant impact when it comes to the data protection and confidentiality of patient information. The health data which these increasingly autonomous robots would generate, share and rely on,

[59]C. Ross and I. Swetlitz 'IBM to Congress: Watson will transform Health Care, So Keep Your Hands off our Supercomputer' *STAT* News 4 October, 2017.

[60]M. Vansuch et al 'Extent of Diagnostic Agreement Among Medical Referrals' (2017) 2 *J. of Evaluation of Clinical Practice'* at 2.

J T james 'A New Evidence-based Estimate of Patient Harms Associated with Hospital Care', (2013) 9 *J of Patient Safety* 122-126

[61] '*Cooper v Royal United Hospital Bath NHS Trust* (2004) All ER (D) 51

See also *Simms v Simms* [2002] 2 W L R 1465

[62] See Supra.

[63]G.Laurie et al Mason and McCall Smith's *Law and Medical Ethics,* 10th, (2016) 4. 112

[64]ibid

Vol. 4, No. 04; 2020

ISSN: 2581-3366

would represent a far more complete and sensitive account of a patient's health than is currently found in medical and health records.[65]

The key to protecting a patient's confidential information, which is held by a Watson-like robot, hinges on the status which the law attaches to Watson. I have submitted in this paper, that I would not favour conferring legal personality on Watson, as although this may solve one problem, i.e. subjecting Watson to the regime of medical negligence and tort law, it would come at the cost of unsettling the well established principles of this branch of law. It is submitted that this is too high a price to pay.[66]

I therefore submit that instead of bastardising the law by attaching legal consequences to the actions of a robot per se and trying to find unlawfulness or negligence in the acts of a machine, it is far neater and more logical to attach the liability of, for example, the breach of confidentiality by a robot, to the failure of a human physician to properly manage the acts of a Watson- like robot.[67] Following this legal route for allocating liability to the acts of a robot is far more predictable and will not involve any complex legal gymnastics to attach blame to a robot person.[68]

Practitioners who use robotic assistance in their practices should be compelled to buy medical indemnity insurance to cover liability incurred by a robot.[69] Will the additional insurance costs price Watson out of the market? The medical practitioner will improve his productivity by using a robot in his practice. This in turn will increase his productivity, which will in turn adequately pay for the increased insurance premiums. Therefore, the doctor, his partners and the medical practice will make higher profits. Most importantly issues regarding negligence by the robot will be easily assigned.[70] A win-win situation.

Technologies like Watson provide a glimpse into how AI can supplement rather than replace human expertise. A combination of the high-speed problem-solving capabilities of machines, in tandem with the moral judgment of humans, places us on the verge of being able to service more patients with fewer resources and thus improve the lives of many more people.[71] The proposed human/robot partnership will also better protect the confidentiality of a patient's case record and other private disclosures to the doctor-robot partnership.

[65]MBM Destephe et al 'Walking in the Uncanny Valley: importance of the attractiveness on the acceptance of a robot as a working partner'. (2015) 6 *Frontiers of Psychology* 1-11

[66]E. Palmerini et al, Robolaw: Guidelines on Regulating Robotics 22 September,2014. at http://www.robolaw.eu/Robolaw_files

[67]D. Schönberger op cit 200-2002

[68]D. Simshaw et al 'Regulating Health Care Robots: Maximising Opportunities While Minimizing Risks' (2019) 23 *Richmond Journal of Law and Technology* 36-38

[69]ibid

[70] Zapursek op cit 121-128

[71] Ibid.