Catholic University Journal of Law and Technology

Volume 31
Issue 2 *Spring 2023*

Article 8

2023

Establishing the Legal Framework to Regulate Quantum Computing Technology

Kaya Derose
Catholic University of America (Student)

ESTABLISHING THE LEGAL FRAMEWORK TO REGULATE QUANTUM COMPUTING TECHNOLOGY

Kaya DeRose[*]

It is no secret that technology is advancing at lightning speed, and as technology advances, so do our computers. Just how quickly are these changes occurring, and what does that mean for our standard devices, such as laptops, cell phones, or even the computer in a vehicle? Soon, we will say goodbye to computers that analyze information in a binary way, using either one or zero, and instead begin using devices that can process information using one and zero simultaneously.[1] The global quantum computing market is projected to grow exponentially between 2021 and 2026, and professionals everywhere are starting to recognize and discuss the societal implications of quantum computing technology.[2]

Lawyers and policymakers should recognize this change too, and proactively consider what legal framework might best apply to regulate this new area of technology. This is important particularly considering the potential threats to security breaches, data leaks, and loss of information it poses to cybersecurity

[*] *Juris Doctor* Candidate, Columbus School of Law, 2023; *Bachelor of Arts*, University of Central Florida, 2020; *The Catholic University Journal of Law and Technology*, Managing Editor, 2022-2023, Associate Editor 2021-2022.

Thank you to Christopher Savage for his assistance and guidance when drafting this article. Thank you to my family and friends for their constant support during this process. Lastly, thank you to JLT Vol. 31 for all your work on my article, as well as the other articles this year.

1 Jake Frankenfield, *Quantum Computing: Definition, How It's Used, and Example*, INVESTOPEDIA, https://www.investopedia.com/terms/q/quantum-computing.asp (Aug. 28, 2022).

2 *The Worldwide Quantum Computing Industry Is Expected to Reach $1.7 Billion by 2026*, CISION PR NEWSWIRE (Feb. 16, 2021), https://www.prnewswire.com/news-releases/the-worldwide-quantum-computing-industry-is-expected-to-reach-1-7-billion-by-2026—301229132.html [hereinafter CISION]; *see generally In re* Huping Hu, 848 F. App'x 416 (Fed. Cir. 2021).

and privacy.[3] Appropriate regulation, such as IP protection and antitrust regulation, will enable legal and non-legal professionals alike to enjoy the benefits of quantum computing technology by avoiding the inevitable downfalls that would occur if it were to remain unregulated.

The concept of "quantum computing" originated from the cornerstone of physics that underlies chemistry and is integrally connected to biology – "quantum mechanics."[4] As physics evolved from the late Nineteenth Century through the early Twentieth Century, scientists encountered puzzling phenomena that could not be explained by then-existing "classical" scientific theories.[5] Instead, scientists discovered that they needed an improved understanding that could handle the idea that some physical phenomena were inherently uncertain.[6] The result was quantum mechanics. The idea of quantum *computing* arose in the 1980s, when computer scientists realized that certain computational problems could be solved more efficiently with "quantum algorithms than with their classical counterparts."[7] Quantum computing, at a high level, is an "area of computing focused on developing computer technology based on the principles of quantum theory."[8] Quantum theory is "the theoretical basis of modern physics" that explains the nature of our reality.[9] In 2018, Google took quantum computing a step further and made an astounding breakthrough that has led to the quantum computing technological advances we are seeing today.[10]

The United States has taken certain preliminary measures, including technological institutions and agencies, to jumpstart exploration of the regulation of quantum computing to ensure protection for both the creators and

---

3 Scott Buchholz et al., *The Realist's Guide to Quantum Technology and National Security*, DELOITTE (Feb. 6, 2020), https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html.

4 Amit Katwala, *Quantum Computing and Quantum Supremacy, Explained*, WIRED (May 3, 2020), https://www.wired.co.uk/article/quantum-computing-explained.

5 *What Is Quantum Physics?*, CALTECH, https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-physics (last visited Apr. 3, 2023).

6 Katwala, *supra* note 5.

7 Frankenfield, *supra* note 2.

8 *Id.*

9 Ivy Wigmore, *Quantum Theory*, TECHTARGET, https://whatis.techtarget.com/definition/quantum-theory (last visited Apr. 3, 2023).

10 Edd Gent, *How Quantum Computers Can Be Used to Build Better Quantum Computers*, SINGULARITY HUB (Oct. 4, 2021), https://singularityhub.com/2021/10/04/how-quantum-computers-can-be-used-to-build-better-quantum-computers/ [hereinafter Gent, *Better Quantum Computers*].

future users of the technology.[11] However, many important questions will remain under consideration in light of the commercialization of quantum computers that is expected within the next five years.[12] With such growth, it is advisable to create flexible standards to account for rapid changes in technology, in conjunction with bright-line rules governing the use of quantum computing, and some form of global regulation may be the best avenue.[13] Existing regulatory regimes may assist in creating regulations that deal specifically with the capabilities of quantum computing. For example, the General Data Protection Regulation, the European Union's comprehensive data privacy law, may provide guidance.[14] In the area of intellectual property ("IP"), questions arise as to whether developments in quantum computing should be protected using patent, copyright, or trade secret law.[15] For example, it may be appropriate for the duration of IP protections for quantum computing technology to be shorter than the protections that exist today, to account for the rapidly changing nature of that technology.[16] Shorter periods of IP protection could result in concentration of market power, signaling the imperative to invoke antitrust

---

11 *See generally* Brian Fung & Alex Marquardt, *Senators Draft Bill that Would Require Many Entities to Report Cyber Breaches Within 24 Hours*, CNN POL., https://www.cnn.com/2021/06/16/politics/bill-report-cyber-breach-24-hours/index.html (June 17, 2021); Inyoung Park, *Current Effort to Combat Potential Danger of Quantum Computing*, WAKE FOREST L. REV. (Oct. 5, 2021), http://www.wakeforestlawreview.com/2021/10/current-effort-to-combat-potential-danger-of-quantum-computing/; Ali El Kaafarani, *Four Ways Quantum Computing Could Change the World*, FORBES (July 30, 2021), https://www.forbes.com/sites/forbestechcouncil/2021/07/30/four-ways-quantum-computing-could-change-the-world/?sh=2afb58a44602; Agnese Smith, *Why Law Firms Need to Worry About Quantum Computing*, CANADIAN BAR ASS'N (Dec. 7, 2018), https://nationalmagazine.ca/en-ca/articles/law/access-to-justice/2019/why-law-firms-need-to-worry-about-quantum-computin.

12 CISION, *supra* note 3.

13 Monica Zent, *INSIGHT: Quantum Computing–A Blueprint for a Proactive Public Policy, Legal Framework*, BLOOMBERG L. (Dec. 16, 2019), https://news.bloomberglaw.com/tech-and-telecom-law/insight-quantum-computing-a-blueprint-for-a-proactive-public-policy-legal-framework.

14 Simon Fogg, *What Is GDPR? The Basis of the EU's General Data Protection Regulation*, TERMLY, https://termly.io/resources/articles/what-is-gdpr/ (May 6, 2022); Felix Sebastian, *GDPR in the US: Requirements for US Companies*, TERMLY (June 21, 2019), https://termly.io/resources/articles/gdpr-in-the-us/.

15 Ben L. Wagner & Gerar Mazarakis, *How to Protect Quantum Computing Innovations with IP Rights*, BLOOMBERG L. (Aug. 13, 2021), https://news.bloomberglaw.com/ip-law/how-to-protect-quantum-computing-innovations-with-ip-rights-5.

