RAND

Research Report

JAMES DIMAROGONAS, MICHELLE GRISÉ, MAYA BUENAVENTURA,
ERIK SILFVERSTEN, ANDREW J. LOHN, JAMES M. ANDERSON,
BETHANY SAUNDERS-MEDINA

The Quantum Age and Its Impacts on the Civil Justice System

For more information on this publication, visit **www.rand.org/t/RRA1020-1**.

About RAND

RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. To learn more about RAND, visit www.rand.org.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/research-integrity.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif.
© 2025 RAND Corporation
RAND® is a registered trademark.

Cover: Composite design by Carol Ponce adapted from images by MF3d/Getty Images and Arturbo/Getty Images

Limited Print and Electronic Distribution Rights

This publication and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited; linking directly to its webpage on rand.org is encouraged. Permission is required from RAND to reproduce, or reuse in another form, any of its research products for commercial purposes. For information on reprint and reuse permissions, please visit www.rand.org/pubs/permissions.

About This Report

Quantum computing technologies promise to offer new capabilities never previously thought possible—such as breaking encryption and searching supermassive datasets for intricate patterns—and revolutionize certain industries along the way. In this report, we examine the potential impact of quantum computing on the civil justice system, the legal profession, and industries that rely on the civil justice system, such as insurance companies. To explore how the advent of quantum computing may affect data security, data privacy, and liability, we conducted a comprehensive review of relevant legal and regulatory frameworks, and we interviewed stakeholders in the justice system, including lawyers, judges, court technology experts, and law enforcement experts. Participants in the civil justice system—such as legal firms, judges, court personnel—and industries that rely on liability and privacy laws—such as insurance and health care companies—will find value in the discussion of emerging implications of quantum computing technologies.

Institute for Civil Justice

The RAND Institute for Civil Justice (ICJ) is dedicated to improving the civil justice system by supplying policymakers and the public with rigorous and nonpartisan research. Its studies identify trends in litigation and inform policy choices concerning liability, compensation, regulation, risk management, and insurance. The Institute builds on a long tradition of RAND research characterized by an interdisciplinary, empirical approach to public policy issues and rigorous standards of quality, objectivity, and independence. ICJ research is supported by pooled grants from a range of sources, including corporations, trade and professional associations, individuals, government agencies, and private foundations. All its reports are subject to peer review and disseminated widely to policymakers, practitioners in law and business, other researchers, and the public. The ICJ is part of the Justice Policy Program within RAND Social and Economic Well-Being. The program focuses on such topics as access to justice, policing, corrections, drug policy, and court system reform, as well as other policy concerns pertaining to public safety and criminal and civil justice. For more information, email justicepolicy@rand.org.[1]

Funding

Funding for this research was provided by gifts from RAND supporters and income from the operation of ICJ.

[1] This paragraph was updated in January 2026 to reflect that this work was completed within ICJ.

Acknowledgments

The authors would like to acknowledge thoughtful reviews from Nicholas M. Pace, Teddy Parker, and Jean-François Blanchette.

Summary

Issue

For the past half-century, computer processing power has doubled roughly every 24 months. As transistors—the basic elements of digital computers—become smaller, they also become faster, more efficient, and more resilient. Coupled with accelerating innovations in algorithms, software, business models, and marketing strategies, these exponential improvements have created opportunities for new devices and applications.

Engineers are now at the point where they cannot make transistors any smaller without fundamentally changing the way they physically operate. As a result, the major players in digital computing are now looking toward the next big innovation that may fuel yet another era of exponential growth in technological capabilities and opportunities: quantum computing.

In this report, we investigate the potential impact of quantum computing on the civil justice system. As of December 2024, the U.S. justice system has struggled to adapt to the existing reality of the digital computer age. Both national and international cyber laws are still evolving as they try to catch up with emerging cybersecurity threats while data privacy laws are continuously lagging behind big data analytics and artificial intelligence (AI) technologies.

We conducted a comprehensive review of relevant legal and regulatory frameworks that will be affected by quantum computing, and we interviewed stakeholders in the civil justice system, including lawyers, judges, court technology experts, and law enforcement experts.

There are three specific domains in which quantum computing will be particularly relevant to the civil justice system: cryptography, liability and insurance, and privacy.

Cryptography

Law firms, insurers, and courts all rely on encryption to protect sensitive data on clients, litigants, medical records, and privileged communications. This reliance on encryption matters both when they *store* the data on servers, cloud services, mobile devices, laptops, and desktops and when they *transmit* the data over wired and wireless networks, including the internet and email. Quantum technologies that can break this encryption represent a particular threat to the ability of the civil justice system to protect sensitive data as required by professional norms, laws, and legal ethics.

Liability and Insurance

The fact that quantum computers are more error-prone than digital computers presents significant difficulties. The separation between quantum components and digital components of computing systems will compound the difficulty of assigning fault to different parts of the systems and different manufacturers. The fact that we cannot peek into the quantum process

itself, and the fact that the process is difficult to understand and explain, may make discussions about liability for the inevitable errors in quantum computing very challenging.

The error-prone nature of computations performed by quantum computers will also likely increase demand for novel insurance products. Entities that rely on quantum computers to perform critical tasks will seek to mitigate the consequences of such errors. While the age of quantum computing is not yet upon us, the insurance industry should begin developing the kinds of new insurance products that will be needed when this age arrives. This will require a careful understanding of the relevant risks.

Quantum computing will also allow insurance companies to improve how they perform risk assessments. Because quantum computers will be able to process vast amounts of data nearly instantaneously, the algorithms used by insurance underwriters today may seem rudimentary, unsophisticated, and uncomprehensive in comparison to those enabled by quantum computing and potentially used by insurance underwriters of the future.

Privacy

Quantum computing has the potential to significantly improve AI systems and the ability to search large datasets for patterns and correlations. There are four overarching privacy implications related to quantum-based AI systems: the de-identification of data, the right to be forgotten, the fair use of information, and the transparency of decisions based on private data.

These implications will challenge compliance with existing U.S. and international privacy laws, including the European Union's General Data Protection Regulation.

Recommendations

- Civil justice system stakeholders should focus on securing sensitive client data by conducting regular risk assessments and keeping up to date on encryption standards and identified cyber threats. Stakeholders should follow the development of quantum-secure encryption solutions and be ready to adopt them into their information technology infrastructure as soon as adoption is feasible.
- Civil justice agencies and institutions should be prepared to navigate new forms of liability and potential litigation arising from the advent of quantum computing. Insurance companies should work with technical experts to quantify the risks associated with and take advantage of the capabilities offered by quantum computing to price risk more efficiently.
- Civil justice agencies and institutions should be prepared to build on emerging conceptions of data privacy and integrate them into existing laws and regulations.
- Civil justice system stakeholders should track regulatory developments related to quantum computing in Europe and China and consider whether the United States might follow.

Contents

About This Report iii
Summary v

CHAPTER 1
Introduction 1
Background 2
Quantum Computing: What It Is and How It Differs from Digital Computing 5
Study Objectives and Approach 6
Report Structure 7

CHAPTER 2
Applications of Quantum Computing 9
What Challenges Do Quantum Computers Raise? 12

CHAPTER 3
Challenges for Protecting Privileged or Sensitive Information 17
Lawyers and Encryption-Protected Client Information 17
Courts and Databases, Digital Evidence, and Digital Signatures 23

CHAPTER 4
Challenges for Litigation, Risk Management, and Insurance 27
Implications for Civil Litigation 28
Implications for Risk Management and Insurance 29

CHAPTER 5
Challenges for Data Privacy 31
Evolution of Quantum Artificial Intelligence and Machine Learning 31
Implications for Data Privacy 32
Implications for U.S. Privacy Laws 34

CHAPTER 6
Challenges in the Global Regulatory Environment 41
The European Union 41
China 45
U.S. Export Controls on Quantum Technologies 46

CHAPTER 7
Recommendations 49

APPENDIXES

A. Context for Quantum Computing: History and Timeline 53
B. Principles of Quantum Mechanics and Quantum Computers 59

Abbreviations 65
References 67

CHAPTER 1

Introduction

Over the past several decades, the increase in digital computing capabilities has revolutionized and changed the way people work and live. These dramatic changes were possible, in large part, by continually increasing the number of transistors that can fit on a chip over time without increasing cost. As chips became exponentially more powerful, humans' ability to collect, store, and process data increased exponentially as well, leading to the development of new products and services at ever increasing rates. Engineers are now reaching the point where they cannot make transistors any smaller without fundamentally changing the way they physically operate. This means that technology is entering an era in which mankind continues to generate data at increasing rates without the ability to increase computational power to store and process these data. This is where quantum computing enters the picture.

Major players in digital computing are now looking toward the next big innovation that will fuel a new era of exponential growth in technological capabilities and opportunities. Quantum computers have been heralded as the solution to this problem. Quantum computers work in a completely different way than classical digital computers do. Today's classical digital computers are made of basic elements of computation (most often transistors on a silicon chip) that are either on or off—zero or one, respectively. Referred to as *bits*, these elements follow the regular laws of physics and are used to encode numbers and letters. Based on simple manipulations of these physical representations of zeros and ones, computers perform the complex tasks that humans see every day.

Quantum computing is based on the fact that, in the world of single particles like photons or electrons, physics behaves differently. The physics that worked in the macroscopic world do not always apply in this quantum world. The basic unit of computation, which has no analogue in our macroscopic world, is called a *qubit*. The behavior of qubits is described by a special branch of physics called *quantum mechanics*. A quantum computer, therefore, is a device designed to perform computations by manipulating elementary participles using quantum mechanical principles that do not have a direct analogue in classical physics. Therefore, understanding digital computers does not provide adequate insights into the inner workings, capabilities, and limitations of quantum computers. This means that current regulations and policies will need to adapt to these new realities and address their new capabilities and limitations.

The purpose of this report is to help policymakers think proactively about the legal, policy, and regulatory implications of quantum computing in the context of the U.S. civil justice

system. Much of this discussion would apply to other countries and regions of the world (and we do touch on some international implications), but it was not our intention to exhaustively address the international legal implications of quantum computing.

To accomplish our goal, we performed a literature review and conducted interviews with knowledgeable representatives of the legal and technical communities. Based on the information collected and drawing on the authors' deep experience and familiarity with both quantum computing and the civil justice system, we developed a set of relevant policy recommendations. In this report, we also provide a basic explanation of quantum computing and its capabilities and limitations. The intended audience includes legal practitioners, policymakers, businesspeople routinely involved in certain types of civil litigation, and technology developers who wish to understand the legal and policy implications of their products and design choices.

