Metropolitan State University

Quantum Computers and their Threat to Privacy

Joshua Hoshiko

Computers, Ethics, and Society

Dr. Jeffrey Ogle

November 20, 2019

On September 20th, 2019, Google officially announced that its quantum computer successfully demonstrated quantum supremacy. Quantum supremacy is a term that refers to a quantum computer’s ability “to successfully solve a problem no classical computer can solve, even a relatively artificial problem” (Friedson, Herman, 7). In Google’s article, they described how their Sycamore processor, a 53 qubit quantum processor, completed a calculation in 200 seconds that the most powerful classical computer would have completed in approximately 10,000 years (Google 1). Although some major companies claim that 10,000 years is an exaggeration, there is no doubt that a general purpose quantum computer is quickly becoming a reality.

So why is this announcement so important? For many years, scientists have been investigating the advantages of quantum computers and whether quantum computers could feasibly become important tools for society. While classical computers use binary bits to represent information, quantum computers use qubits, which are quantum particles that can be in a mixture of two states. The main advantage of quantum computers is their ability to simultaneously compute multiple solutions to a problem as opposed to slowly calculating solutions one by one like classical computers. While there is still a debate as to how useful quantum computers will be compared to our existing systems, because of a quantum computers ability to calculate multiple solutions concurrently, there are multiple problems that quantum computers are predicted to be extremely efficient at solving (protein folding, database management, etc). However, quantum computing is likely to be a double edged sword primarily because quantum computers are also predicted to “render discrete logarithm and factoring based cryptographic systems like those based on Rivest, Shamir, Adleman (RSA) and Elliptic Curve Cryptography (ECC) algorithms woefully obsolete” (Majot, Yampolskiy, 17) using Shor’s algorithm. While these encryption techniques keep our information safe now, quantum computers could inadvertently jeopardize our security and privacy if they are not used ethically. We are still far away from being able to utilize quantum computers to their full potential, but many predict that a fully operational quantum computer could be around the corner. Many countries are now racing towards the first general purpose quantum computer and not all countries may use quantum computers for good. With quantum computers becoming a reality, we are entering a critical period in which new policies and protections must be created to protect people’s information from those who seek to abuse the power of quantum computers.

Information is power in this day and age. In such an interconnected world, information is collected in massive quantities and the concern for privacy of our data is growing as well. We trust that companies and stakeholders are transparent with what information is being gathered, but many internet users are just now realizing how much data is collected in the background. People rely on systems like encryption and secure communication to keep information private. Other technologies such as VPNs, or virtual private networks, and decentralized digital currencies such as bitcoin are becoming much more popular to help aid in maintaining our privacy. Information is not always handled ethically, and with quantum computing becoming a reality, these technologies may not be sufficient to protect our privacy in the future. Without a sense of security on our networks, we could even experience a chilling effect in which users stop trusting the security of information being shared simply because that information could be decrypted by a quantum computer. To avoid as much damage as possible, a combination of regulations, careful implementation of these new devices, and better data practices will help preserve privacy and security of society’s information.

Many scientists are designing new encryption methods and protocols for the quantum age. Quantum encryption and new transmission protocols offer promising alternatives to our current security systems, but it is very likely that there will be period of time in which we will be transitioning from our classical systems to a quantum internet. Companies and governments are likely to be the first to create functional quantum computers because of the amount of resources needed to create such computers. The race is all around the world as well, with many countries creating quantum technology programs in a similar fashion as the space race or the Manhattan project. This will create disparity between these powerful entities and the general public as they will have quantum computing and we will not. The hope is that corporations and government bodies respect our privacy, but given a master key in the form of a quantum computer, the temptation to use such a powerful tool will always be present. Arthur Herman and Idalia Friedson from Hudson Institute describes quantum computers as “a system [that] would pose a threat to national security because it could open the encrypted secrets of countries, companies, and individuals and cripple critical infrastructure and financial systems. A foreign competitor with the edge in quantum computing could also threaten America’s economic security while reaping the many economic benefits of the quantum era” (Friedson, Herman, 3). Until the new security precautions are in place, there are several measures that should be taken to preserve security and privacy of our information.

Concerning corporations and companies, policies should be enacted to help preserve the privacy of users and the data of opposing companies. Powerful companies could feasibly fund the creation of a quantum computer system and claim that these systems are for database search efficiency, research, or quantum assisted machine learning for advertisement algorithms, but there will always be temptation to use these systems for secondary uses. A company could potentially use quantum computers to decrypt rival company data or intercept their own employee information and bypass any precautions made to keep that information private. Monetary gain may be primary incentive for companies to do this, but there may be other situations for which companies may want to abuse the power of quantum computers. Strategically created regulations could aid in preventing companies from using quantum computing for unethical reasons and help maintain security of information while we transition into new cybersecurity protocols and systems. Transparency with customers/employees and education of customers/employees can also help put privacy concerns to rest. The hope is that as quantum computers are being implemented, we are careful with the execution and we keep these concerns in mind to prevent an uninformed population from being taken advantage of by quantum computer systems. It is important to remember that safe use is not guaranteed and while abuse of these systems may not frequently occur, there will always be a temptation.