16 Mauritz Kop, *Regulating Transformative Technology in the Quantum Age: Intellectual Property, Standardization & Sustainable Innovation*, STAN.–VIENNA TRANSATLANTIC TECH. L. F. (Oct. 7, 2020), https://airecht.nl/blog/2020/regulating-transformative-technology-in-the-quantum-age-intellectual-property-standardization-sustainable-innovation [hereinafter Kop, *Regulating Transformative Technology*].

principles to mitigate this risk.[17]

This comment will focus on quantum computing technology and explain the importance of establishing a legal framework for its regulation. It will explore beneficial measures for lawyers and policymakers to implement when creating a regulatory legal framework for this technology. To achieve this objective, it is helpful to define what quantum theory is, understand what quantum computing means, and identify potentially applicable regulations as quantum computing technology is commercialized. Lastly, this comment will analyze proactive measures that governments, agencies, and institutions have taken to regulate this developing technology; identify deficiencies in these preliminary measures; discuss the benefits and repercussions of this technology in the legal field; and consider alternative regulatory measures and whether they will benefit or stifle technological innovation.

I. A GLIMPSE INTO QUANTUM COMPUTING – MORE THAN JUST A SCIENCE-FICTION PLOTLINE

A. Origins of Quantum Theory

Quantum theory poses deep questions about the nature of physical reality. According to quantum theory, a wide range of physical events exist in a "superposition" of multiple states until they are measured.[18] Scientists have accepted two main interpretations of what quantum theory suggests about this kind of situation: the "many-worlds," or "multiverse," interpretation, and the Copenhagen interpretation.[19] The many-worlds interpretation posits that there are multiple worlds, or universes, which exist "in parallel at the same space and time as our own."[20] For any possible consequence of any act or action, "the universe splits to accommodate each one."[21] The Copenhagen interpretation, proposed by Niels Bohr, does not call for a multiplying cascade of separate universes, but instead essentially states that reality doesn't exist until it is

---

17 *Id.*; Mauritz Kop, *Quantum Computing and Intellectual Property Law*, 25 BERKELEY TECH. L.J. 101, 109 (2021), https://law.stanford.edu/wp-content/uploads/2021/06/Mauritz-Kop_Quantum-Computing-and-Intellectual-Property-Law_BTLJ.pdf [hereinafter Kop, *Quantum Computing*].

18 Wigmore, *supra* note 10.

19 *Id.*

20 Lev Vaidman, *Many-Worlds Interpretation of Quantum Mechanics*, STAN. ENCYCLOPEDIA OF PHIL., https://plato.stanford.edu/entries/qm-manyworlds/ (Aug. 5, 2021).

21 Josh Clark, *How Quantum Suicide Works: The Copenhagen Interpretation*, HOWSTUFFWORKS, https://science.howstuffworks.com/innovation/science-questions/quantum-suicide4.htm (last visited Apr. 2, 2023).

measured.[22] This concept is illustrated by the well-known thought experiment of Schrödinger's Cat. You place a living cat in a thick lead box.[23] You know the cat is alive.[24] But, when you throw in a cyanide vial and seal the box, you are unsure if the cat is alive, or if the capsule has broken and the cat is dead.[25] Due to this uncertainty, the cat is simultaneously dead and alive, "according to quantum law – in a superposition of states."[26] Under the many-worlds interpretation of quantum theory, there is one universe where the cat is dead and a different, otherwise equivalent parallel universe where the cat is alive.[27] Under the Copenhagen interpretation, the cat is neither dead nor alive until its state is observed.[28]

There are three principles that underlie quantum information science: superposition, entanglement and observation.[29] "Superposition" describes the ability of a particle to exist across various possible states at the same time.[30] Quantum "entanglement" applies to a scenario where two or more particles are linked in a way that makes it impossible for them to be independent of one another, even if there's a great distance separating them.[31] Both superposition and entanglement exist only as long as the quantum particles aren't measured or observed.[32] "Observing" the quantum state produces information but leads to the collapse of the system, called "decoherence" – in which the cat is either dead or alive.[33]

B. Quantum Computing Explained

With this background, we now dive deeper into how exactly quantum computing works. Computers today use binary arithmetic: they operate on information representing one of two values: off, represented by a zero, or on, represented by a one.[34] The state of a particular location in the computer's

---

22 Wigmore, *supra* note 10.

23 Joshua Rapp Learn, *Schrödinger's Cat Experiment and the Conundrum that Rules Modern Physics*, DISCOVER (May 5, 2021), https://www.discovermagazine.com/the-sciences/schroedingers-cat-experiment-and-the-conundrum-that-rules-modern-physics.

24 *Id.*

25 *Id.*

26 Wigmore, *supra* note 10.

27 Vaidman, *supra* note 21.

28 Wigmore, *supra* note 10.

29 Buchholz et al., *supra* note 4.

30 *Id.*

31 *Id.*

32 *Id.*; Wagner & Mazarakis, *supra* note 16.

33 Buchholz et al., *supra* note 4; Wagner & Mazarakis, *supra* note 16.

34 *How Do Quantum Computers Work?*, SCIENCEALERT, https://www.sciencealert.com/quantum-computers (last visited Mar. 31, 2023).

memory being on or off is called a "bit."[35] Regular computers use "bits" to encode information, which can only take the value of one or zero.[36] It cannot take both at the same time.[37] Any social media app or website you use, or any photo or video you take, is made up of millions of bits using a combination of ones and zeros.[38] Quantum computers, however, use "qubits," which allow them to use values of one and zero at the same time.[39] The entanglement between these qubits, which cannot be described independently of one another, are maximized when in "Bell states."[40] Coined by John Stuart Bell who discovered the Bell theorem, Bell states are four states, represented by mathematical equations, which can be created when qubits are maximally entangled.[41] The term "Bell pairs" describes "one of four entangled two qubit quantum states, known collectively as the four 'Bell states.'"[42] Essentially, the entanglement of two qubits, or "Bell pairs," permits instantaneous connection between distant locations, and two particles that are usually considered distinct entities become one single entity.[43] Measuring the Bell states is integral to quantum communications.[44]

In 2019, Google made an astounding breakthrough. Its researchers "performed a calculation that the largest supercomputers could not complete in under 10,000 years. And they had done it in 3 minutes 20 seconds."[45] This was referred to as a "groundbreaking display of 'quantum supremacy.'"[46] Quantum

---

35 *Id.*

36 Frankenfield, *supra* note 2.

37 *Id.*

38 Katwala, *supra* note 5.

39 Frankenfield, *supra* note 2.

40 Oak Ridge Nat'l Lab'y, *Quantum Internet Breakthrough – Bell State Analyzer Presents Giant Leap Toward Fully Quantum Internet*, SCITECHDAILY (Apr. 15, 2022), https://scitechdaily.com/quantum-internet-breakthrough-bell-state-analyzer-presents-giant-leap-toward-fully-quantum-internet/amp/?fbclid=IwAR2XPyep7MrwIsZT6z628YAd6FXWPPNz8_VeM0BelGiCjCp5mgFiFoFknQc.

41 Daniel Winton, *What are Bell States?*, ALIRO, https://www.aliroquantum.com/blog/what-are-bell-states (last visited Mar. 25, 2023); Oak Ridge Nat'l Lab'y, *supra* note 41.

42 Winton, *supra* note 42.

43 Ben Brubaker, *How Bell's Theorem Proved 'Spooky Action at a Distance' Is Real*, QUANTA MAG. (July 20, 2021), https://www.quantamagazine.org/how-bells-theorem-proved-spooky-action-at-a-distance-is-real-20210720/; Winton, *supra* note 42.

44 Oak Ridge Nat'l Lab'y, *supra* note 41.

45 David Yaffe-Bellany, *Quantum Computing Explained (in Mere Minutes!)*, N.Y. TIMES (Oct. 23, 2019), https://www.nytimes.com/2019/10/23/business/quantum-computing-google.html?.?mc=aud_dev&ad-keywords=auddevgate&gclid=CjwKCAjw_L6LBhBbEiwA4c46up3P6oBWODylz5w2CWDXGzPfD_MnHV6kqhpbgI33_MQ7cOJlXxwUrBoC46MQAvD_BwE&gclsrc=aw.ds.

