Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What To Expect In The Emerging Age Of Quantum Computing

By **Nicholas Smith and Ryan McKenney** (April 21, 2020, 5:23 PM EDT)

Nicholas Smith

Ryan McKenney

Once considered a scientific impossibility, quantum computing is now expected to have a far-reaching commercial impact thanks to an increase in investment and a myriad of new discoveries by physicists and computer scientists. Quantum computers have the potential to transform industries from auto manufacturing to pharmaceuticals to finance, but the technology has only recently moved from the laboratory to the commercial market.

At the Consumer Electronics Show in Las Vegas in January, IBM Corp. announced it had struck partnerships with Daimler AG (the parent company of Mercedes-Benz) and Delta Air Lines Inc. to harness quantum computing to solve real-world issues for the two companies. Advancing electric vehicle batteries and improving route scheduling could be some of the first commercial applications for the nascent technology.

Quantum Computing 101

Quantum computing marries the properties of quantum physics with advanced computer science, creating a potent combination that is immensely more powerful than classical computing. While classical computer algorithms scale exponentially, quantum computers scale polynomially. This leads to huge advantages in time, accuracy, and processing capability.

Ordinary classical computers perform calculations using “bits” of information in the form of 0s and 1s, while quantum computers use quantum bits, or qubits, that can simultaneously exist as both a 0 and a 1. In the quantum universe, a flipped coin can exist as both heads and tails. Qubits have the power to vastly increase the predictive powers of quantum computers, allowing them to solve complex equations that could take a classical computer thousands of years to solve, if solvable at all.

The Future Is Now

In October 2019, Google Inc. published an article in the journal Nature detailing how its quantum computer performed a complex computation in 200 seconds that they claim would have taken the most powerful supercomputer some 10,000 years (a magnitude of 1.5 trillion times faster). With this, Google achieved what it called “quantum supremacy” — the successful demonstration that a programmable

quantum device can solve a problem that classical computers practically cannot. In the article announcing Google's breakthrough, researchers stated that "we are only one creative algorithm away from valuable near-term application."

IBM's announcement shows that real-world applications are already upon us. Jamie Thomas, general manager of systems strategy and development for IBM, hailed the partnerships: "[Daimler and Delta] join more than 100 clients already experimenting with commercial quantum computing … to tackle problems like risk analytics and option pricing, advanced battery materials and structures, manufacturing optimization, fraud detection, chemical research, logistics and more."

The promise of this technology is great, and there is a sense within the computing industry that we are entering a period of time where the technology and its possibilities will develop rapidly. IBM's director of research, Dario Gil, stated that "this is the most exciting time in computing in many decades" and claims that by the end of the decade we will reach a point of "Quantum Advantage," the exploitation of quantum computing for scientific and commercial advantage.

Amazon.com Inc. recently set up its AWS Center for Quantum Computing at Caltech that will leverage academic-commercial partnerships to accelerate development of quantum computing hardware and software. The e-commerce giant has also begun offering its cloud users the ability to experiment with quantum computing via Amazon Web Services. Similarly, Microsoft Corp. provides access to quantum processes via its Azure cloud service.

IBM has created its "Q Network," a cloud-based setup that provides access to the company's quantum computing hardware, software and developer tools. This was the fourth year in a row IBM doubled the quantum volume of their computers. Currently, 15 IBM quantum computers are powering over 200,000 users and the now 100 commercial partners announced at the Consumer Electronics Show.

In December 2018, President Donald Trump signed the National Quantum Initiative Act, which allocates $1.2 billion to advance research and development of quantum technologies. The president's budget proposal announced in February includes a proposal to spend $25 million on what it calls a national "quantum internet," a network of machines designed to make it harder to intercept digital communication. The administration also vowed to double funding for artificial intelligence and quantum computing research outside the U.S. Department of Defense by 2022.

Meanwhile, China has developed a new quantum research facility worth $10 billion in addition to a dedicated quantum communication network between Beijing and Shanghai, costing some $80 million. The European Union has developed a $1.1 billion quantum master plan.

The Technological and Commercial Opportunities

The power of quantum computers could change the research and creation of products as diverse as antibiotics, polymers for lightweight airplanes, electronic materials, electrolytes for next generation batteries, and more. Quantum computers also have the computational power to solve complex optimization issues for logistics and transportation companies that previously were insurmountable.

Accenture PLC, for example, is currently examining ways in which quantum computers can tackle specific business problems such as finding the ideal route for retail deliveries and optimizing machine learning. Given this, it is not surprising that a growing number of companies are exploring the benefits of quantum computing.

Lastly, and maybe most importantly, quantum computers could improve encryption technology by generating random numbers so complex that neither classical nor quantum computers can hack them. But this also poses the greatest known risk associated with quantum computers: the computational power to hack all current encryption systems. In an environment already rife with data breaches (in 2019 alone there were nearly 4,000 publicly known cyberattacks against financial institutions), quantum computing is the next frontier of cyber risk and cybersecurity.