Background

For the past half-century, computer processing power has doubled roughly every 24 months at the same cost.[1] As transistors—the basic elements of digital computers—have become ever-smaller, they also have become faster, more efficient, and more resilient. Coupled with accelerating innovations in algorithms, software, business models, and marketing strategies, these exponential improvements have created opportunities for new devices and applications that have replaced many of the old ways of doing things. For example, the explosion of raw processing power and the continuous miniaturization of transistors allowed for the development of smartphones, which have more processing power than the National Aeronautics and Space Administration's (NASA's) supercomputers of the 1990s and have largely replaced our wired phone lines, our cameras, our rolodexes, our flashlights, our pagers, our maps, and so much more.[2]

Presently, scientists cannot make transistors any smaller without fundamentally changing the way they physically operate. As a result, the major players in digital computing are now looking toward the next big innovation that will fuel a new era of exponential growth in technological capabilities and opportunities: quantum computing. Major technology companies have started developing quantum computing technology because, without it, the digital computing race of the past few decades will most likely be reduced to a slow crawl.

Quantum computers work in a completely different way than classical digital computers. It is inherently difficult to explain how and why they work, and there will almost certainly be a considerable amount of mistrust, disinformation, and confusion about quantum computing capabilities. Initially, of course, this was also true of digital computers. When digital

[1] Tim Cross, "After Moore's Law," *The Economist Technology Quarterly*, March 11, 2016.

[2] Samantha Bookman, "15 Huge Supercomputers That Were Less Powerful Than Your Smartphone," *The Clever,* April 18, 2017.

computers were first invented, it was difficult to explain what a bit was or how a computation took place inside the computer. However, after several decades of living with computers, we have come to accept—often, albeit, with seeming blind faith—the basic premise of computing and how it works. Explanations of digital computing feel familiar and intuitive to many people because they have heard them so often. It will take time until people can talk about quantum computers in the same familiar way, and there is a long and arduous education process required by technologists and nontechnologists alike to reach a common understanding and common vocabulary regarding these new systems.

Quantum computing evolved in four years from the first basic theoretical concepts to the first technical demonstration of capabilities. In another nine years, the first commercially available quantum computing system (albeit a limited and flawed one) hit the open market (see Appendix A for a more detailed timeline of quantum computing development).[3] The history of digital computers highlights the difficulties of developing policies and regulations in response to new technologies. For example, digital computers were publicly acknowledged in 1946, and they almost immediately revolutionized the way people collect and use data. But it was not until the 1960s that concerns about the privacy implications of digital computing were raised, and it was not until 1966, with the passage of the Freedom of Information Act, that Congress actively began to address these concerns.[4] Currently, this space relies on an evolving patchwork of laws and regulations, both state and federal, as regulators struggle to keep up with new developments in digital computing. As new regulatory and oversight frameworks are developed to address issues with current information technologies, future potential technological breakthroughs should be addressed to ensure that policy and regulatory frameworks are flexible enough to adapt to new challenges as breakthroughs evolve.[5] To this end, it is important to understand some of the emerging challenges associated with quantum computing.

A driving force behind the U.S. government's effort to address quantum computers early is encryption. In Chapter 3, we describe how quantum computers may threaten our current cryptographic systems and standards, allowing unauthorized parties to read sensitive information or to modify or corrupt valuable information by decrypting it, modifying, and then re-encrypting it. In 2022, President Biden signed a memorandum that recommends public and private entities "prioritize the timely and equitable transition of cryptographic systems

[3] It is important to note, however, that a minority of researchers claim, and attempt to prove mathematically, that quantum computers will never provide any definitive advantage over digital computers. See Gil Kalai, "The Argument Against Quantum Computers," in Meir Hemmo and Orly Shenker eds., *Quantum, Probability, Logic: Itamar Pitowsky's Work and Influence,* Springer, 2020.

[4] Daniel J. Solove, "A Brief History of Information Privacy Law," in Kristen J. Matthews, ed., *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, 2nd ed., Practicing Law Institute, January 7, 2017.

[5] Gary E. Marchant, Douglas J. Sylvester, and Kenneth W. Abbott, "What Does the History of Technology Regulation Teach Us About Nano Oversight?" *Journal of Law, Medicine, and Ethics*, Vol. 37, No. 4, Winter 2009.

to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035."[6] To comply with the memorandum, in 2022, the National Institute of Standards and Technology (NIST) selected four post-quantum algorithms for standardization.[7] The National Security Agency went a step further: In 2022, it mandated all national security systems equipment and services that cannot use post-quantum algorithms to be phased out by 2030.[8]

Several quantum computers are already available on the open market. While these computers do not offer the full benefits of universal quantum computing, they are increasingly powerful. In 2010, the D-Wave quantum annealing computer became the first commercially available system.[9] Early devices were sold to such government agencies and corporations as NASA and Lockheed Martin. In 2019, Volkswagen demonstrated the use of a D-Wave quantum computer for bus route and traffic optimization in Lisbon in live driving conditions for three days.[10] IBM in 2016 and Rigetti in 2017 made their quantum computers available over the web for researchers for remote use. In 2019, IBM announced that it was building the first European quantum computer in Germany and in 2023 unveiled its IBM Quantum System Two.[11] These computers are still primarily used for research and experimentation, but considerable effort is being made to find practical uses in the areas of optimization, machine learning (ML), and materials design. Even though they are not significantly more powerful than digital computers, they are actively being used to solve real-world problems, and this has policy and regulatory implications.

---

6 White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," May 4, 2022.

7 Standardization is important to facilitate interoperability between different systems and organizations. NIST selected one algorithm for general encryption and three algorithms for digital signatures. For further details, see NIST, *Status Report on the Third Round of NIST Post-Quantum Cryptography Standardization Process*, update 1, IR 8413, 2022.

8 National Security Agency, "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ," September 7, 2022.

9 Alex Knapp, "D-Wave Sells Quantum Computer to Lockheed Martin," *Forbes,* May 25, 2011.

10 Volkswagen Group, "Where Is the Electron and How Many of Them?" *Global Energy World*, November 6, 2019. Throughout this report, we use the term *optimization* in its mathematical definition as determining the best result (best defined quantitatively as a maximum or minimum with respect to a set of chosen metrics) over a set of possible outcomes, given a set of desired constraints.

11 Jacob Aron, "Try Your Hand at Programming IBM's Online Quantum Computer," *NewScientist,* May 4, 2016; Tom Simonite, "The Quantum Computer Factory That's Taking on Google and IBM," *Wired,* June 20, 2017; Douglas Busvine, "IBM, Fraunhofer Partner on German-Backed Quantum Computing Research Push," Reuters, September 10, 2019; IBM, "IBM Debuts Next-Generation Quantum Processor: IBM Quantum System Two, Extends Roadmap to Advance Era of Quantum Utility," December 4, 2023.

Quantum Computing: What It Is and How It Differs from Digital Computing

Often, the term *quantum computer* is misunderstood. Most people might think that a quantum computer is a new type of computing machine that basically does the same things as a normal computer—just better or faster. For the most part, however, aside from a few specialized tasks that quantum computers perform more quickly than digital computers, this perception is inaccurate. Quantum computing is an entirely new way of performing computing tasks. It relies on new types of devices and incorporates new processes for using those devices to perform tasks. While some of those tasks are similar to the typical computing tasks of digital computers today, many of them are tasks for which these new devices are especially well suited.

Today's classical digital computers comprise basic elements of computation (most often transistors on a silicon chip) that are either on or off—zero or one. Referred to as *bits,* these elements follow the regular laws of physics and are used to encode numbers and letters. Using simple manipulations of these physical representations of zeros and ones, computers perform the complex tasks humans see every day.

Transistor-based computing has grown increasingly powerful over the decades because transistors have been getting smaller and smaller, allowing for more and more bits to be on a square-inch chip. But transistors are approaching physical limits on how small they can be made, with production versions of about 3 nanometers (nm), and some experimental ones at just 1 nm (about one–one-hundred-thousandth the size of a human hair). Anything smaller than that would be in the realm of atoms and subatomic particles, and so instead of using a transistor-like object to work as a bit, atoms, ions, electrons, and various particles would have to perform the same task. The problem and promise of quantum computing is that, at that level, the classical laws of physics no longer apply, and certainty gives way to probability and a host of other strange behaviors that are inconsistent with the normal laws of physics. Quantum computers would exploit these unexpected, fantastical properties to allow, for example, parallel processing on a massive scale, providing the ability to quickly solve problems that current computing resources would take years to address.

However, unlike in the macroscopic world that is the basis for digital computing, in the quantum world of single particles, such as photons or electrons, which are the basis of quantum computing, things behave differently. The physics that worked in the macroscopic world do not always apply in this quantum world. Instead, a photon can be looking up and down at the same time, while a particle can be in two different positions at the same time. In other words, something can be on *and* off, or zero *and* one. This basic unit of computation, which has no analogue in our macroscopic world, is called a *qubit*. The behavior of qubits is described by a special branch of physics called *quantum mechanics*. Quantum mechanics applies to anything smaller than an atom. A quantum computer, therefore, is a device designed to perform computations by manipulating elementary particles using quantum mechanical principles that do not have a direct analogue in classical physics.

The three quantum mechanical principles that make computation possible are quantum *superposition*, *entanglement*, and *interference*. *Superposition* is the property of elementary particles to exist in multiple states at the same time: up *and* down, on *and* off. *Entanglement* is the ability of two particles to exist in a common, intertwined state that allows them to be manipulated in tandem over arbitrary distances. *Interference* allows particles to be in multiple places at the same time and even interfere with themselves. Superposition is what allows for the massive parallelism in the computation. Entanglement allows the computation between the qubits to take place. Interference is what allows users to extract the final result from the output of the calculation.

All this may seem counterintuitive, but this incredibly complex behavior of qubits is well suited for solving equally complex, multidimensional problems far more efficiently than traditional computers. The subatomic nature of the qubits move computing into a world where the laws of physics that we are used to no longer apply and where millions of calculations can take place simultaneously.

Readers interested in an in-depth analysis of the quantum mechanical principles that make computations with qubits possible and the types of quantum computers currently theorized can turn to Appendix B.

Study Objectives and Approach

U.S. civil justice stakeholders, including courts, law firms, and insurers, have traditionally been slow to react to technological advances, let alone prepare for an uncertain quantum future. The intent of this report is to highlight challenges the civil justice system will need to address to better prepare for a possible quantum future. These measures will also help address concerns raised by existing technology. As of December 2024, the U.S. justice system has struggled to adapt to the reality of the digital computer age, even one that is still based on silicon transistors. Current cyber laws, both national and international, are still evolving and trying to catch up with emerging cybersecurity threats, while data privacy laws lag behind big data analytics and artificial intelligence (AI) technologies. The consequences of failing to adapt legal and regulatory structures to recent technological innovations will become more acute in the coming years as we move beyond digital computing.

Literature Review

In the literature review, we assessed the state of quantum computing, its maturity, and its potential for revolutionizing certain applications and providing services that are not possible with any future digital computer. We also looked for ways quantum computing could affect the civil justice system, such as civil justice policies, laws, regulations, and civil litigation. We considered different technical approaches to quantum computing and how these approaches can be used to break current encryption, develop quantum simulations to design new materials and new drugs, and create new quantum AI and quantum data analytics. Doing so

entailed considering hundreds of documents, including academic literature, reports, media sources, websites, and *gray literature* (i.e., unpublished or informally published working papers, white papers, government documents).