46 Gent, *Better Quantum Computers*, *supra* note 11.

supremacy occurs when a quantum computer "does something that no conventional computer could do in a reasonable amount of time."[47] Quantum supremacy refers to the quantum computer's ability to solve *any problem*, whereas "quantum advantage" is the ultimate goal, and means the quantum computer has demonstrated it can solve any *real-world problem*.[48] Google's remarkable technological feat demonstrated the potential of quantum computing and helped spur the technological advances we've seen since, and will continue to see within the next five years and beyond.

More recently, Google has used artificial intelligence ("AI") to further advance quantum computing, specifically to "design the next generation of its AI chips."[49] AI is a prevalent, fairly new, field of technology that uses computer science in conjunction with datasets to solve problems in a rational, human-like way.[50] Google's recent approach would lead to a "process of recursive self-improvement that could lead to rapid performance gains for AI."[51] In 2021, IBM unveiled the first processor to surpass the 100 qubit mark, the "127-Qubit Eagle," which was the biggest gate model quantum computer at that time; a European annealing quantum computer surpassed it a year later.[52] The Eagle came two years after IBM's first quantum computer, the 27 qubit Falcon, which

---

47 Delia Paunescu, *What Is "Quantum Supremacy" and Why Is Google's Breakthrough Such a Big Deal?*, VOX (Oct. 29, 2019), https://www.vox.com/recode/2019/10/29/20937930/google-quantum-supremacy-computer-physics-reset-podcast.

48 Rebel Brown, *Why Quantum Advantage & Supremacy Aren't That Complex*, QCI, https://www.quantumcomputinginc.com/blog/quantum-advantage/ (last visited Mar. 25, 2023).

49 Gent, *Better Quantum Computers*, *supra* note 11.

50 *What is Artificial Intelligence (AI)?*, IBM, https://www.ibm.com/topics/artificial-intelligence (last visited Mar. 23, 2023).

51 Gent, *Better Quantum Computers*, *supra* note 11.

52 Edd Gent, *IBM's 127-Qubit Eagle Is the Biggest Quantum Computer Yet*, SINGULARITY HUB (Nov. 22, 2021), https://singularityhub.com/2021/11/22/ibms-127-qubit-eagle-is-the-biggest-quantum-computer-yet/?fbclid=IwAR1cvVFdD25TpL5jFY6sKyUMSBqo7ijhg2KL0hYFeI1mDaH__5E-Rx2r83k [hereinafter Gent, *IBM's 127-Qubit Eagle*]; Forschungszentrum Juelich, *European Milestone: Quantum Computer with More Than 5,000 Qubits Launched*, SCITECHDAILY (Jan. 20, 2022), https://scitechdaily.com/european-milestone-quantum-computer-with-more-than-5000-qubits-launched/?fbclid=IwAR1NxF2SgiE9Xu4wdJy1L9Ogs83guaxubAB6-BE0ttoGDaQPgtUU_9EEn3Y. Gate model quantum computers are available in the marketplace, and operate at low temperatures, requiring expensive refrigeration technology and can only express problems in terms of quantum gates. Quantum annealing computers allow problems to be expressed in the form of operation and research problems, and the company D-Wave Systems has made quantum annealing computers public. Rebel Brown, *Quantum Annealing vs Gate Models Explained*, QCI, https://www.quantumcomputinginc.com/blog/quantum-annealing-gate/ (last visited Mar. 23, 2023).

was made possible after ten years of testing.[53] The Eagle allowed users to delve into "uncharted computational territory," and while it still lacks the ability to provide quantum advantage, it was the first quantum processor that was unable to be simulated on a normal supercomputer due to its size.[54] In 2022, IBM introduced The Osprey, a 433 qubit gate model quantum computer, which is the largest gate model computer as of 2023.[55] IBM is projected to introduce additional quantum processors in 2024, which are anticipated to begin solving previously unmanageable problems and pave the way to true quantum advantage.[56]

These technological milestones are getting harder to measure and assess. IBM and Google continue to build their quantum devices out of superconducting qubits, but they are wired in different ways, which prevents them from being compared qubit to qubit.[57] Esoteric metrics have been proposed in an attempt to provide a comparison between different technologies, such as IBM's "quantum volume" and "Circuit Layer Operations Per Second (CLOPS)," but the large number of variables in the performance of quantum computers make it hard to select the perfect metric.[58] In 2022, as noted above, Europe reached the biggest milestone to date: the launch of a quantum annealing computer with more than 5,000 qubits.[59] The immense size of this cloud-based quantum computer has pushed Germany and Europe to the forefront of the quantum computing race, and the device can solve application-related problems, developed with industrial applications in mind.[60]

Researchers recently proved that nearly error-free quantum computing in silicon-based quantum processors is possible. The researchers shared that their quantum processors had hit an astounding (for quantum computers) 99% accuracy in operations.[61] This rate of accuracy allows quantum computers to

---

53 Jay Gambetta, *IBM's Roadmap for Scaling Quantum Technology*, IBM (Sept. 15, 2020), https://research.ibm.com/blog/ibm-quantum-roadmap.

54 Gent, *IBM's 127-Qubit Eagle*, *supra* note 53.

55 Jay Gambetta, *Quantum-Centric Supercomputing: The Next Wave of Computing*, IBM (Nov. 9, 2022), https://research.ibm.com/blog/next-wave-quantum-centric-supercomputing.

56 *Id.*

57 Gent, *IBM's 127-Qubit Eagle*, *supra* note 53.

58 *Id.*; Jay Gambetta et al., *Driving Quantum Performance: More Qubits, Higher Quantum Volume, and Now a Proper Measure of Speed*, IBM (Nov. 1, 2021), https://research.ibm.com/blog/circuit-layer-operations-per-second.

59 Juelich, *supra* note 53.

60 *Id.*

61 *Quantum Computing in Silicon Hits 99% Accuracy*, PHYS.ORG (Jan. 19, 2022), https://phys.org/news/2022-01-quantum-silicon-accuracy.html?fbclid=IwAR3fdKMWth2we2aPgWw0kxxCCyDi88dP2bs5o9yiVh9mopO5ChXUVPbWiBM. For standard digital computers, accuracy of much greater than 99% is

detect and correct errors when they occur, demonstrating "that it is possible to build quantum computers that have enough scale, and enough power, to handle meaningful computation."[62] Another giant leap toward a fully quantum internet was taken on April 15, 2022, by researchers at the Department of Energy's Oak Ridge National Laboratory, SRI International, Freedom Photonics, and Purdue University.[63] The researchers designed and demonstrated a way to measure Bell states by creating a Bell-state analyzer.[64] Currently, the analyzer can only distinguish between two of the four total Bell states at any given time, but so far measuring the other two states has proven unnecessary, and it is unlikely to prove necessary in the future.[65]

Quantum computers are now utilized to create more efficient autonomous vehicle technology.[66] On April 20, 2022, Hyundai announced it will be expanding its partnership with IonQ, a leader in quantum computing, to use quantum computing for object detection in self-driving cars.[67] This project will use quantum computers "to run machine learning algorithms for learning image classification and 3d objects" to create technologies for its future autonomous vehicles.[68] Hyundai and IonQ plan to develop fundamental quantum techniques for object detection on the road using IonQ's quantum computer, the Aria.[69] The Aria is one of the most powerful quantum computers on the planet, containing 20 algorithmic qubits.[70] These innovations will pave the way for the integration of quantum computers in future vehicle technology. Quantum computing advancements will make fundamental contributions to a wide range of fields: military affairs and intelligence, Big Data search, drug design and discovery,

---

routine. The issue with quantum computing is the difficulty in maintaining multiple qubits in a state of superposition. As individual qubits experience decoherence, the accuracy of the quantum computing process decays. *See, e.g.*, Eric Hazan et al., *The Next Tech Revolution: Quantum Computing*, MCKINSEY & CO. 4 (Mar. 2020), https://www.mckinsey.com/fr/~/media/McKinsey/Locations/Europe%20and%20Middle%20East/France/Our%20Insights/The%20next%20tech%20revolution%20Quantum%20Computing/Quantum-Computing.ashx#:~:text=particular%20%E2%80%9Cnoise%20or%20accuracy%E2%80%9D%20is%20a%20big%20issue,calculation%20errors%20up%20to%2010-100%20times%20higher%20than (noting quantum computers experience error rates 10-100 times greater than classical computers).