Spying and acquisition of private information is not limited to only corporations. Government agencies or hacktivist groups of the future may also have incentives to use quantum computers for ill will. Government agencies have been known to collect private information in large quantities today and are likely to continue to do so in the future without some form of formal regulation. Quantum computers could provide these agencies the ability to also decrypt information that the general population would rather keep private. The difficulty here is that regulating the regulating body of a country is already difficult and even if the populace was educated about the risk of privacy violation by quantum computers, agencies could very well continue to unethically collect the public encrypted data regardless of society’s wishes. On the flip side, Hacktivist groups could feasible afford quantum computers at some point as well and they have even less incentives to hold back with the use of their quantum technology. The only way to guarantee the safety of information is to carefully monitor the implementation of these quantum systems. While regulations can help keep corporations in check, close monitoring of the implementation of quantum computers and educating the public are the best ways to keep quantum technology out of the wrong hands. Regulatory boards whose sole purpose is to preserve security could also help keep a watchful eye for corporations abusing the use of these powerful tools. The pairing of regulation and careful implementation would help give us the time needed to introduce the before mentioned updated quantum security systems during this critical period of time.

On a global scale, multiple countries have now created quantum computing projects to race to the first fully operation quantum computers. The United States, China, United Kingdom, and many more have created formal projects with goals and funding. Incentives to abuse quantum computers on a global scale are even more present then incentives for corporations to abuse quantum computing. Rival countries are already preparing for the inevitable emergence of quantum decryption, where “Nation-states whom we consider competitors or adversaries are currently collecting and storing sensitive data knowing that they will be able to decrypt this information when a quantum prime computer is realized. This means that data not protected prior to Q-Day will be just as vulnerable as data not protected afterwards” (Friedson, Herman, 10). Sensitive information is quite appetizing to other countries and a lot of information is already destined to be compromised.

The key here is to have a coordinated strategy between countries. With many countries already preparing quantum security and communication systems, there are three major focuses to aid in the preservation of our information in the approach to quantum computing: “the security shelf life of the information assets, the migration time to systems designed to resist quantum attacks, and the time remaining before quantum computers break the security” (Mosca 1). Global regulation might help reduce some risks of information breaches, but it will not stop all countries from abusing the power of quantum computers. In this scenario, countries should take a defensive approach to protect sensitive information of both the country and its residents. While high priority systems will likely be migrated first, the general public’s data will likely experience a delay if we do not begin preparing safeguards now. Companies that handle sensitive information should begin preparing for these scenarios by creating migration locations or investing in quantum security once the infrastructure is feasible to build. Educating users about better data practices can also help diminish the amount of sensitive information that is online. We as a society will have to consider what information needs to be stored, how long it will be relevant, and how necessary it is for entities to keep that information. Better data practices now can help prepare us for privacy risks of the future.

With all of the before mentioned risks, it is important for the world to begin preparing for the inevitable quantum age. While it is hard to gauge the impact quantum computing will have on cyber security and privacy, the risks are too great to ignore. Regulating the implementation and use of these computers in companies and agencies should be the first big step of transitioning into the quantum age. This will hopefully help mitigate unethical breaches of information. A central governing body could help enforce these regulations and selectively placing these computers would help stop them from falling into the wrong hands. Better data practices and educating the public will help prevent sensitive information from being available to steal in the first place. However, it is inevitable that some information is destined to be compromised. When all of the above reasons fail to deter unethical use, the creation of contingency plans and coordinated defensive strategies help prevent some of the damage. Focusing resources on quantum security and secure communication pipeline research will help reduce the amount of time that we will go unprotected. With the careful execution of all of these precautions, we will be ready for the arrival of the quantum computing era.

Work Cited

Arute, Frank., Arya, Kunal., Babbush, Ryan. *et al.* *Quantum supremacy using a programmable superconducting processor.* Nature, 2019.

Herman, Arthur, and Idalia Friedson. *Quantum Computing: How to Address the National Security Risk.* Hudson Institute, 2018.

Majot, Andy. *Global Catastrophic Risk and Security Implications of Quantum Computers*. Elsevier, 2014.

Mosca, Michele. *Cybersecurity in an Era with Quantum Computers: Will We Be Ready?* IEEE, 2018.