Interviews

We talked with approximately two dozen civil justice and technology actors, including judges, lawyers, court technology experts, legal researchers, quantum computing researchers, information technology practitioners, and cybersecurity experts. We interviewed these individuals by phone or in person; the interviewees did not receive incentives for participation. The interviewees were selected to represent a variety of perspectives on quantum computing technologies, the use of encryption in the courts and the legal profession, privacy implications of big data analytics and AI, and liability and insurance issues.

Limitations

Readers should keep several limitations in mind when considering the key findings and implications in this report. There were doubtless important perspectives that were not captured in our interviews. Thus, study findings should not be interpreted as touching on all possible implications of quantum computing. Second, interview data were based on self-reports by respondents who participated voluntarily; thus, the interview data could also reflect respondents' own biases. We sought to mitigate these limitations with the literature review and by employing our team's deep technical expertise and familiarity with the civil justice system.

Report Structure

The remainder of this report proceeds as follows: In Chapter 2, we provide a discussion of the basic principles and potential applications of quantum computing. In Chapter 3, we describe how advances in the field will affect encryption and how law firms, courts, and insurers will need to change the way they handle and protect client data. In Chapter 4, we argue that quantum computing presents both new challenges and opportunities for litigation and risk management. In Chapter 5, we consider the privacy implications of quantum computing.

In Chapter 6, we focus on the global impact of quantum computing on national and supranational regulatory schemes, with particular attention to the European Union (EU) and China. In Chapter 7, we conclude with a series of recommendations detailing how the civil justice system can adapt to the coming quantum age.

The report also has two appendixes that provide further in-depth information on the history, timeline, and principles involved in developing quantum computing.

CHAPTER 2

Applications of Quantum Computing

While the quantum age is just beginning, technologists already know specific applications that will surface in the future. As Figure 2.1 illustrates, one can see that the use of quantum computers in simulation will affect applications in physics, while quantum communications—encryption—and quantum algorithms will affect math, quantum machine learning (ML) will affect ML applications and biology, and quantum chemistry will affect chemistry and biology applications.

Although at this point, these applications are largely theoretical, the applications described earlier in this report will bring with them both new opportunities and new risks.

In the next sections, we describe some of the most-predicted applications for quantum computing, such as encryption, pattern recognition, AI and ML, simulations, and optimizations. These areas are ones we believe are most likely to have relevance to the civil justice system, although there will likely be applications and second-order effects that have other civil justice system implications.

Breaking Encryption

This is the one of the most touted and concerning capabilities of quantum computing. Once quantum computers of sufficient size become available, their capacity to break encryption means that current cryptographic standards will be vulnerable.

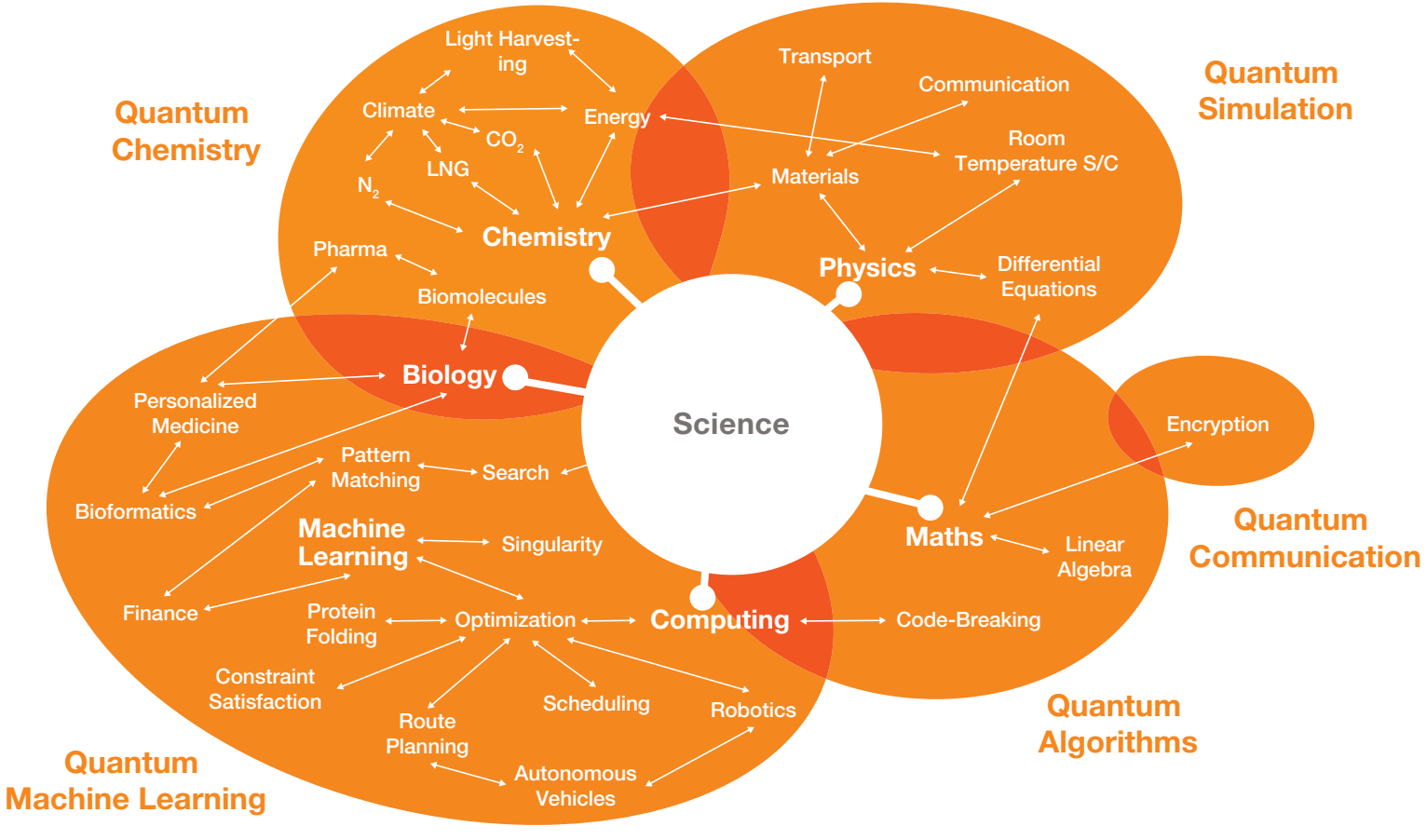
As a result, data that are currently protected by encryption could become readable in the future. A bad actor simply needs to make a copy of existing encrypted data today and then wait until quantum computing technology makes it possible to decrypt these data—in effect, banking encrypted data for later decryption. This possibility makes it imperative to change the way encryption is handled and make fundamental changes to our data management systems and processes.

Searching Data for Patterns

Because of the fundamentally different way that quantum computers store and process information, they could theoretically scale the number of qubits linearly while increasing the amount of information they can process exponentially. Each time a qubit is added, the

FIGURE 2.1

Future Applications of Quantum Computing



SOURCE: Infographic by Jeremy O'Brien and Pete Shadbolt at PsiQuantum. Used with permission.
NOTE: N_2 = nitrogen gas, LNG = liquefied natural gas, CO_2 = carbon dioxide, pharma = pharmaceuticals, S/C = superconductor.

amount of states that can be represented is doubled.[1] In practical terms, this means that if universal quantum computers of sufficient size become a reality, it would be possible to load all the knowledge of the world on a single quantum chip and process it in seconds or minutes.

The implications of this capability are enormous: Users may be able to see patterns in data that were not previously detectable. Users may be able to search for these patterns in vast datasets (e.g., in such fields as bioinformatics and finance) at speeds that are simply not possible today.

Artificial Intelligence and Machine Learning

The development of increasingly larger sets of data will require more-efficient techniques for finding and retrieving information and extracting patterns from these datasets. The ability to extract complex patterns from these large datasets in reasonable amounts of time will have significant impact for AI and ML applications (shown in Figure 2.1). In a quantum era, AI and ML will most probably use a combination of classical and quantum computing techniques. Some techniques, such as artificial neural networks, are more efficiently performed on classical computers, but some computations will perform faster and more efficiently on a quantum computer. For example, Grover's algorithm can be used to search large databases quadratically faster than a classical computer.[2] The Harrow-Hassidim-Lloyd (HHL) algorithm can solve large systems of linear equations exponentially faster than a classical computer (under certain conditions and certain types of problems).[3] Quantum random access memory can provide exponentially more addressable memory.[4] All these techniques could provide AI and ML capabilities that are beyond the capability of any classical computer.

Using these more-intelligent algorithms will reduce the ability to protect privacy because it will be significantly easier to connect a person's identity with personal data collected over time. It will also affect the way technologists design autonomous vehicles and robotics, allowing machines to exhibit significantly more-complex and nuanced behaviors and decisionmaking.

[1] Cathal O'Connell, "Quantum Computing for the Qubit Curious" *Cosmos*, July 5, 2019.

[2] Christof Zalka, "Grover's Quantum Searching Algorithm is Optimal," *Physical Review A*, Vol. 60, No. 4, 1999.

[3] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd, "Quantum Algorithm for Solving Linear Systems of Equations," *Physical Review Letters,* Vol. 103, No. 15, October 2009; Scott Aaronson, "Read the Fine Print," *Nature Physics,* Vol. 11, No. 4, 2015.

[4] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone, "Quantum Random Access Memory," *Physical Review Letters,* Vol. 100, April 2008.

Quantum Simulation

Studying properties of materials, chemicals, and pharmaceuticals at the atomic and subatomic levels cannot be done with classical computers; it requires the use of quantum mechanics.[5] A quantum computer would be able to simulate and study the quantum behavior of molecules directly and, therefore, more efficiently. This could open the door to discovering new pharmaceuticals tailored to a person's DNA, stronger materials, and catalysts that extract carbon from carbon dioxide in the atmosphere. It could also allow us to combat previously unknown virus outbreaks in record time by simulating the viral interactions with human cells at the atomic level. In short, quantum simulation could transform the way pharmaceutical, chemical, biochemical, and material design companies operate and develop products.

Optimization

Many everyday problems can be formulated as optimization problems, from estimating stock market returns to optimizing supply chain deliveries. With quantum computers, important calculations could be made at rates that today are impossible. For example, quantum computers will allow users to optimize entire complex supply chains, travel routes, and distribution systems. Optimization touches practically every industry and will affect multiple scientific disciplines.

What Challenges Do Quantum Computers Raise?

By their very nature, quantum computers are significantly different from classical digital computers. These differences will challenge expectations and processes in ways we discuss below.

Lack of Visibility

Fundamental quantum mechanical properties make it impossible to measure what is happening inside a quantum chip. It was difficult enough to observe the internal workings of digital silicon chips, but scientists developed ways to measure or indirectly observe what was occurring inside the chip. While the chip itself was a kind of black box, it was possible to metaphorically poke at it, rattle it, and maybe take small peeks at some of its contents. For example, digital forensics enables the user to create a fairly accurate copy of what the computer is doing at a particular time.