62 PHYS.ORG, *supra* note 62.

63 Oak Ridge Nat'l Lab'y, *supra* note 41.

64 *Id.*

65 *Id.*

66 Sahil Gupta, *Hyundai to Use Quantum Computing for Object Detection for Self Driving*, CAR&BIKE (Apr. 20, 2022), https://www.carandbike.com/news/hyundai-to-use-quantum-computing-for-object-detection-for-self-driving-2904562.

67 *Id.*

68 *Id.*

69 *Id.*

70 *Id.*

aerospace engineering, polymer design, machine learning, and digital manufacturing; the list is endless.[71] In this comment, our focus is on potential contributions to the legal field.

As technology advances, new risks emerge as well. Quantum computing technology can easily overcome the standard security defenses of a regular computer, resulting in a threat to national security, including loss of secrets and loss of intelligence.[72] Information security is fundamental to national security, and governments and private companies currently use cryptography to secure information and avoid data breaches.[73] Cryptography uses complex mathematical equations to protect digital information, such that the information is only accessible to someone who holds the mathematical solution, referred to as the "key."[74] While in theory it is possible for regular computers to break into a strongly encrypted system by completing numerous computations, in practical terms a normal computer would take hundreds of thousands if not millions of years to complete the required calculations.[75] In principle, however, quantum computers will be able to break even very strongly encrypted systems within a very short time.[76] Due to quantum superposition and entanglement, even a quantum computer with relatively limited capabilities could break very strong encryption based on current systems in a few hours.[77] This poses a large problem for governments, commercial companies, and law firms, if left unaddressed.

Quantum communications, if used incorrectly, can lead to loss of intelligence. Quantum communication relies on "the collapsing nature of qubits once they are read."[78] The most developed approach to quantum communications thus far is "quantum key distribution" ("QKD").[79] QKD uses "attenuated laser pulses to share a classical encryption between two users."[80] It uses "pulses of light containing single photons (the smallest possible amount of light)."[81] QKD creates a situation where, if someone tries to intercept the communication, they cannot, with the limitation arising not as a result of the limits of current technology, but instead as a result of the laws of nature.[82] If the eavesdropper

---

71 Frankenfield, *supra* note 2.
72 Buchholz et al., *supra* note 4.
73 *Id.*
74 *Id.*
75 *Id.*
76 *Id.*
77 *Id.*
78 *Id.*
79 *Id.*
80 *Id.*
81 NAT'L RSCH. COUNCIL, CONTROLLING THE QUANTUM WORLD: THE SCIENCE OF ATOMS, MOLECULES, AND PHOTONS 149 (2007).
82 *Id.*

tries to "read the quantum key, it will collapse in the quantum state, making the intrusion known to both sender and receiver."[83] Therefore, if there is a data breach, that breach will instantly become known to the owner of the data upon the hacker's attempt to read the quantum key.[84] Thus, if quantum communications are used correctly, and the QKD does not fall into the wrong hands, the data will remain secure.[85] Although QKD provides an additional layer of protection for highly sensitive data, it is not entirely impenetrable.[86] Ensuring the security of the stations where the sender and receiver operate is still necessary, and it may remain susceptible to certain types of attacks and jamming, both on the quantum setup and classical encryption.[87]

C. Preliminary Regulatory Measures Being Explored by the Government, Agencies, and Institutions

As the use of quantum computing technology is on the rise, the United States government and other authorities have begun taking the necessary preliminary steps to begin formulating a legal framework to regulate the technology.[88] In response to concerns over accountability in quantum computing, the United States introduced new legislation designed to help individuals who may fall victim to cybersecurity breaches arising from the application of quantum computing.[89] So far, forty-five states and Puerto Rico have introduced over 250 resolutions or bills that deal with cybersecurity risks.[90] These proposed laws include proactive implementing task forces to advise and research cybersecurity issues, and measures "[r]equiring government agencies to implement cybersecurity training, to set up and follow formal security policies, standards, and practices, and to plan for and test how to respond to a security incident."[91] In 2021, President Biden issued an Executive Order to improve the nation's cybersecurity and expressed cybersecurity concerns by stating that the private

---

83 Buchholz et al., *supra* note 4.

84 *Id.*

85 *See id.*

86 *Id.*

87 *Id.*

88 Park, *supra* note 12. The United States ranks third globally as one of the top government backers for quantum, having funded $2.8 billion as of 2022, with Germany in second place at $3 billion and China in the lead at $5 billion. IQM QUANTUM COMPUTERS ET AL., STATE OF QUANTUM 2022 REPORT 10–11 (2022).

89 Park, *supra* note 12.

90 *Id.* Of course, not all cybersecurity risks directly involve quantum computing, but, as noted above, quantum computing substantially increases a wide range of such risks.

91 *Cybersecurity Legislation 2021*, NCSL (June 22, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2021.aspx; Park, *supra* note 12.

sector must "partner with the Federal Government to foster a more secure cyberspace."[92] Within that same Executive Order, President Biden also addressed the need to keep up with rapidly evolving technology, and stated that "the Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services . . . and invest in both technology and personnel to match these modernization goals."[93] To address the lack of a federal standard for notification of cybersecurity breaches, a bill was drafted by several Senators that would require both private and public institutions to report any cybersecurity breaches to the government within 24 hours of the breach.[94]

These general responses to cybersecurity issues, however, have not focused on the unique problems posed by quantum computing, and the United States government has spent little time addressing the societal implications of quantum computing or developing appropriate regulatory principles to deal with them.[95] There has been a considerable amount of federal funding supporting the creation of quantum computers, yet very little funding has been allocated toward quantum-resistant security.[96] Despite this funding discrepancy, the United States government is concerned with formulating quantum-safe encryption methods for its own use, calling upon the National Security Agency and the National Institute of Standards and Technology (NIST) to address these issues.[97] The federal government has also created a framework to promote and develop quantum computing technology: The National Quantum Initiative Act (NQIA).[98] When President Trump was in office, he signed NQIA into law on December 21, 2018 "to accelerate quantum research and development for the economic and national security of the United States."[99] The Act permits NIST, the National Science Foundation (NSF), and the Department of Energy (DOE), to improve Quantum Information Science (QIS) centers, programs and

---

92 *Executive Order on Improving the Nation's Cybersecurity*, THE WHITE HOUSE (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; Park, *supra* note 12.

93 THE WHITE HOUSE, *supra* note 93; Park, *supra* note 12.

94 Fung & Marquardt, *supra* note 12; Park, *supra* note 12.

95 Bruce Levinson, *Regulating Magic: Why We Need to Establish a Regulatory Framework for Quantum Computing and Artificial Intelligence*, CIRCLEID (Oct. 28, 2021), https://circleid.com/posts/20211028-why-we-need-to-establish-regulatory-framework-for-quantum-computing-artificial_intelligence.

