QUANTUM COMPUTING

A Potential Shift in Encryption and Litigation

Richard R. Marsh Flaherty Sensabaugh Bonasso PLLC

Attorneys have always adapted to new technology and utilized those advancements in their practice, including in the areas of confidentiality, discovery, and the presentation of evidence. Quantum computing, once just a theory, is becoming real in small ways and will soon affect many industries, including law.

WHAT IS QUANTUM COMPUTING?

In discussions of quantum computing, devices such as desktops and smartphones are considered classical computers. Quantum computers are not just faster classical computers; rather, they work in a completely different way.

Any computer relies upon binary code: the basic language of all digital communications. Binary code is comprised of only two characters: 0 and 1. Classical computers use bits to express this code. This creates an "either-or" or "on-off" setup that limits how they compute. Quantum computers use qubits, which can be 0, 1, or both at the same time. This feature, called superposition, allows quantum systems to handle many possibilities simultaneously, greatly boosting their power for some tasks.

Quantum computers are not meant to take over everyday computing. They are built for specialized uses such as complex modeling, running simulations and analyzing large amounts of data. These abilities could affect encryption, scientific research and product development.

FROM STRONG ENCRYPTION TO VULNERABILITY: A PRIVACY RECKONING

Quantum computing poses a real challenge to today's encryption methods. In the past, attorneys did not need to know much about encryption, but now their professional duties require at least a basic understanding.

In the past, keeping information confidential meant locking up paper files. As digital records became common, attorneys also had to protect electronic data. Now,

they must follow rules such as HIPAA and state data breach laws, and guard against risks such as wire fraud. Due to these changes, attorneys could (and can) no longer ignore rules of encryption and instead had to have a basic user's understanding of the technical mechanisms by which their clients' sensitive information was protected. Today's encryption methods rely on mathematical problems, such as factoring large prime numbers or solving certain discrete logarithm problems. Classical computers cannot solve these math problems quickly. Quantum computers, on the other hand, can solve these problems much faster. A classical computer could take thousands of years to crack an encrypted file, whereas a quantum computer might only take hours.

In response, governments and industry are developing post-quantum cryptography or PQC. PQC encompasses new encryption methods designed to withstand quantum attacks. Transitioning to PQC will take years; the U.S. government aims to mitigate quantum-related risks by 2035.

Attorneys should keep an eye on this change. Big companies such as Microsoft and Google are working to add PQC to their systems, which matters because so many people use cloud services. Still, lawyers need to carefully select and vet vendors to ensure data remains safe.

Importantly, even before quantum systems become mainstream, attorneys must still practice good cybersecurity and encryption protocols. Attackers have been focused on a "harvest now, decrypt later" strategy, which is already in use. With this strategy, bad actors may collect encrypted data today, anticipating future decryption capabilities. This reinforces the need for continued vigilance in data security as part of an attorney's duty of confidentiality.

THE COURTROOM OF THE FUTURE: SIMULATION, EVIDENCE, AND LIABILITY

Technology has steadily transformed courtroom practice, from overhead projectors to digital presentations and AI-assisted tools. Attorneys started with overhead projectors and then started using computers to present slide decks. Today, the presentation of video and audio recordings is almost expected. And with the latest AI advancements, "on the fly" slide decks can be prepared as part of openings or closings to provide near real-time advocacy to the jury.

Expert witnesses have frequently relied upon technology in developing and presenting their opinions. This technology includes modeling software for accident reconstruction, engineering analysis and financial projections. Courts have responded to this modeling software by developing standards, such as Daubert, to evaluate the reliability and admissibility of such evidence.

Quantum computing has the potential to significantly enhance these capabilities. One key application is advanced simulation. For example, in pharmaceutical research, companies want to model chemical interactions before performing lab experiments. Classical computers have a difficult time with these and similar scenarios. Quantum systems can run multiples of those scenarios and thereby model chemical interactions with significant accuracy. Instead of relying on limited scenarios and then focusing on physical experiments, researchers can simulate numerous scenarios and refine their hypotheses before testing a closer-to-final product in the lab. As a result, quantum computing is predicted to greatly change pharmaceutical research and lead to quicker creation of new drugs.

The advancement in scenario simulation could translate directly into litigation. Experts in product liability cases, for instance, currently analyze a limited number of scenarios to assess defect or foreseeability. Quantum computing could enable them to simulate hundreds or thousands of variations, generating a broader, more detailed evidentiary record.

These enhanced simulations could benefit both plaintiffs and defendants. Plaintiffs may use them to demonstrate that harm was likely across a wide range of conditions. Defendants could simulate the occurrence and show that it could only occur under rare or unforeseeable circumstances. Early adopters of quantum tools could gain a significant strategic advantage.

At the same time, these developments will raise familiar evidentiary issues. Courts will still need to evaluate whether quantum-generated evidence is reliable, testable, and reproducible under Daubert. Questions of transparency may become more complex if opposing parties lack access to comparable technology. Attorneys with a working understanding of quantum methods will be better equipped to address these challenges.

DISCOVERY REIMAGINED: QUANTUM-ACCELERATED ANALYSIS

Over the last 25 years, discovery has changed significantly due to the rapid growth of digital information. Moreover, with e-discovery, there is "hidden" information to find and disclose. Historically, in large lawsuits, teams of attorneys and staff would review thousands or perhaps millions of documents for relevance, privilege and responsiveness. This process was obviously time-consuming and expensive.

Artificial intelligence and machine learning have already improved document review by increasing speed and accuracy. Courts have largely accepted these tools and their methodologies.

Quantum computing is positioned to make another leap forward for large-scale document review. Quantum algorithms are especially adept at solving optimization problems, including the identification of related documents, the determination of communication methods, and the detection of patterns of concealment or spoliation. They can process and categorize documents far faster and on a larger scale than classical computers. These quantum algorithms will be better able to tackle discovery-intensive large lawsuits.

Quantum systems will make discovery much more efficient by sorting and analyzing data faster than ever before. As with earlier technologies, attorneys need to know how these tools work, including their limitations and potential pitfalls. If they do not, then they are poorly positioned to supervise their use or to respond when opposing counsel challenges the methodology. Those who learn about quantum tools early will probably work more efficiently and have better strategies.

CONCLUSION

Quantum computing is moving from theory to practical reality, with meaningful implications for encryption, discovery and evidence. While it will not replace classical computing, its ability to disrupt existing encryption and expand simulation capabilities introduces both risks and opportunities.

As post-quantum cryptography becomes standard and quantum-enhanced tools enter legal practice, attorneys will need to understand these technologies as part of their professional obligations. Those who proactively engage with these developments will be better positioned to safeguard client data, evaluate emerging forms of evidence, and advocate effectively in a changing technological landscape.

Richard Marsh is an attorney in Flaherty's Morgantown, West Virginia, office, focusing on trust and estate planning, administration and litigation; real property; general business representation; and municipal law. He has developed a growing interest in cybersecurity and data privacy issues. Richard is expanding his practice to help clients safeguard sensitive information, manage cyber risks, and navigate the legal implications of data breaches and digital asset protection. He may be reached at 304.225.3057 or rmarsh@flahertylegal.com.