[5] In 1982, Richard Feynman showed that simulating quantum mechanical systems with digital computers is very inefficient and becomes exponentially harder as the size of the system under study increases (Richard P. Feynman, "Simulating Physics with Computers," *International Journal of Theoretical Physics*, Vol. 21, 1982).

The properties of quantum computers make forensic investigation much more difficult, if not impossible. By trying to observe a qubit, its entanglement—and hence its computation—is automatically destroyed. Indeed, the only way to know that the computation even took place is because of the resulting output. In other words, a quantum computer is a true black box. The box disappears with any attempt to look in or poke at it. With a quantum computer, unlike a digital one, the inputs and outputs are visible, but there is no way of creating a copy of what is loaded onto the qubits.[6]

Moreover, quantum computers require the ability to store massive amounts of data to function. This will only add to the lack of visibility into its inner workings.

Propensity of Quantum Processes for Errors

If we cannot see what is happening inside the black box of the quantum computer, how can we trust that the computation it produces has been done correctly? While digital computers produce very few errors, quantum computers (at least early instantiations for several years to come) are rather error-prone because of the relative instability of current qubits. If a digital processor produces an error, there is a high probability that the computer will crash, and the user will immediately know that something has gone wrong. This happens because the digital processor is not only responsible for the computation but also for running the entire computer. However, a quantum computer will provide no such indication that something has gone awry because the quantum processor is reserved for only computations and not for running the different processes responsible for the operation of the quantum computer itself. It will not crash.

At the same time, quantum computers are very sensitive to environmental conditions that can corrupt the output of the computation. Because these errors are not visible, a user-cannot tell if they occurred. From the outside, an observer sees a computer that is either behaving perfectly or is not producing a result, but it will not be immediately obvious that an error has occurred.

To check, the user can verify that the result is correct. However, not all results will be easily verifiable.

- *Problems with easily verifiable solutions:* An example of this challenge is breaking encryption. It is very difficult to factor a large number into primes. However, it is very easy to verify if the two primes multiplied together produce the original number. This can even be done with pencil and paper.
- *Problems without easily verifiable solutions:* For searching large datasets or large optimization problems, it may be very difficult or even impossible to verify if the result produced by the quantum computer is correct.

[6] William Wootters and Wojciech Zurek, "A Single Quantum Cannot Be Cloned," *Nature,* Vol. 299, No. 5886, 1982.

Designers of quantum computers address the potential for errors by adding error correction. By adding redundant qubits, one can get a smaller number of error-resistant logical qubits.[7] This approach is also currently used in digital computers and digital communications. With quantum computers, however, the challenge will be greater because the probability of error will depend on the complexity of the problem the quantum computer is asked to solve. The greater the level of complexity, the higher the probability of error. Thus, while it is possible to quantify the probable error rate for a digital computer as estimated in errors per million computations, there is currently no equivalent error metric for quantum computing. This is mainly because the error rate depends on the complexity of the problem it is being used to solve and not on the number of computations. However, a complex metric based on the number of qubits used and the quality of each qubit may be possible. Far into the future, with quantum computers of sufficient size, this may not be an issue. But for the foreseeable future, the near-term systems that are and will be available on the market (often termed *noisy intermediate-scale quantum* technologies) will have to address this issue.

Difficulty of Explaining What Makes Quantum Computers Work

If quantum computers will produce errors but we cannot be sure of their error rate, how do we explain errors when they occur? This becomes a challenge for two reasons. First, as previously discussed, there are no simple, agreed-on explanations for basic quantum phenomena. For example, one common explanation for the superposition of states inside the qubits is that a qubit exists in multiple parallel universes. Once the state of the qubit is measured, these universes branch off.[8] For a quantum physicist, this may seem like a perfectly plausible explanation, albeit not the only possible explanation for this phenomenon. However, to most people outside the world of quantum physics, it sounds very weird and counterintuitive.

Initially, of course, this was also true in the digital age. As previously mentioned, when digital computers were first invented, it was difficult to explain what a bit was or how a computation took place inside the computer. However, after several decades of living with computers, we have come to accept—often with seeming blind faith—the basic premise of how computing works. Explanations of digital computing feel familiar and intuitive to most people because they have heard them so often. Many have come to trust these explanations without pausing to verify them or really trying to understand what is going on inside a transistor or on a thin layer of silicon.

[7] *Redundant* here means in the sense of representing each qubit in multiple physical copies to detect and correct errors among them.

[8] This theory was first proposed by Hugh Everett in 1956 (Hugh Everett, *Theory of the Universal Wave Function*, Princeton University, 1956). The "many worlds" formulation was popularized by Bryce Dewitt in the 1960s and 1970s (Bryce S. DeWitt, "Quantum Mechanics and Reality," *Physics Today,* Vol. 23, No. 9, 1970). A less technical presentation of this theory (while not less puzzling) is presented in Chad Orzel, "What The Many-Worlds Interpretation of Quantum Physics Really Means," *Forbes,* January 5, 2016.

Second, humans live in a macroscopic world. They rely on their senses to verify the truth about the world. People's expectations of how the world works are based on observations of how macroscopic objects behave. In the quantum world, however, objects behave differently, thus violating a person's basic accumulated intuition about how physical objects actually behave: An object cannot be in two different states at the same time. Objects cannot be entangled. But objects can do both these things in the quantum world. These quantum properties violate humans' basic understanding of the world, and humans will have to adapt to think in quantum mechanical terms.

Mistrust and Confusion About What Quantum Computing Really Is

As difficult as it is to understand and explain what quantum computers do and how they do it, this difficulty is compounded by the amount of misinformation surrounding the term *quantum*. In fiction, the term is frequently used as a synonym for anything too advanced for human comprehension or something that simply sounds futuristic. In the *Star Trek* universe, for example, starships can be propelled with "quantum singularity" engines, and they can fire "quantum torpedoes."[9] One British newspaper theorized that the "force" described in the *Star Wars* movie franchise could in fact be the result of quantum entanglement.[10]

Even the basic terms used to explain quantum mechanics have been misused. For example, one possible explanation of superposition relates to the theory of parallel universes. In fiction, the idea of a parallel universe is most commonly associated with a reality that parallels our own. Our living counterparts—usually evil counterparts, for dramatic effect—can interact in both of these universes. In quantum physics, however, that is not what is meant by a parallel universe—nor do we mean that our evil twin in a parallel universe can affect qubits in this universe.

Even in nonfiction, there is frequent misinformation or misuse of the term *quantum*. For example, the news contains reports of "quantum teleportation," which imply the instantaneous transfer of information over a distance. In reality, this phenomenon is simply the transmission of entangled photons in a manner similar to how we use fiber-optic cables to transmit regular photons. This tendency toward misinformation makes it even more difficult to explain what a quantum computer is and how it works because the general public has been exposed to so many erroneous uses of related terms over the past several decades.

It is important to remember that the advent of digital computers led to scholarly concern and public debate about privacy issues and broader regulatory implications of what was then an emerging technology.[11] At the time, commentators did not fully understand how digital

[9] Michael Okuda, Denise Okuda, and Debbie Mirek, *The Star Trek Encyclopedia*, Pocket Books, 1994.

[10] Joseph Carey, "Star Wars the Last Jedi: Is 'the Force' of Kylo Ren and Rey REAL? Quantum Science Reveals," *Express,* December 17, 2017.

[11] See Pat Washburn, "Electronic Journalism, Computers and Privacy," *Computer Law Journal,* Vol. 3, No. 1, 1981; John T. Soma and Richard A. Wehmhoefer, "A Legal and Technical Assessment of the Effect of

computers worked, and they worried that digital computer capabilities would challenge compliance with existing legal and regulatory regimes. Over time, however, public understanding of the technology matured, and the legal system was sufficiently flexible to adapt.

In the coming years, judges, juries, and lawyers will have to become familiar with the technology behind advances in quantum computing. While there is a learning curve associated with all emerging technologies, the difficulty of explaining and understanding how quantum computers work—as shown in the preceding paragraphs—will represent a particularly acute challenge. Judges and lawyers may require additional training on complex technical concepts to adequately resolve cases involving quantum computing. The challenges posed by quantum computing will require legal practitioners to work together with technologists to increase their technical literacy. This challenge is not particularly new to quantum computing. As technology evolves, lawyers and judges have faced similar challenges in applying old concepts to new technologies.

In the next three chapters, we discuss specific implications of quantum computing that will affect the civil justice system: cryptography, liability, insurance, and privacy.

Computers on Privacy," *Denver Law Review,* Vol. 60, No. 3, 1983; Louise M. Benjamin, "Privacy, Computers, and Personal Information: Toward Equality and Equity in an Information Age," *Communications and the Law*, Vol. 3, No. 2, 1991; Suzan Dionne Balz and Olivier Hance, "Privacy and the Internet: Intrusion, Surveillance and Personal Data," *International Review of Law, Computers and Technology,* Vol. 10, No. 2, 1996.

CHAPTER 3

Challenges for Protecting Privileged or Sensitive Information

In this chapter, we consider the potential impacts of quantum technologies that can break encryption and these effects on the civil justice system and discuss policy options. There is little written on the implications of quantum computing for the civil justice system.[1] However, as previously noted, the rise of quantum computers will threaten the security of existing cryptographic processes, including encryption. This threat has important implications for practitioners seeking to safeguard sensitive information. There are two key issues to consider when it comes to breaking encryption: (1) the ability of an unauthorized party to read sensitive information and (2) the ability to modify or corrupt valuable information by decrypting, modifying, and re-encrypting it.

Lawyers and Encryption-Protected Client Information

Attorneys maintain significant amounts of valuable client information, including trade secrets, investment plans, business strategies, intellectual property, litigation strategies, family histories, and critical evidence.[2] Attorneys rely on encryption to protect these data when stored on servers, cloud services, mobile devices, laptops, and desktops, as well as when transmitted over wired and wireless networks, including through the internet and email.[3] Lawyers' billing records also contain clients' financial information (e.g., bank account numbers and Social

[1] A book from 2018 provides a high-level overview of the areas of law that might be impacted by breaking cryptography (Pavan Duggal, *Quantum Computing Law*, Cyberlaw University, 2018). In addition, an article from 2019 presents governance and regulatory frameworks for managing the development of quantum computing technologies (Walter G. Johnson, "Governance Tools for the Second Quantum Revolution," *Jurimetrics Journal*, Vol. 59, February 2019).

[2] Nathan Powell, "Electronic Ethics: Lawyers' Ethical Obligations in a Cyber Practice," *Georgetown Journal of Legal Ethics*, Vol. 29, No. 4, 2016; Alan W. Ezekiel, "Hackers, Spies, and Stolen Secrets: Protecting Law Firms from Data Theft," *Harvard Journal of Law and Technology*, Vol. 26, No. 2, Spring 2013.