96 Kaafarani, *supra* note 12.

97 Park, *supra* note 12.

98 Levinson, *supra* note 96.

99 National Quantum Initiative Act, Pub. L. No. 115-368, 132 Stat. 5092 (2018); *About the National Quantum Initiative*, QUANTUM.GOV, https://www.quantum.gov/about/ (last visited Apr. 21, 2022).

consortia.[100] The Act requires a coordinated approach to QIS Research and Development (R&D) endeavors throughout the United States Government.[101] The Act not only focuses on the defense and intelligence applications of quantum technology, but also provides a comprehensive framework to develop and coordinate QIS R&D efforts not only across U.S. departments and agencies, but within the private sector and the academic community as well.[102] In addition, the privately-funded Wallenberg Foundation has created a ten-year Initiative for Humanistic and Social Scientific Research in AI and Autonomous Systems.[103] This initiative is intended to address the quantum computing risks and implications that the federal government seems to be glossing over.[104] Research institutions and agencies like these are currently studying, testing, and developing methods to formulate quantum computing standards and regulations.[105]

NIST is one of the leading institutes in quantum computing research, and it is focusing on one issue that law firms should already be considering – encryption risk.[106] This issue is of particular concern to law firms, because encryption of sensitive client data is an integral part of most firms' security practices.[107] The introduction of quantum computers creates the potential for data security disasters.[108] Legal experts have suggested that multiple layers of data protection are essential, and "[a]t the very least, law firms should put in place a data retention policy that reduces the amount of sensitive data being retained unnecessarily."[109] In cases where a firm needs to keep information confidential for a decade or more, it needs to ensure that its private networks "have a quantum-safe algorithm protecting [its] communications."[110] To combat quantum-induced encryption risks, NIST and other authorities are working on developing standards and have requested "proposals for post-quantum public-key cryptographic algorithms to protect against quantum attacks."[111] In 2016, global contenders submitted "69 cryptographic schemes for potential standardization" and in July of 2022, NIST selected four, three of which were

---

100 National Quantum Initiative Act, Pub. L. No. 115-368, § 103, 132 Stat. 5092, 5095–96 (2018); QUANTUM.GOV, *supra* note 100.

101 QUANTUM.GOV, *supra* note 100.

102 *Id.*

103 Levinson, *supra* note 96.

104 *Id.*

105 *Id.*

106 Smith, *supra* note 12.

107 *Id.*

108 *See generally id.*

109 *Id.*

110 *Id.*

111 *Id.*

developed by IBM.[112] NIST originally stated that its post-quantum cryptography standards would be announced by the end of 2021 and would be ready for widespread adoption in private sectors; however, as of 2023, it appears to have missed that target.[113] The cryptography standards are now projected to be disseminated within the next couple of years.[114] There is also a need to establish benchmarks for standards and metrics for quantum computing, which is currently under development by the Defense Advanced Research Projects Agency, a military technology agency within the U.S. Department of Defense.[115] Other developers are in the process of creating "platform-agnostic software tools" that would allow for rapid creation and modification of quantum algorithms.[116]

The Wallenberg AI, Autonomous Systems and Software – Humanities and Society ("WASP-HS") initiative, noted above, will "study the ethical, economic, labor market, social and legal aspects of the ongoing technological transformation of society."[117] WASP-HS recently created the Quantum Law Project, "the first research project dedicated specifically to the study of the legal implications of quantum computing."[118] Its goal is to "carry out a comprehensive appraisal of the legal implications of quantum computing," but the three key legal questions it aims to analyze are: 1) "How does quantum computing affect the practice of law? How does quantum computing affect the legal process? How does quantum computing affect metaphysical assumptions about law?"[119] WASP-HS' Quantum Law Project is a promising research project that supplements the lack of federal funding and research into the legal implications of commercialization of quantum computing technology, and its work will be closely followed by legal professionals and technology leaders.[120]

All these preliminary measures and developments are imperative, but further steps must be taken to ensure creators' and users' cybersecurity and data privacy will not be infringed upon once quantum computers are commercialized.

---

112 Michael Osborne & Vadim Lyubaschevsky, *IBM Scientists Help Develop NIST's Quantum Safe Standards*, IBM (July 6, 2022), https://research.ibm.com/blog/nist-quantum-safe-protocols.

113 Kaafarani, *supra* note 12; *see e.g.*, *Post-Quantum Cryptography*, NIST, https://csrc.nist.gov/Projects/post-quantum-cryptography/news (last visited Apr. 10, 2022) (illustrating that new standards are not yet available).

114 Osborne & Lyubaschevsky, *supra* note 113.

115 Matthew Marrone, *Are You Prepared for the Quantum Revolution?*, BUILT IN (Nov. 15, 2021), https://builtin.com/hardware/quantum-computing-revolution.

116 *Id.*

117 Levinson, *supra* note 96.

118 *Id.*; THE QUANTUM L. PROJECT, http://quantum-law.org/ (last visited Dec. 4, 2021).

119 Levinson, *supra* note 96.

120 *Id.*; THE QUANTUM L. PROJECT, *supra* note 119.

D. Whether and How Quantum Computing and AI Should be Regulated

There are ongoing debates between innovators and technology leaders about the regulation of AI and quantum computing.[121] AI and quantum computing are intimately linked because the widespread deployment and commercialization of quantum computing will expand the capabilities of AI far beyond the considerable range of its capabilities today.[122] On one hand, the need for regulation is apparent due to the magnitude and power of AI and quantum computing technology; on the other, technology regulation is often viewed as a hindrance to innovation and growth within the industry.[123] Industry titans like Google CEO Sundar Pichai have acknowledged the advantageous nature of proactive regulation of AI applications, specifically in relation to quantum computing technology.[124] The power and potential that accompanies quantum computing technology and the commercialization of quantum computing creates a clear need for assessment and regulation of AI technology.[125]

Those opposed to AI regulation have argued that increased regulation will stifle creativity and innovation and reduce market competition.[126] The worry is that tech giants such as Google, Microsoft, Amazon, and Facebook, who have come to dominate the technology market by merging and acquiring smaller tech start-ups, will lose the incentive to innovate if more regulations are in place.[127] More regulation leads to closer scrutiny, and big companies will have to proceed with far more caution than before. Some experts warn that "being careful up and down an organization stifles innovation."[128] Taking the arguments for and against AI regulation into account, it appears the future regulations need to be adequately balanced to protect the public while also promoting industry innovation.[129] It should not trade one for the other.[130]

---

121 *See generally* Mark MacCarthy, *AI Needs More Regulation, Not Less*, BROOKINGS (Mar. 9, 2020), https://www.brookings.edu/research/ai-needs-more-regulation-not-less/; Tom Relihan, *Will Regulating Big Tech Stifle Innovation?*, MIT SLOAN (Sept. 27, 2018), https://mitsloan.mit.edu/ideas-made-to-matter/will-regulating-big-tech-stifle-innovation.

122 Levinson, *supra* note 96.

123 MacCarthy, *supra* note 122; Relihan, *supra* note 122.

124 MacCarthy, *supra* note 122; Levinson, *supra* note 96.

125 Levinson, *supra* note 96.

126 Relihan, *supra* note 122.

127 *Id.*

128 *Id.*

129 MacCarthy, *supra* note 122.

130 *Id.*

II. LEGAL BENEFITS AND REPERCUSSIONS OF COMMERCIALIZATION OF QUANTUM COMPUTING

A. Legal Benefits

A quantum computer could save law firms and legal professionals a significant amount of time and money.[131] The cutting-edge technology could help identify ways to assist clients and restructure research and paperwork with great efficiency.[132] As quantum technology advances, it could have the ability to "interpret laws autonomously" and offer firms "automated legal advice."[133] Today, some law firms already use predictive analytics to theorize likely outcomes of a case.[134] Predictive analytics is "a branch of advanced analytics that makes predictions about future outcomes using historical data . . . ."[135] Quantum computing technology will generate these possible outcomes more efficiently and with greater accuracy.[136] Some legal scholars even argue quantum computing technology will make it possible to accurately predict the outcome of litigated cases.[137] Quantum computing technology will allow computers to complete numerous complex tasks with enormous speed, easily surpassing human intelligence, even that of the brightest lawyers.[138] Law firms could have the ability to accurately predict if a prospective hire is a good fit for the firm, when where their caseload will peak, and how clients will behave.[139] These powerful artificial intelligence tools could automate the legal reasoning process, from automatically conducting due diligence for mergers and acquisitions transactions, to drafting contracts.[140] For remote workers or international attorneys at large law firms, a quantum computing system would be able to share information at an accelerated speed, allowing for easier distant collaboration.[141]

---

131 Shannon Flynn, *What is Quantum Computing and How Is It Disrupting Law Firms?*, L. TECH. TODAY (Dec. 15, 2020), https://www.lawtechnologytoday.org/2020/12/what-is-quantum-computing-and-how-is-it-disrupting-law-firms/.