The Greatest Known Risk: Encryption and Data Security

According to Newsweek, true quantum supremacy would render the most common forms of encryption obsolete. The potential negative impacts of quantum computing are leading to a quantum encryption arms race.

Quantum computers will be able to simultaneously break all existing cryptographic keys while also creating quantum encryption systems that are unhackable with existing technologies. The first country to achieve quantum encryption could theoretically hide all of its information from traditional surveillance methods. Christopher Painter, a former diplomat on cybersecurity at the U.S. Department of State, stated that "we have really strong tech companies, but if we really want to maintain an edge, we need to take this seriously at a strategic level." Thus, China and the U.S. are both working to scale up their quantum computing infrastructure to achieve hegemony on this new battlefield.

Current methods of encryption rely on mathematical complexity and random numbers, scrambling data that can be unlocked with keys. These schemes can be easily cracked by quantum computers, leading to vulnerabilities in data systems as vital as banking, health care, national security, and trade secrets. Security researches believe quantum computers could have the power to instantly break even the strongest encryption protocols within a few years. Thus, companies must begin transitioning to quantum-safe encryption methods now in order to prevent future breaches.

Financial institutions that employ blockchain technology for corporate record-keeping, smart contracts, and distributed ledgers are also at risk of falling prey to a quantum data breach. Over the last five years, many banks have turned to blockchain to keep transaction records safe by relying on public-key cryptographic systems, which makes the encryption key public and keeps the decryption key private.

While this security is what makes blockchain safer than storing records on an internal or cloud server, it too relies on factoring large numbers which a quantum computer could break instantaneously. John Prisco, the CEO of quantum security firm Quantum Xchange, notes that "new blockchain banking topologies, which are progressively adopted, show multiple vulnerabilities in their storage of private-public key pairs." These vulnerabilities are leading companies to take proactive steps now.

It is realistically a matter of when, not if, a financial institution will suffer a cybersecurity hack at the hands of a quantum computer. It is also possible that bad actors could be harvesting data now that will be decrypted in the future where quantum computers are commercially available.

With this in mind, several large banks and hedge funds are piloting quantum key distribution technology in preparation for future quantum attacks. The QKD market is estimated to grow from $85 million in 2019 to $980 million by 2024. IBM plans to offer quantum-safe cryptographic services on its public cloud in 2020 and researchers and corporate IT specialists alike are currently at work to find ways to quantum-proof encryption systems. The National Institute of Standards and Technology is developing a uniform method for quantum-proof encryption that will provide much needed standardization to the quantum

computing market.

Contractual and Compliance Considerations, and What Comes Next

The risks and opportunities posed by quantum computing will bring about new issues for business leaders and lawyers alike. There will be a need to anticipate and respond to this emerging technology, and for consumers of technologies and related services to negotiate contracts with clear and enforceable provisions to protect data as quantum computers become more powerful and widespread.

As part of rethinking security and service agreements in the context of quantum computing, parties must reconsider the issue of liability — this could arise in a variety of ways, including from hacks exploiting safeguards that ostensibly are quantum-proof but that prove not to be, and from errors in calculations and outcomes that are more likely in the early days of any emerging technology.

For example, a number of data protection regulations globally obligate companies collecting or processing personal data take appropriate technical and organizational security measures to protect personal data against unauthorized access; those steps may prove difficult to comply with when quantum computers can break current cryptography, and setting out appropriate contractual obligations in a context in which the relevant technology is changing so rapidly is likely to be a point of contention and wide variation in approach for some time.

There are also commercial implications as the large technology firms are the ones currently leading the quantum research race. Google, Microsoft, IBM and Amazon Web Services already have contractual arrangements with many companies and their quantum services will mean they have further leverage in contract negotiations.

With these technologies concentrated in the hands of companies that already possess enormous leverage when negotiating licenses and services agreements, it seems that individual potential customers may — for the near future, at least — need to consider cloud computing strategies in the context of having limited contractual rights vis-à-vis that customer's key providers of those technologies.

This last point is of particularly great concern for customers in regulated industries, where transparency, auditability, and the ability to manage and allocate risk effectively across supplier networks are all required under industry regulation. Much as is the case with cloud computing, there is a deep tension emerging between the commercial leverage of tech giants and the needs of regulated entities to interface with regulators and to manage risk.

Though the full effects of quantum computing likely won't be felt for a number of years, business leaders and legal counsel must begin to consider how to protect from the cybersecurity risks posed by the technology and how best to take advantage of its potential. The future of quantum computing is still very fluid as the technology continues to be developed in the lab and tested by companies around the globe, but it is wise for companies to begin planning for a quantum world.

Nicholas Smith is a partner and Ryan McKenney is a law clerk at Milbank LLP.