[3] American Bar Association Center for Professional Development, "Encryption for Lawyers: Fulfilling Your Ethical Duties," continuing legal education training, American Bar Association Law Practice Division, September 28, 2016.

Security numbers). Many states require that such personally identifiable information (PII) must be encrypted when it is stored on mobile devices or transmitted through public networks.[4] Quantum technologies that can break encryption represent a particular threat to law firms that store and transmit sensitive information. The threat is even more pronounced for data that could remain sensitive for many decades (such as trade secrets, settlements, or sensitive family information). With the price of data storage falling rapidly, malicious actors could copy encrypted data today and store it until encryption is finally breakable. Even if data is safe from quantum computing today, risk assessment of future decryption sensitivity should be performed, and appropriate protections for data that may remain sensitive for long periods of time should be established. This may mean keeping certain categories of information offline or in cold rooms where the information would be difficult for malicious actors to obtain.

The fact that quantum computers might break the encryption that attorneys use to protect valuable and sensitive client information is especially worrisome because lawyers are already a frequent target of cyberattacks. According to the American Bar Association (ABA), attorneys often store some of their clients' most significant business information, and because law firms tend to have fewer cybersecurity protections than their clients, they are targets for cyberattacks.[5] The ABA's 2023 Cybersecurity TechReport indicated that nearly 30 percent of U.S. law firms reported experiencing a security breach at some point.[6] In 2021, *Forbes* reported that in May 2020 cybercriminals stole more than 700 gigabytes of data from New York law firm Grubman Shire Meiselas & Sacks, which represented many high-profile entertainers, including Bruce Springsteen, Lady Gaga, and Bette Midler. The hackers "initially demanded $21 million and later doubled it to $42 million and published over 2 gigabytes of Lady Gaga's contracts and other data on the dark web as proof of compromise."[7] In 2023, Orrick, Herrington & Sutcliffe, a law firm that *specializes in cyberattacks*, reported a major breach that affected more than 600,000 individuals, mainly customers of client organizations, such as Delta Dental and the U.S. Small Business Administration.[8] *Forbes* surmised

[4] Ezekiel, 2013, p. 657.

[5] Powell, 2016, p. 1238; Ezekiel, 2013, p. 650. In the introduction to its Formal Opinion 477R on securing communication of protected client information, the ABA's Standing Committee on Ethics and Professional Responsibility noted the following:

> Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client (ABA, "Securing Communication of Protected Client Information," Formal Opinion 477R, revised May 22, 2017).

[6] ABA, "Ensuring Security: Protecting Your Law Firm and Client Data," *Law Technology Today*, 2024.

[7] A. J. Shankar, "Ransomware Attackers Take Aim at Law Firms," *Forbes*, March 12, 2021.

[8] Ionut Arghire, "Law Firm Orrick Reveals Extensive Data Breach, over Half a Million Affected," *SecurityWeek*, January 5, 2024.

that law firms are especially attractive to hackers because the nature of the information they collect can have potentially high financial value.[9]

Ethical and Professional Considerations When Safeguarding Client Information

The ABA's *Model Rules of Professional Conduct* require lawyers and law firms to stay current on technologies that safeguard client data. The Model Rules advise on lawyers' use of technology to safeguard client data, specifically including: competence (Model Rule 1.1), confidentiality of information (Model Rule 1.6), and safekeeping property (Model Rule 1.15).[10]

The duty of competence under Model Rule 1.1 covers the competent use of technology. As of 2022, 40 states have adopted the ethical duty of technological competence.[11] Comment 8 to the rule states: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." Although this requirement is nebulous, the chief reporter of the ABA Commission on Ethics noted that this is because "a competent lawyer's skill set needs to evolve along with technology itself" and "the specific skills lawyers will need in the decades ahead are difficult to imagine."[12] State ethics opinions also avoid specific recommendations when it comes to technological issues because of how quickly technology evolves.[13]

Subpart (c) of Model Rule 1.6 on confidentiality of information requires that a lawyer "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[14] Comment 18 to the rule states that if a lawyer made "reasonable" efforts to prevent the access or disclosure of data, compromise of the data does not constitute a violation of Subpart (c).[15] The comment

[9] Shankar, 2021.

[10] ABA, *Model Rules of Professional Conduct*, 1983, last updated August 2023.

[11] Robert Ambrogi, "Another State Adopts Duty of Technology Competence for Lawyers, Bringing Total to 40," *LawSites* blog, March 24, 2022.

[12] Steven M. Puiszis, "Perspective: Technology Brings a New Definition of Competency," Bloomberg Law, April 12, 2016.

[13] "It is beyond the Committee's ability to conduct a detailed information technology analysis. . . . Even if we had that ability our analysis would soon be outdated" (Ethics and Practice Guidelines Committee, "RE: Ethics Opinion 11-01," memorandum to Iowa State Bar Association executive director, Iowa State Bar Association, September 9, 2011, p. 2).

[14] ABA, 1983.

[15] ABA, 1983.

also includes factors to be considered in making a determination of whether a lawyer's efforts were reasonable, such as

- sensitivity of the information
- likelihood of disclosure if additional safeguards are not employed
- cost of employing additional safeguards
- difficulty of implementing the safeguards
- extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[16]

Model Rule 1.15 on safekeeping property requires that a lawyer "appropriately safeguard" client property and the property of third persons that is in the lawyer's possession. This rule would be violated if lawyers stored sensitive client information on their personal devices or the cloud and a hacker accessed the information through the personal device or the cloud.[17]

The Model Rules do not contain a specific requirement stating that breaches of client information being stored by law firms must be disclosed.[18] However, there is an argument that "a duty to disclose the breach is implied under the fiduciary duties of loyalty and candor," and under the "spirit of the Model Rules" generally.[19] In addition, legal commentators argue that there *should* be an explicit duty to disclose a breach.[20] In light of these arguments and the ABA's evolving guidance on technology used to safeguard client data, it is possible that when quantum computing becomes a reality, an explicit duty to disclose breaches will exist. In addition, although there is no explicit duty to provide notification of a breach of sensitive client information generally, if a hacker accessed a law firm's billing records that contained the financial account numbers of individuals, disclosure of the breach would likely be required under state privacy protection laws.[21]

Preparing for Potential Encryption Breaches

On May 11, 2017, the ABA's Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477, which addresses Model Rules 1.1 (duty of competence) and 1.6 (duty of confidentiality).[22] Formal Opinion 477 notes that

[16] ABA, 1983.

[17] ABA, 1983; Louise Lark Hill, "Cloud Nine or Cloud Nein: Cloud Computing and Its Impact on Lawyers' Ethical Obligations and Privileged Communications," *Journal of the Professional Lawyer,* 2013.

[18] Ezekiel, 2013, pp. 649, 653–564, 657, 660–661; Powell, 2016, pp. 1237, 1249, 1251–1252.

[19] ABA, 1983.

[20] Powell, 2016.

[21] Ezekiel, 2013, p. 657.

[22] ABA, 2017.

> [a]t the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology [Model Rule 1.1]," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client [Model Rule 1.6]," lawyers must exercise reasonable efforts when using technology in communicating about client matters.[23]

The opinion adopts the language in the ABA Cybersecurity Handbook, which

> rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.[24]

The opinion reiterates that the five factors from Comment 18 to Model Rule 1.6, Subpart (c) should guide lawyers' "reasonable effort" determinations.

While the committee says that it is beyond the scope of the opinion to list reasonable steps under a specific set of facts, it offers seven considerations to be used as guidance. One of these considerations is understanding the nature of the threat. Thus, when quantum computers are able to break encryption, attorneys and firms will need to understand the threats posed to communications with clients and storage of client information.

Another consideration is determining how electronic communications about client matters should be protected. The opinion notes that "if client information is of sufficient sensitivity, a lawyer should encrypt the transmission and determine how to do so to sufficiently protect it."[25] The opinion also notes that "[a] fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances" and that reasonable efforts may entail "avoid[ing] the use of electronic methods or any technology to communicate with the client altogether."[26] In addition, the opinion notes that

> Model Rule 1.4 [Communication with Clients] may require a lawyer to discuss security safeguards with clients. Under certain circumstances, the lawyer may need to obtain informed consent from the client regarding whether to the use enhanced security measures, the costs involved, and the impact of those costs on the expense of the representation where nonstandard and not easily available or affordable security methods may be required or requested by the client.[27]

---

[23] ABA, 2017, p. 4.

[24] ABA, 2017, p. 4.

[25] ABA, 2017, p. 7.

[26] ABA, 2017, p. 5.

[27] ABA, 2017, p. 5.

With respect to "routine communication with clients" (i.e., communication of information that is not deemed sensitive), the opinion notes that "the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication."[28]

In other words, when communicating information with a client or storing client information, attorneys and firms should understand where on the spectrum (ranging from "normal or low sensitivity" to "highly sensitive") the information falls. The opinion does not provide any specific guidance on what constitutes highly sensitive information. However, it does provide some examples, including "proprietary information in highly sensitive industries such as industrial designs, mergers and acquisitions or trade secrets, and industries like healthcare, banking, defense or education. . . ."[29] Instead of offering a specific definition of highly sensitive information, the opinion notes that the sensitivity of information should be determined on a case-by-case basis by attorneys and their clients. The opinion mentions encryption as a way to protect the most sensitive information several times, but if quantum computers can break encryption, law firms and attorneys will need to determine how to best protect information in other ways.[30]

Firms and attorneys will need to understand the technology used to communicate and store information and potential threats to technology to determine the best means of protection. If a situation arises in which quantum computers can routinely break encryption, reasonable efforts may entail entirely avoiding use of electronic methods of communication and storage, at least until the development of a means of protecting highly sensitive electronic communication and information. As quantum computing or other next-generation technology becomes a more imminent threat to encryption, law firms will need to start discussing additional security measures with clients and discussing whether the costs of protective measures are justified given the sensitivity of the information and the likelihood of a breach.

An information technology expert we interviewed similarly recommended that to adapt to quantum computers and other potential breaches of client information, attorneys should identify any information they have that is sensitive or that might be valuable to a potential hacker.[31] The expert noted that if quantum computers could break encryption, lawyers with high-profile clients would likely be particularly targeted.

Law Firms and Consulting Outside Experts on Quantum Technologies

Ethical guidance issued by the California State Bar states that if an attorney "lacks the necessary competence to assess the security of the technology, he or she must seek additional

[28] ABA, 2017, p. 5.

[29] ABA, 2017, p. 6.

[30] ABA, 2017, p. 6.

[31] Court technology expert, phone interview with the authors, April 30, 2018.

information or consult with someone who possesses the necessary knowledge, such as an information technology consultant."[32] Similarly, as Blaustein, McLellan, and Sherer noted,

> in construing all of these Model Rules and comments, it is clear that attorneys who are not tech- [sic] must (1) understand their limitations; (2) obtain appropriate assistance; (3) be aware of the areas in which technology knowledge is essential; (4) evolve to competently handle those challenges; or (5) retain the requisite expert assistance. This list applies equally to data security issues, such as being aware of the risks associated with cloud storage, cybersecurity threats, and other sources of potential harm to client data, and can easily be extended to include awareness and understanding with respect to domestic and foreign data privacy issues.[33]

If a law firm is unsure about whether quantum computers pose a threat to sensitive client information or how best to protect information, the law firm should seek the assistance of outside experts and adopt encryption methods specified by NIST or other national authorities.