132 *Id.*

133 *Id.*

134 *Id.*

135 *Predictive Analytics*, IBM, https://www.ibm.com/analytics/predictive-analytics (last visited Oct. 21, 2021).

136 Flynn, *supra* note 132.

137 Steven De Schrijver, *Quantum Computing: The Certainty of the Uncertain*, WHO'S WHO LEGAL (Dec. 16, 2019), https://whoswholegal.com/features/quantum-computing-the-certainty-of-the-uncertain.

138 *Id.*

139 Flynn, *supra* note 132.

140 De Schrijver, *supra* note 138.

141 Flynn, *supra* note 132.

Computational law will also benefit from the implementation of quantum computing technology.[142] Computational law "is the branch of legal informatics concerned with the automation of legal reasoning."[143] Today, the primary focus of computational law is compliance management.[144] Computational law differs from other legal technology in the sense that computational law systems have the "ability to apply regulations to real or hypothetical cases without additional input from human legal experts."[145] In other words, computational law uses algorithms to analyze the law, and these legal algorithms use logical processes to generate legal conclusions.[146]

Legal scholars have anticipated that the emergence of quantum-powered computational law will radically enhance current computational law abilities.[147] To illustrate this potential enhancement, scholars have discussed a prominent claim in the Critical Legal Studies movement: "that law is inherently indeterminate."[148] However, computational law reaches a different presumption: that in most cases, the law is deterministic and can be expressed through algorithms.[149] When certain information is input into an algorithm, there should be an invariable outcome.[150] These differing views of the law may be reconciled by the implementation of quantum-powered computational law, "permitting robust outputs while addressing the well-recognized sources for law's asserted indeterminacy."[151] Commercialization of quantum computers will pave the way for tremendous legal breakthroughs and may allow for a much more efficient legal system.

B. Legal Repercussions

With rapidly evolving quantum computing technology, cybersecurity and data breaches are a chief concern.[152] Since quantum computers are far more advanced than traditional computers, they could lead to a power imbalance in cybersecurity, allowing quantum computers to surpass the defenses of a standard

---

142 Michael Genesereth, *What is Computational Law?*, STAN. L. SCHOOL BLOGS: CODEX (Mar. 10, 2021), https://law.stanford.edu/2021/03/10/what-is-computational-law/.

143 *Id.*

144 *Id.*

145 *Id.*

146 Jeffrey Atik & Valentin Jeutner, *Quantum Computing and Computational Law*, 13 L., INNOVATION & TECH., no. 2, 302, 316 (2021).

147 *Id.* at 313.

148 *Id.*

149 *Id.*

150 *Id.*

151 *Id.*

152 Flynn, *supra* note 132.

device.[153] This could lead to huge data breaches at firms, potentially exposing confidential client information, litigation strategies and intellectual property.[154] Law firms will have to reevaluate and reformulate their information and cyber security systems in order to avoid irreparable loss of personal or highly sensitive information that is currently held in encrypted networks.[155]

1. Risks Upon Commercialization

Once quantum computing is commercialized, numerous legal threats and challenges are bound to arise.[156] First, current cybersecurity programs will be rendered useless. "Exponentially higher computing power" will instantly breach the cryptography and algorithms that currently protect legal data.[157] With a breach of cybersecurity come breaches of data privacy, and terabytes of personal information will be collected, analyzed, transmitted, stored, used and monetized by leveraging quantum computing technology.[158] Existing privacy and security regulations do not, and cannot, contemplate the colossal amount of personal data that can be collected in seconds with quantum computing technology.[159] Experts are not advocating for better privacy law, but rather improved technology to protect privacy. Quantum computing also raises concerns about data privacy implications with entities such as data brokers, credit reporting bureaus, and

---

153 *Id.*

154 *Id*.

155 De Schrijver, *supra* note 138.

156 *See* Carpenter v. United States, 128 S. Ct. 2206, 2212, 2224, 2251 (2018) (These legal challenges could implicate areas of constitutional law, such as Fourth Amendment search and seizure law. In *Carpenter v. United States*, the Court held that the Fourth Amendment requires a warrant for law enforcement to obtain "cell site location information (CSLI)" from wireless service providers. Wireless service providers' networks routinely and automatically record CSLI indicating the cell site(s) to which someone's mobile phone connects, which means that this information can be used to generate a highly detailed record of someone's movements over an extended amount of time. The Court held that allowing this level of detailed, intrusive information to be made available to law enforcement without a warrant violated the Fourth Amendment. Other sources of information, if subjected to quantum-computing-enabled analysis, might lead to such detailed information about individuals that allowing the police obtain it without a warrant is problematic, but this is beyond the scope of this paper.).

157 Louis Lehot, *Bring on the Qubits: How the Quantum Computing Arms Race Affects Legal*, LEGALTECH NEWS (Aug. 19, 2020), https://www.law.com/legaltechnews/2020/08/19/bring-on-the-qubits-how-the-quantum-computing-arms-race-affects-legal/?slreturn=20211024164743.

158 *Id.* One terabyte equals one trillion bytes, and are used to measure bandwidth, which is data transferred in a specific amount of time, and to measure storage capacity on large storage devices. *Terabyte*, TECH TERMS, https://techterms.com/definition/terabyte (last visited Nov. 26, 2021).

159 Lehot, *supra* note 158.

online advertising entities, like Google and Facebook, who have already collected vast amounts of user data.[160] Quantum computing may also improve these organizations' ability to capture and analyze user data, allowing them to figure out ways to target and manipulate people into buying or doing things they may not actually want to do.[161]

2. Risks of Smart Contracts

Second, some law firms utilize "smart contracts" based on blockchains, a form of encrypted, distributed ledger technology.[162] A blockchain is a distributed database shared among the unit structures of a computer network and "[a]s a database, [it] stores information electronically in digital format."[163] The blockchain database stores the data in "blocks."[164] Once stored, the blocks are linked together using cryptography.[165] The purpose of a blockchain is to preserve digital information in a form that cannot be edited, which is why "a blockchain is the foundation for immutable ledgers, or records of transactions that cannot be altered, deleted, or destroyed."[166] Smart contracts are programs that are stored on blockchains, set to "run when predetermined conditions are met."[167] Law firms utilize smart contracts to automate the execution of agreements, providing immediate certainty of the outcome to all parties, thus eliminating the need for intermediaries.[168]

The encryption used for these smart contracts/distributed ledgers can easily be compromised or lost upon the introduction of quantum computing technology.[169] A blockchain system lacks a central authority to manage access keys for users.[170] The private encryption keys determine ownership of resources.[171] Offline backups are non-existent, and the blockchain serves as the

---

160 Venky Anant et al., *The Consumer-Data Opportunity and the Privacy Imperative*, MCKINSEY (Apr. 27, 2020), https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative.

161 *Id.*

162 Adam Hayes, *What is a Blockchain?*, INVESTOPEDIA (Sept 27, 2022), https://www.investopedia.com/terms/b/blockchain.asp.

163 *Id.*

164 *Id.*

165 *Id.*

166 *Id.*

167 *What are Smart Contracts on Blockchain?*, IBM, https://www.ibm.com/topics/smart-contracts (last visited Jan. 10, 2023).

168 *Id.*

169 Joseph J. Kearny & Carlos A. Perez-Delgado, *Vulnerability of Blockchain Technologies to Quantum Attacks*, 10 ARRAY 100065 (2021), https://www.sciencedirect.com/science/article/pii/S2590005621000138.

170 *Id.*

171 *Id.*

online cryptographic system that acts as the resource. Losing a key results in permanent loss of the secured data asset, and if the key or the device storing it is compromised or vulnerable, the data asset can be irreversibly stolen.[172] Essentially, the encryption system used in blockchain technologies is tightly bound to the protected resources, making them more susceptible to potential threats from quantum technology.[173] As a result, as quantum computing advances, it will be necessary to develop means to protect the security of blockchains, including smart contracts, as well as a way to fairly determine who will be accountable if the information is lost or compromised.[174]

3. Risks of Cloud Computing

Third, cloud computing, another computing technology utilized by law firms, will also be significantly disrupted by the introduction of quantum computing technology.[175] Cloud computing is a more recent technological phenomenon in which both databases and computing power are accessed remotely from the "cloud," *i.e.,* the vast collection of servers operated and made available by vendors such as Microsoft, Amazon, and Google.[176] Cloud computing enables the delivery of different services through the internet, and includes tools such as databases, data storage, servers, software, and networking.[177] Cloud computing eliminates the need for law firms to keep files on a hard drive or storage device, and allows them to save money, increase productivity and efficiency, and enhance performance and security.[178] Today, the computers in the cloud are conventional, not quantum, in nature; this will change once quantum computers enter the data center.[179] Indeed, due to the likely high cost of initial commercialized quantum computing capabilities, it is likely that quantum computing capabilities will first be implemented in the cloud by large technology firms, rather than by individual law firms.[180] To account for this potentially monumental disruption, it must be decided who will have access to quantum cloud computing, i.e., which firms, and when.[181] Due to these risks, it is imperative for legal professionals and policy makers to begin formulating

---

172 *Id.*
173 *Id.*
174 Lehot, *supra* note 158.
175 *Id.*
176 Jake Frankenfield, *What Is Cloud Computing?*, INVESTOPEDIA (July 28, 2021), https://www.investopedia.com/terms/c/cloud-computing.asp.
177 *See id.*
178 *Id.*
179 Lehot, *supra* note 158.
180 *See id.*
181 *Id.*

some sort of legal framework to regulate quantum computing technology.

III. Proposed Legal Framework to Protect Cybersecurity and Information Privacy in The Face of Quantum Computing

To account for the inevitable cybersecurity and privacy breaches that will be enabled by the commercialization of quantum computers, it is essential that a legal framework is in place prior to the widespread implementation of quantum computers to systematically manage the avalanche of potential data leaks. Consideration of this regulatory legal framework must begin with several key questions: should national or global regulations exist, or instead, will self-regulation or co-regulation be sufficient?[182] Should quantum computing IP be protected by patents or copyrights, by trade secret protection, or by some other means?[183] Should privacy and similar regulations currently in place, such as European Union's General Protection Regulation guidelines, be modified to account for the technological differences of quantum computing technology?[184]

A. Geographic Scope – Going Global

Legislation is vital to establish a policy framework for quantum computing technology, but policy questions must be answered prior to the legislative process.[185] The legal industry's role in this process is largely to provide insight while a policy framework is created and implemented, to oversee the legal foundation built, and, once these procedures are solidified, to advise corporate and technology companies on regulatory compliance requirements and issues.[186] Beginning with the question of the geographic scope of quantum computing technology regulations, the answer depends on whether broader or narrower principles will be most effective.[187] Because quantum computing technology will be implemented worldwide, and not only commercialized in the United States, it makes sense to take a look at creating broad global standards "to ensure federal and state policies adhere to a shared set of global standards."[188] A variety of global organizations could bolster this endeavor, such as the United Nations or the World Trade Organization.[189] Within these organizations, groups devoted entirely to creating, maintaining, and updating quantum computing technology

182 De Schrijver, *supra* note 138.
183 Wagner & Mazarakis, *supra* note 16.
184 Park, *supra* note 12.
185 Zent, *supra* note 14.
186 *Id.*
187 *Id.*
188 *Id.*
189 *Id.*

standards and regulation could be established.[190] This type of organization has already been created for climate change within the United Nations, with a group called the Intergovernmental Panel on Climate Change ("IPCC"), which provides "policymakers with regular scientific assessment on climate change, its implications and potential future risks . . . [and] put[s] forward adaptation and mitigation options."[191] Despite overt challenges related to gaining consensus amongst all nation states, global regulations allow for global collaboration and cohesion, which appears to be the most beneficial approach for creating standards and regulations when dealing with technology of this magnitude.[192]

B. Looking to Existing Technology Regulations to Create Quantum-Specific Standards

There are technology regulations in place today that may be helpful to guide the creation of quantum computing regulations, at least in certain fields. In the area of privacy, for example, the General Data Protection Regulation ("GDPR") is the European Union's "most comprehensive data privacy law to date" since it became enforceable on May 25, 2018.[193] It extends beyond the boundaries of the EU however, and applies to U.S. businesses if either, "[t]he company offers goods or services (even in the absence of commercial transactions) to EU/EEA residents" or, "[t]he company monitors the behavior of users inside the EU/EEA."[194] There are six key requirements for businesses that fall into one of the aforementioned categories, and therefore must comply with GDPR.[195] The first is "data breach notifications" which sets out the specific procedures companies must follow when a data breach has occurred; for example, the timeframe the breach must be reported and to whom.[196] This concept is analogous to the bill that has been drafted by Senators that would require both private and public institutions to report any cybersecurity breaches to the government within twenty-four hours of the breach.[197] The second key requirement is regular "data protection impact assessments" to avoid

---

190 *Id.*

191 THE INTERGOVERNMENTAL PANEL ON CLIMATE CHANGE, https://www.ipcc.ch/ (last visited Mar. 25, 2021); Zent, *supra* note 14.

192 Zent, *supra* note 14.

193 Sebastian, *supra* note 15.

194 *Id.*

195 *Id.*

196 *Id.*; Regulation 2016/679 of the European Parliament and of the Council of 27 of April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 33, 2016 O.J. (L 119/1).

197 Fung & Marquardt, *supra* note 12; Park, *supra* note 12.

compromising personal data, such as biometric or genetic data.[198] The third requirement is "privacy by design," which means that every business must have data protection built into its core framework.[199] The fourth requirement is "strict consent conditions" which requires gathering consent from "data subjects" - those whose private information gets collected by the corporations.[200] The fifth requirement is "data subject access requests," which is the right of users to be able to obtain the information that a data controller (the entity collecting information) has about the user.[201] The sixth requirement is "appointing a data protection officer" which is essential to ensure companies are compliant with GDPR.[202] These GDPR principles provide a comprehensive foundation for policymakers and legal professionals to reference when formulating data protection guidelines to combat data breaches that may occur upon the commercialization of quantum computing technology.[203]

C. Intellectual Property Issues

Arguably, the most pressing legal question involving quantum computing technology is how the IP of the technology will be regulated.[204] There are three avenues to explore: patent protection, copyright protection, and trade secret protection.[205] A patent grants an exclusive property right to the inventor for a fixed term, preventing others from using, selling, manufacturing, or importing the innovation without a license, for a duration of typically 20 years.[206] Today, there are 1892 granted patents relating to quantum computing, covering "machine learning, optimizing supply chains or financial asset portfolios, enhancing molecular simulations for pharmaceutical development, and improving the error-correction of quantum hardware."[207] This indicates significant growth of quantum patents, after seven years of inaction from 2006-2014, the amount of quantum-related patents granted annually increased from thirty-seven, in 2014, to 435, in 2021.[208] Patents can be licensed or sold, but