Courts and Databases, Digital Evidence, and Digital Signatures

We interviewed the chief information officer (CIO) for a large court system and two other court technology experts. These interviewees noted that courts have not started preparing for the introduction of quantum computers or the encryption implications outlined earlier in this report. There are multiple reasons for the lack of focus on quantum computers. First, the CIO and other individuals in charge of court technology whom we interviewed do not think quantum computers will have any practical uses any time in the near future.[34] Second, the interviewees suggested that courts tend to have conservative cultures and tend to observe how private industry adapts to new technologies before moving forward themselves.[35]

Another reason for the lack of focus on quantum computers and other novel technological issues an interviewee provided is that court technology budgets typically do not have enough buying capital to invest in cutting-edge technology.[36] Planning and preparing is centered

[32] California State Bar Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179, 2010.

[33] Stacey Blaustein, Melinda L. McLellan, and James A. Sherer, "Digital Direction for the Analog Attorney—Date Protection, E-Discovery, and the Ethics of Technological Competence in Today's World of Tomorrow," *Richmond Journal of Law and Technology*, Vol. 22, No. 4, 2016.

[34] Court technology experts, phone interview with the authors, April 30, 2018; CIO of a large court system, phone interview with the authors, April 16, 2018. We recognize these interviews may not reflect the current technological climate because of the rapid growth of technology in the past few years.

[35] Court technology experts, phone interview with the authors, April 30, 2018.

[36] CIO of a large court system, phone interview with the authors, April 16, 2018.

around a biannual budget cycle. Technology personnel tend to think more about gradual upgrades to existing technology and ways to make court technology marginally better. [37] Interviewees also said that individuals in charge of court technology also tend to focus on day-to-day priorities rather than big-picture issues.[38]

Access to Encrypted Judicial Data Repositories

Courts use encryption in two primary ways: to protect data being stored and to protect data being transported. A bad actor who used quantum computing technology or other technology to breach encryption would probably seek to breach encrypted data stores (which sit in a well-known location and contain known types of information) rather than encrypted information that is being transported (of which it is difficult to predict what type of information is transported when).[39] Data repositories protected by encryption include libraries of case documents, some of which (e.g., juvenile records) are deemed confidential by law. These case documents are sometimes available to the public but in other cases are sealed by the court. These documents or transcripts could contain a variety of highly sensitive information. If the court system relies on encryption to control access to this information, developments in quantum computing could threaten the confidentiality of this material.

Encryption is also used to protect information being transported. For example, a member of the public might be legitimately querying an online case management system to see the register of actions on a case. All this is public information, but the path is still encrypted as data moves from court servers to the person accessing the data. Because the information being transmitted is already technically public information, it is not likely that this information would be targeted by hackers unless the intent is to corrupt or slightly modify the information transported.[40] But other types of court information will be sensitive and will need to be protected during transportation, such as when a judge is accessing sensitive juvenile records.

Generally, most state courts do not allow or support evidence transmitted to the court directly in digital format. In most cases, litigants are required to deliver evidence in a physical medium. The evidence can stay digital in nature, but parties have to compress the evidence to a thumb drive or DVD and submit it to the court as evidence that is managed through the traditional evidence safeguarding process (e.g., put in a safe and stored according to regular chain-of-custody procedures).[41] From an efficiency standpoint, this process is suboptimal. An electronic manifest that holds all the digital evidence for a case would allow an attorney

[37] Court technology experts, phone interview with the authors, April 30, 2018.

[38] Court technology experts, phone interview with the authors, April 30, 2018.

[39] CIO of a large court system, phone interview with the authors, April 16, 2018.

[40] CIO of a large court system, phone interview with the authors, April 16, 2018.

[41] CIO of a large court system, phone interview with the authors, April 16, 2018.

to click on a particular exhibit rather than trying to find the exhibit on the correct thumb drive.[42] Federal courts use these types of electronic manifests, and some state courts are looking into similarly efficient ways to store and present electronic evidence.[43]

However, state courts may choose to slow the movement toward accepting digital information because offline evidence on thumb drives and DVDs would be safer from attacks.[44] In addition, if quantum computers pose a threat to digital evidence in the future, courts that have moved beyond storage on thumb drives and DVDs could return to methods of digital storage and transmission that are currently being used by state courts.[45] For example, in the aftermath of the SolarWinds cyberattack on government agencies in 2020 (in which case, management and electronic filing systems were hacked and many highly sensitive documents were exposed), the Administrative Office of the U.S. Courts sent a letter to all U.S. federal judges recommending that all courts issue a standard order that highly sensitive documents should be accepted for filing only in paper form or via a secure electronic device and should be stored in a secure paper filing system or a secure stand-alone system not connected to a network.[46]

One interviewee said that it is also important to remember that even physical evidence can be accessed and manipulated: There is a risk whether data are digital or not, and court systems should not let fear stop them from adopting useful technology.[47]

Digital Signatures

Both electronic signatures and digital signatures are used in court systems. Individuals often use an electronic signature on court documents when they are submitting or filing a document electronically. A digital signature is a specific type of electronic signature that is used to authenticate the sender of an electronic document (i.e., that the person signing the document really is the stated person) and the document's integrity (i.e., that the current document is identical to the one originally signed).[48] Digital signatures used for such documents as electronic court filings by attorneys could be threatened by quantum computers able to break encryption. Digital signatures are also used to securely sign an electronic file to ensure the authenticity of the document. Digital signatures will allow for the capture of metadata when a judge digitally signs a document—for example, what login was used and when was

[42] CIO of a large court system, phone interview with the authors, April 16, 2018.

[43] Court technology experts, phone interview with the authors, April 30, 2018.

[44] Court technology experts, phone interview with the authors, April 30, 2018.

[45] Court technology experts, phone interview with the authors, April 30, 2018; CIO of a large court system, phone interview with the authors, April 16, 2018.

[46] Jonathan Greig, "U.S. Court System Demands Massive Changes to Court Documents After Solarwinds Hack," *TechRepublic*, February 12, 2021.

[47] CIO of a large court system, phone interview with the authors, April 16, 2018.

[48] CIO of a large court system, phone interview with the authors, April 16, 2018.

the document signed. Although it is possible that quantum computers might compromise judicial digital signatures, it important to keep in mind that such image editing applications as Photoshop can falsify documents even when they are signed by hand. [49]

[49] CIO of a large court system, phone interview with the authors, April 16, 2018.

CHAPTER 4

Challenges for Litigation, Risk Management, and Insurance

It is still very early in the quantum computing revolution, which means that there are many unknowns and uncertainties. It is difficult to envision the types of threats quantum computers will be subjected to, and, more important, what new cyber threats quantum computers may facilitate.

Quantum computers will essentially be a hybrid of different computers that feature the quantum processor and several classical digital computing components made by a variety of manufacturers. These digital components will feed the quantum computation with data, monitor and correct for noise in the system, pass around massive amounts of data over traditional digital networks to enable the computation, and more. Each one of these digital components brings along its own inherent vulnerabilities, adding to the unknown vulnerabilities that quantum processors will introduce.

To complicate things further, the race to create the first quantum computers is leading designers to make risky choices in the architecture, the design of quantum computer languages, and the development of the underlying supporting libraries—just as designers did in the early days of digital computers. Many of today's cybersecurity vulnerabilities were built into designs as far back as the 1950s and 1960s, by the poor choice of computing architectures or insecure programming languages. A famous example of this was the choice of representing the year using two digits, which was highlighted as an issue as far back as 1958 and eventually led to the Y2K bug, which in the year 2000 cost the world hundreds of billions of dollars to fix.[1] Current computers are yet to be properly secured, and scientists are in the process of developing a new generation of even more complex quantum machines without any thought about their security. The complexity, the rush to get them working, and the inheritance of all the problems associated with digital computers may make quantum computers even more vulnerable. Therefore, the risks associated with their use and their power bring forth new potential liabilities.

[1] David Ferro, "The Unbelievable Bug of the 21st Century," editorial, *Standard-Examiner*, March 25, 2020.

Implications for Civil Litigation

Quantum computing–facilitated breaches of computer networks and confidential or sensitive information of businesses, nonprofits, and governments will undoubtably trigger significant litigation. Key questions that may be litigated include the following: Was there a duty to secure the information that was disclosed? Did the party whose duty it was to protect the information take reasonable efforts to protect it? How was the plaintiff harmed by the loss of confidentiality? There are also interesting variant questions. Imagine, for example, that the relevant confidential information was adequately encrypted against existing decryption approaches at time *x* when it was acquired by the malicious actor. But by time *y*, quantum computing has permitted decryption of the data. Was it negligent for the possessor of the sensitive data to lose possession of it even though it was adequately encrypted at one time? Finally, there are likely to be important insurance coverage questions that may affect whether these cases are brought—is this kind of loss covered by the relevant policy?

Quantum computing–enabled breach litigation would be possible in any industry, but a recent class action lawsuit related to one of the worst data hacks in the past decade could be instructive as we consider what the future might hold. In April 2024, National Public Data, a background-check data aggregator, announced a data hack that exposed 2.9 billion PII records. This hack was particularly dangerous because Social Security numbers were included in the data obtained by hackers and sold on the dark web.[2]

Plaintiffs filed a class action lawsuit against National Public Data. Under their cause of action for negligence in the complaint, plaintiffs alleged that "NPD owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards" and that "NPD breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII."[3] It is easy to imagine that quantum computing–enabled breaches could obtain even larger sources of PII, which could affect even larger populations.

Error Rate and Lack of Transparency

The nature of quantum computer operations will also raise interesting liability questions as quantum computers are integrated into the economy and used to control important processes or make decisions. As noted in Chapter 2, quantum computers are relatively error-prone. It is also difficult or impossible to observe their functioning. Moreover, the separation between quantum components and digital components of computing systems will compound the difficulty of assigning fault to different parts of the systems and different manufacturers. The fact that one cannot peek into the quantum process itself and the fact that the process is difficult to understand and explain will complicate attribution of fault. If these machines are used to design life- and safety-critical systems or are used to make sensitive decisions, errors will

[2] *Hofmann v. Jerico Pictures, Inc.*, 0:24-cv-61383, Southern District of Florida, August 1, 2024.

[3] *Hofmann v. Jerico Pictures, Inc.*, 2024.

occasionally be made. When these errors lead to litigation, it will be very difficult to identify what went wrong and which component of the quantum computers was at fault.

These challenges are unlikely to entirely defeat tort liability. Tort law has doctrines that permit factfinders to infer fault or negligence even when the precise details of what went wrong are not observable. But it will raise interesting questions about the reasonableness of the use of quantum computers in a particular context. Suppose, for example, that a quantum computer is orders of magnitude faster and more efficient at a particular process than a classical digital computer but has a slightly higher error rate. Is it reasonable for a company to employ quantum computing in that process?