198 Fogg, *supra* note 15.
199 *Id.*
200 *Id.*
201 *Id.*
202 *Id.*
203 *Id.*
204 Wagner & Mazarakis, *supra* note 16.
205 *Id.* (discussing the practical limitations of regulating quantum computing technology through patent, copyright, and trade secret protection).
206 *Id.*
207 *Id.*; Mauritz Kop et al., *Intellectual Property in Quantum Computing and Market Power: A Theoretical Discussion and Empirical Analysis*, 17 J. INTELL. PROP. L. & PRAC. 613, 622 (2022).
208 Kop et al., *supra* note 208.

many companies become opportunistic when groundbreaking technology is involved, leading to "patent wars."[209] Because organizations such as NIST are in the process of developing quantum computing standards, conflicts may arise between those organizations and holders of current quantum computing patents who may be unwilling to license their technology, and at a minimum may demand substantial royalties in exchange for permitting others to use them.[210] Even those in the tech industry who aren't "interested in offensive litigation, may benefit from patents as a bargaining tool or to preclude competitors from gaining interfering intellectual property rights, thereby ensuring freedom to operate."[211] Patents are a useful tool to protect technological innovations, but the vast potential of quantum computing technology will likely produce patent wars between the leading technological innovators.[212]

Patentability issues may arise that could complicate patent enforcement or prosecution due to certain United States Code (U.S.C.) provisions.[213] Quantum computing technology involves frequent improvements to hardware, "in which cases, potential rejections will commonly arise from obviousness under 35 U.S.C. § 103 or lack of novelty under § 102."[214] U.S.C. § 101 may pose the biggest patentability issue for quantum computing technology, because § 101 deems abstract ideas, like "mathematical formulas and natural phenomena," ineligible for patent protection, which is, at least arguable, precisely what comprises quantum computing.[215] Quantum computing is fueled by algorithms that utilize the quantum mechanical phenomena of entanglement and superposition, which may create issues with some quantum patent claims.[216] In the case of *In re Huping Hu*, the U.S. Patent Trial and Appeal Board sustained a § 101 rejection of a quantum-computing-related patent application, based on the fact that quantum entanglement is not an invention, but instead is a natural phenomenon.[217] To reduce the risk of patent rejection, applicants may find it worthwhile to tailor claims to quantum software as "tangible, non-transitory matter, with hardware elements added when possible."[218] Regardless, the risk of rejection is high for quantum computing software patentability, and it would be

---

209 Wagner & Mazarakis, *supra* note 16.
210 *Id.*; Kaafarani, *supra* note 12.
211 Wagner & Mazarakis, *supra* note 16.
212 *Id.*
213 *Id.*
214 *Id.* A purportedly new invention is not patentable if it would have been obvious to someone skilled in the field or if it does not in fact contain anything novel. 35 U.S.C. § 103.
215 35 U.S.C. § 103; Wagner & Mazarakis, *supra* note 16.
216 Wagner & Mazarakis, *supra* note 16; Buchholz et al., *supra* note 4.
217 *In re* Huping Hu, 848 F. App'x 416, 420 (Fed. Cir. 2021); Wagner & Mazarakis, *supra* note 16.
218 Wagner & Mazarakis, *supra* note 16.

wise to consider alternative IP protections.[219]

Copyright protection appears a more viable alternative for quantum computing IP protection.[220] Software copyrights are acquired through registration and grant the creator exclusive rights for their lifetime, plus 70 years.[221] Copyright registration is far more efficient than the patent process, as it can be expedited to take only a few days, which aligns with the speed at which quantum computing technology will be advanced.[222] However, given the lengthy duration of copyright protection, this form of IP protection could stifle innovation. Additionally, certain areas need special attention and legal innovation, such as the protection of functionality, which is not covered by copyright laws.[223] This prompts the debate over whether quantum software functionality should be eligible for patent protection.[224]

Whether patents or copyright will protect quantum computing technology, detecting infringement may prove difficult.[225] Establishing infringement of quantum computing technology may require reverse engineering, but the hardware itself "may be inaccessible because much of today's quantum computing is cloud-based."[226] Additionally, because "quantum computing occurs in a superposition of states" and is destroyed once observed, and current logic operations measure only final results, reverse engineering of quantum computing phenomena will be further complicated.[227]

Trade secret protection is another avenue to explore, as quantum computing technology cannot be easily reverse engineered.[228] Trade secret protections occur automatically and contain no time limitations, and the protection lasts indefinitely unless the confidential technology is either reverse engineered, independently discovered, or disclosed by the owner.[229] Trade secret protections typically stifle innovation, so a time limitation would need to be implemented to combat this. Companies often take legal action to prevent the theft of trade secrets, and to ensure that if the information is leaked, those who are responsible are subject to civil and criminal penalties.[230] Companies must also take "reasonable measures" to prevent their secrets from exposure; reasonableness is

---

219 *Id.*
220 *Id.*
221 *Id.*
222 *Id.*
223 Kop et al., *supra* note 208, at 619.
224 *Id.*
225 Wagner & Mazarakis, *supra* note 16.
226 *Id.*
227 *Id.*; Buchholz et al., *supra* note 4.
228 Wagner & Mazarakis, *supra* note 16.
229 *Id.*
230 *Id.*

determined by a fact-specific inquiry.[231] There is no precise "reasonable measures" test, but companies must balance varying factors such as the value of the information, the financial burden and labor cost of acquiring the information, marketplace competition, and the ease of reverse engineering.[232] Reasonable protective measures include digital security, physical security, and legal safeguards such as non-competes, non-disclosure agreements (NDAs), and confidentiality.[233] Given the issues already arising with patent applications covering quantum computing technology, copyright and trade secret protection seem to provide the most viable protection for quantum IP.[234]

Regardless of whether patent, copyright, or trade secret protection is used, the duration of IP protection for quantum technology should be shortened significantly to leave room for necessary adjustment as quantum technology advances.[235] Moreover, it will be important to avoid IP overprotection, which would grant too broad a scope of exclusive rights, in order to avoid a narrow concentration of market power.[236] It may be necessary to be aggressive about applying antitrust principles to overzealous efforts to enforce potentially broad quantum-computing-related IP rights.[237] Antitrust regulations will encourage fair competition in the context of quantum computing.[238]

IV. CONCLUSION

Quantum computing is still in its infancy but will continue to grow and evolve rapidly. Therefore, it is essential that legal professions and policymakers continue to explore policies and regulations to protect businesses and individuals from irreparable harm that may be caused by cybersecurity and privacy data breaches upon the commercialization of quantum computing technology and quantum computers. Decisions must be made to address the geographical scope of quantum computing standards and policies, and global regulation appears to be the best avenue.[239] We must also determine how quantum IP will be protected, whether through patent, copyright, or trade secret protection, although copyright

---

231 Michael J. Kasdan, Kevin M. Smith & Benjamin Daniels, *Trade Secrets, What You Need to Know*, NAT. L. REV. (Dec. 12, 2019), https://www.natlawreview.com/article/trade-secrets-what-you-need-to-know.

232 *Id.*

233 *Id.*

234 *In re* Huping Hu, 848 F. App'x 416, 420 (Fed. Cir. 2021).

235 Kop, *Regulating Transformative Technology*, *supra* note 17, at 2, 14.

236 *Id.*

237 *Id.*

238 Kop, *Quantum Computing*, *supra* note 18, at 1, 8.

239 Zent, *supra* note 14.

and trade secret protection seem best suited to address quantum IP.[240] Shorter IP durations are strongly suggested to account for the rapidly changing nature of quantum computing technology.[241] Finally, antitrust regulations should be utilized to avoid a narrow market concentration of power that may arise from shorter IP regulations.[242] Quantum computing is an exciting and influential technological innovation, but it must be regulated and have proper standards in place to ensure it leads to the advancement of the legal system and of society, rather than to their demise.

240 Wagner & Mazarakis, *supra* note 16.
241 Kop, *Regulating Transformative Technology*, *supra* note 17, at 2, 14.
242 *Id.*; Kop, *Quantum Computing*, *supra* note 18, at 8.