Implications for Risk Management and Insurance

Quantum computing poses both risks and opportunities for the insurance industry. The risks associated with breaking encryption might be farther out on the horizon, but the opportunities for new insurance products and better risk calculation could materialize in the next few years.

Demand for New Insurance Products

Historically, the emergence of new technologies has provided opportunities for traditional insurance companies to modernize, reinvent themselves, and remain relevant in the marketplace. The rise of the personal automobile, for example, led to growing consumer demand for automobile insurance policies. As more individuals purchased personal automobiles, the number of automobile accidents rose. Consumers sought insurance to protect themselves from the financial consequences of automobile accidents. More recently, the advent of the internet and growing concerns about information security have led insurance companies to offer cyber liability policies.

The rise of quantum computing will also present insurers with an opportunity to develop new insurance products. As quantum computing is integrated into the economy, insurers will need to understand the particular risks posed by quantum computing and how the risk profiles differ from conventional computing. This will have important implications for insurance underwriting and the pricing of various lines of insurance. For example, if quantum computing solves optimization problems particularly well, risks of supply chain interruption or other risks that affect business interruption insurance products may decline. On the other hand, the ability of quantum computing to breach encryption standards may increase the costs of cyber insurance.

There may also be increased demand for insurance to cover potential losses associated with the breach of encryption. As quantum computing technology enables the breaking of popular encryption standards and makes it more difficult to comply with the privacy requirements that are enshrined in federal and state laws, it is likely that demand for insurance products designed to mitigate the financial impact of these risks will increase.

The error-prone nature of computations performed will also likely increase demand for novel insurance products. Entities that rely on quantum computers to perform critical tasks will seek to mitigate the consequences of such errors.

Improved Calculation of Risk

Quantum computing also represents an opportunity for the insurance industry as it relates to the calculation of risk. Quantum computers will be able to solve complex mathematical problems in a fundamentally different way. They will be able to search large sets of data for complex patterns that would be unimaginable today in terms of information volume and the breadth of factors being considered. Commentators have noted that quantum computing will "[open] astonishing vistas in everything from predicting the weather to developing new drugs."[4]

This characteristic of quantum computing has important—and beneficial—implications for the insurance industry. At the heart of insurance is the concept of risk. Insurance companies use a methodology called *risk assessment* to calculate premium rates for policyholders. Insurance underwriters often use proprietary software based on predetermined algorithms to gauge the risk that a particular policyholder will file a claim against their policy involving a particular amount sought and what the likely outcome of that claim might be. These algorithms are programmed using multiple categories of data to weigh risk. It is in the insurers' best interest to use as many relevant data points as possible to set premiums, because they must carefully balance profitability and risk—if a premium is too high, they risk losing customers, while if it too low, they risk being unable to offset losses.

Quantum computing will allow insurance companies to improve how they perform risk assessments. Because quantum computers may be able to process vast amounts of data nearly instantaneously, the algorithms used by insurance underwriters today will seem rudimentary, unsophisticated, and incomprehensive in comparison to the quantum algorithms that will be used by underwriters of the future. For example, a number of different quantum algorithms may facilitate the nearly instantaneous modeling of risk assessments, ranging from the potential impact of natural disasters to the life expectancies of everyone on the planet. This may permit near real-time adjustments in the ability to measure risk and in innovative products that could take advantage of these capabilities.

[4] Bill Briggs, Khalid Kark, Peter Vanderslice, Anthony Abbattista, George Collins, David Sisk, David Schmitz, Andy Dacher, Tom Galizia, Prashanth Ajjampur, et al., "Tech Trends 2015: The Fusion of Business and IT—An Insurance Industry Perspective," Deloitte, 2015.

CHAPTER 5

Challenges for Data Privacy

If universal quantum computers of sufficient size become a reality, it may become possible to load all the digitized knowledge in the world on a single quantum computer and process it in seconds or minutes. This possibility has significant implications for privacy. In the age of big data, privacy has heretofore been preserved because it is very difficult to collect and process all the relevant data about any given person. It is generally accepted that if you remove some personal identifiers from available data, it becomes difficult to re-identify a person from the anonymized data. While current big data capabilities have made complete anonymization of data more difficult to achieve, it is still possible if a sufficient effort is made. But the emergence of quantum computers that can access and process unimaginable volumes of data at once would pose significant challenges in terms of preserving the anonymity of personal data. In this chapter, we first discuss the major privacy implications stemming from the differences between digital and quantum computers. Then, we examine the most important privacy statutes in the United States and consider the potential impact of quantum computing on these statutes.

Evolution of Quantum Artificial Intelligence and Machine Learning

Before turning to the privacy implications of the quantum revolution, we will provide some background on the evolution of quantum-based AI systems. The future emergence of quantum-based AI systems poses the most significant challenge to existing privacy norms. Even before a full-scale universal quantum computer is built, early quantum computers will be used as part of AI systems. Even the quantum annealing computers of today can solve complex optimization problems, although a definitive advantage over classical computers has yet to be demonstrated. Given the large class of problems that can be conceived of in terms of optimization, many have envisioned early quantum computers as helping to make traditional digital AI engines smarter and faster. Already, we are seeing discussions of the quantum equivalents of artificial neural networks (ANNs), which are computer-based models that

learn to process data by mimicking the human brain.[1] However, as these emerging quantum systems become faster and more stable, we will start seeing hybrid quantum-digital AI systems that will capitalize on the maturity of the digital systems along with some of the new capabilities of emerging quantum systems. As quantum technologies mature, fully quantum AI systems may also become possible.

Quantum-based AI systems may also have significant privacy implications because of the unique characteristics that make them different from present-day digital AI systems. Today's ANNs are black boxes that learn from a training dataset and encode their decisionmaking processes in a set of values that control the behavior of their artificial neurons. This collection of values encodes information about the training dataset. The ANN is then used to make decisions about input data that was not explicitly included in the training dataset.[2] Even so, it is possible to explain what is happening at each step of the decisionmaking process.

In quantum-based AI systems, however, this explainability disappears for three reasons. First, the quantum states of the individual qubits that are participating in a computation cannot be directly observed. Once observed, the computation collapses and any observation would be rendered meaningless. Second, in a quantum computer, the entire problem is loaded into the qubits, and there are generally no intermediate computations. In other words, the quantum computer looks at all the data at once and executes the computation in one step.[3] Trying to explain what happened in that one step is very complicated. Third, explanations of the quantum mechanical principles that allowed the computation to happen would be very counterintuitive to most people. These characteristics of quantum-based AI systems challenge current privacy norms.

Implications for Data Privacy

There are four key ways in which quantum-based AI systems may affect data privacy:

1. *The de-identification of data.* As mentioned earlier, there are processes in place to remove personal identifiers from data so they can be used for government statistical purposes, medical research, marketing, and other purposes. If quantum computers

[1] Kerstin Beer, Dmytro Bondarenko, Terry Farrelly, Tobias J. Osborne, Robert Salzmann, Daniel Scheiermann, and Ramona Wolf, "Training Deep Quantum Neural Networks," *Nature Communications,* Vol. 11, No. 808, 2020.

[2] For example, a developer might use a set of pictures of male and female faces to train the ANN and then provide a new unclassified picture asking the ANN to judge whether this new picture is male or female. Information about all the faces used to train the ANN is implicitly stored in these values, but it is not possible to know how each picture is encoded in the set of values.

[3] This is not to say that there cannot be multiple steps of quantum computation—just that each quantum step in the digital world would have been broken up into millions or billions of individual, step-by-step computations.

can conduct searches in vast databases in seconds—and then correlate this scattered information back to its original identifiers—will these de-identification processes be sufficient?[4] And can these processes be used to identify such personal attributes as race or sexual orientation from publicly available data?[5]

2. *The right to be forgotten.* Existing privacy laws give individuals the right to control what data are stored about them. Under these laws, individuals can either correct this information or even have it removed. The development of the ANN has already made this difficult in practice. As mentioned earlier in this report, it already is very difficult to know what information is encoded in the ANN. If the ANN is connected to a quantum computer that feeds back and forth into the ANN, this becomes even more complicated, because the personal information resides both in the ANN and in quantum memory, making it even harder to attempt to locate information that is now residing in two separate black box systems. And it is vastly more difficult to locate and erase personal information in quantum memory because we will not be able to see what is happening inside the qubits, let alone understand what information resides where. Additionally, it is theorized that information stored in quantum states cannot be perfectly erased, as it can be in regular digital computing systems. Therefore, some personal information may continue to linger on in the system.[6]
3. *The fair use of information.* There are laws that require personal information to be used only for the specific purposes for which it was collected. Today, an ANN would be trained using vast datasets that include private data, which will then be part of that ANN forever. These AI engines tend to be used for many different purposes, and they tend to have a long lifespan. For example, a self-driving car algorithm can be trained by learning the behavior of thousands or millions of drivers. Originally, this algorithm may have been intended to be used in a particular model of car. However, it may eventually be adapted for use in an entirely different model or type of vehicle. This makes it more difficult to explain to consumers how their private data will be used in the future and ensure that their consent is an informed one. Because quantum computers will have the ability to easily handle enormous datasets that can be used

[4] PII are any data that can be used to identify a specific individual. Social Security numbers, mailing or email address, and phone numbers are most commonly considered PII, but as technology evolves, an internet protocol (IP) address, geolocation data, social media posts, or digital images could also be considered as PII.

[5] For example, there are algorithms today that can identify an individual's race through their name and address. See Marc N. Elliott, Kirsten Becker, Megan K. Beckett, Katrin Hambarsoomian, Philip Pantoja, and Benjamin Karney, "Using Indirect Estimates Based on Name and Census Tract to Improve the Efficiency of Sampling Matched Ethnic Couples from Marriage License Data," *Public Opinion Quarterly*, Vol. 77, No. 1, 2013.

[6] Arun K. Pati and Samuel L. Braunstein, "Impossibility of Deleting an Unknown Quantum State," *Nature,* Vol. 404, No. 6774, 2000, p. 164.

for many different purposes, the description of "future fair use" given to consumers will become even murkier.[7]

4. *The transparency of decisions made based on private data.* If private data are used to make a decision, such as the determination of a credit score, companies need to be able to explain how that score was calculated.[8] Quantum computers will make it very challenging to explain this process of calculating credit scores and other decisions, especially when social and personal biases are bound to be contained in the data and influencing decisions in nontransparent ways.

Implications for U.S. Privacy Laws

The rise of quantum computing would also have considerable implications for privacy laws in the United States.[9] In this section, we consider the implications of quantum computing for U.S. privacy laws, focusing on seven major privacy laws: (1) the Fair Credit Reporting Act (FCRA), (2) the Fair and Accurate Credit Transactions Act (FACTA), (3) the Gramm-Leach-Bliley Act (GLBA), (4) the Health Insurance Portability and Accountability Act (HIPAA), (5) the Children's Online Privacy Protection Act (COPPA), (6) the Privacy Act, and (7) the Freedom of Information Act (FOIA). Broadly speaking, quantum computing would affect these laws in three ways. First, quantum computing would affect how agencies and institutions comply with notice and disclosure requirements. Second, agencies and institutions would need to consider the risks associated with the re-identification of personal information. Third, the advent of quantum computing would require agencies and institutions to reevaluate and redesign their existing security procedures to comply with provisions mandating the adoption of appropriate and reasonable safeguards.

[7] In addition, the quantum algorithms in the intermediate hybrid systems designed to help the digital ANNs, for example, are a separate part of the ANN itself. But information is loaded to and from the ANN. If one ANN is disconnected and its information is used with a different ANN, does the information encoded in the qubits constitute private information that is not under the original fair use assumption?

[8] This is required by the Fair Credit Reporting Act (Peder Magee, "Privacy and Identity Protection from the Fair Credit Reporting Act to Big Data," *Antitrust*, Vol. 29, 2014).

[9] Under U.S. law, there is no general right of information privacy. There are, however, "some privacy protections for particular categories of information under existing statutes" (C. Christine Porter, "De-Identified Data and Third Party Data Mining: The Risk of Re-Identification of Personal Information," *Washington Journal of Law, Technology and Arts,* Vol. 5, No. 1, 2008).

FCRA and FACTA

Enacted in 1970, FCRA was the first federal law designed to protect the privacy of consumer credit information.[10] More than 30 years later, in 2003, FACTA was enacted as an amendment to FCRA. However, the Federal Trade Commission has questioned "whether privacy regimes [have] sufficiently kept pace [with technology] and [can] adequately protect consumers."[11]

Under FCRA, consumer reporting agencies must provide, on request, an explanation of "all of the key factors that adversely affected the credit score of the consumer."[12] The rise of quantum computing could make it more difficult for consumer reporting agencies to comply with this notice requirement. There are already concerns that digital AI will enable "devices [to] eventually outgrow their initial coding and use new sets of data to produce an outcome."[13]

Adding a quantum computing component to these devices will make this even more pronounced. Because quantum computers are essentially black boxes, the ways in which key factors were used to calculate an individual's credit score will not be immediately understandable to consumer reporting agencies. With current AI technology, a "calculation that led to said outcome [will be] unknown" to the consumer reporting agency.[14] Even without the transformative power of quantum computing, an AI device today will be able to act "on data that [its programmers] are unaware of, or, unbeknownst to them, it has created its own algorithms. . . ."[15] The use of key factors in the calculation of an individual's credit score, therefore, will even be "unknown to [its] programmers."[16] This is true with current AI systems and will only become more opaque with the addition of quantum devices. To maintain their compliance with FCRA, consumer reporting agencies should continue to rely on more easily traceable computing algorithms. This will permit the agencies to explain the role of key factors in the calculation of credit scores to consumers.

Privacy Act

Enacted in 1974, the Privacy Act establishes a code governing the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of

[10] Magee, 2014.

[11] Magee, 2014, p. 59.

[12] U.S. Code, Title 15, Chapter 41, Subchapter III, Section 1681, Disclosures to Consumers. FACTA clarifies these requirements to provide further protections against identity theft, but the issues posed by quantum computing are similar for both statutes.

[13] Iria Giuffrida, Frederick Lederer, and Nicolas Vermerys, "A Legal Perspective on the Trials and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law," *Case Western Reserve Law Review,* Vol. 68, No. 3, 2018, p. 778.

[14] Giuffrida, Lederer, and Vermerys, 2018, p. 778.

[15] Giuffrida, Lederer, and Vermerys, 2018, p. 779.

[16] Giuffrida, Lederer, and Vermerys, 2018, p. 779.

records by federal agencies.[17] Under the Privacy Act, government agencies must allow an individual, on request, to "gain access to his record or to any information pertaining to him."[18] An individual must be given the opportunity to "review the record and have a copy made of all or any portion thereof in a form comprehensible to him."[19] Additionally, the Privacy Act requires agencies to provide individuals with clear information about the authority to collect their data, the intended uses of that data, and any routine uses that the information may be used for.[20]

The rise of quantum computing would affect compliance with these provisions. What obligations does a federal agency have, for example, if an individual's personal information is used to train a quantum AI? The nature of quantum computing means that it will be virtually impossible for the agency to explain to the individual precisely how their personal information was used. If data are stored in quantum memory, it is impossible to make and provide a copy to the individual, let alone provide it in a comprehensible form. Existing standards for compliance with these provisions would need to be modified to account for the characteristics and capabilities of quantum computers. These modifications may take several forms. One option is to simply require federal agencies to reveal to the individual the fact that their personal information was used to train a quantum AI. A second option is to require federal agencies to inform the individual, in more detail, of the intended uses, potential future uses, and security risks associated with the quantum AI.

The Privacy Act also requires federal agencies to take measures to safeguard records. Each agency must

> establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness. . . .[21]

The rise of quantum computing would require federal agencies to reevaluate their procedures for safeguarding records. It will be necessary for these procedures to change, moreover, as quantum computing technology becomes more widespread. As discussed previously, post-quantum cryptography will influence emerging minimum standards for safeguarding records.

---

[17] U.S. Department of Justice, *Overview of the Privacy Act of 1974 (2020 Edition)*, 2020.

[18] U.S. Code, Title 5, Section 552a, Records Maintained on Individuals, paragraph (B)(d)(1).

[19] U.S. Code, Title 5, Section 552a(d)(1).

[20] U.S. Code, Title 5, Section 552a(e)(3).

[21] U.S. Code, Title 5, Section 552a(e)(10).

GLBA

Enacted in 1999, the GLBA requires financial institutions (i.e., companies that offer consumers financial products or such services as loans, financial or investment advice, or insurance) to explain their information-sharing practices to their customers and safeguard nonpublic personal information.[22] The GLBA consists of two parts: the Privacy Rule and the Safeguards Rule. The Privacy Rule of the GLBA prohibits financial institutions from disclosing nonpublic personal information to a nonaffiliated third party without notifying the consumer.[23] Prior to any disclosure, moreover, the consumer must be given the opportunity to "direct that such information not be disclosed to such [a] third party."[24]

Quantum computing raises the following concerns: As discussed previously, it would be impossible to know what personal data are stored in the system and how exactly they are being used. Under the GLBA, is the financial institution required to notify any consumer whose personal information may be used before training a quantum AI? If so, what information should that notice include? This problem could be solved if the GLBA were amended to include a requirement that financial institutions notify consumers of the fact that their personal information may be used to train a quantum AI. This amendment could additionally require that financial institutions allow consumers to opt out of that specific use case.

Unlike the Privacy Rule, the Safeguards Rule requires financial institutions to take affirmative steps to safeguard nonpublic personal information. In particular, they must "insure the security and confidentiality of customer records and information," "protect against any anticipated threats or hazards to the security and integrity of such records," and "protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[25]

The rise of quantum computing would present several challenges in terms of compliance with these provisions. First, it would be necessary for financial institutions to reassess the *appropriateness* of their current standards for safeguarding consumers' nonpublic personal information. As quantum computing becomes more widespread in the coming decades, these standards will need to be reevaluated and modified. Second, as quantum computing evolves and becomes more mainstream, what is currently a *potential* security threat may need to be upgraded to a reasonably *anticipated* security threat. To make these determinations, technologists, lawyers, and policymakers will need to work collaboratively to assess the sufficiency of existing safeguards and precisely characterize the threat to nonpublic personal information posed by quantum computing.

---

[22] The GLBA defines *nonpublic personal information* as information that is not publicly available and is provided by a consumer to a financial institution. This includes such personal details as names, addresses, Social Security numbers, account numbers, and financial history (Public Law 106-102, Gramm-Leach-Bliley Act, November 12, 1999).

[23] Pub. L. 106-102, 1999.

[24] Pub. L. 106-102, 1999.

[25] Pub. L. 106-102, Title V, Subtitle A, Disclosure of Nonpublic Personal Information, 1999.

HIPAA

Enacted in 1996, HIPAA mandates that *covered entities* take measures to safeguard health information. In particular, covered entities must "ensure the confidentiality, integrity, and availability of all electronic protected health information."[26] They must also "protect against any reasonably anticipated threats or hazards to the security or integrity of such information."[27] Finally, covered entities must "protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required."[28] Covered entities are given some latitude in choosing security measures, as long as these measures "allow [them] to reasonably and appropriately implement the standards and implementation specifications."[29] When choosing security measures, however, they must take into account several factors, including their existing security capabilities and infrastructure, the cost of implementing additional security measures, and the risk posed by unauthorized or inadvertent disclosure of protected health information.[30]

The rise of quantum computing would necessitate that covered entities reevaluate their existing security measures. HIPAA requires covered entities to safeguard protected health information from threats that are "reasonably anticipated."[31] Information security standards are a moving target. The development and proliferation of quantum computing technology would change the risk calculus. At present, covered entities have no reasonable basis for anticipating that protected health information might be threatened by a quantum device. With the evolution of more powerful—and more readily available—quantum computing capabilities, it may become reasonable for covered entities to anticipate the penetration of their existing security measures by quantum computers. Covered entities would need to invest in cryptographic systems that are secure against both classical and quantum computers. Quantum computing "may one day make 95% or more of our encryption and data security obsolete."[32] In the future, therefore, it will become "reasonable" for covered entities to invest in post-quantum cryptographic systems.[33]

---

[26] HIPAA defines *covered entities* as health plans, health care clearinghouses, and health care providers who electronically transmit any health information (Code of Federal Regulations, Title 45, Subtitle A, Subchapter C, Part 160, Subpart A, Section 160.103, Definitions; Code of Federal Regulations, Title 45, Subtitle A, Subchapter C, Part 164, Subpart C, Section 164.306, Security Standards: General Rules, paragraph [a][1]).

[27] Code of Federal Regulations, Title 45, Subtitle A, Subchapter C, Part 164, Subpart C, Section 164.514, Other Requirements Relating to Uses and Disclosures of Protected Health Information.

[28] Code of Federal Regulations, Title 45, Part 164.306 (a)(3).

[29] Code of Federal Regulations, Title 45, Part 164.306 (b)(1).

[30] Code of Federal Regulations, Title 45, Part 164.306 (b)(2).

[31] Code of Federal Regulations, Title 45, Part 164.306 (a)(2).

[32] Stephen L. Tupper, "The View from the GC's Desk: Security and Privacy Issues That Keep General Council Up at Night," *Michigan State Journal of International Law,* Vol. 16, No. 1, 2007, p. 229.

[33] Researchers have made progress toward the development of quantum-safe cryptosystems. See Karen Martin, "Waiting for Quantum Computing: Why Encryption Has Nothing to Worry About," *TechBeacon,*

An additional issue is the potential re-identification of protected health information. Under HIPAA, health information is protected if it is individually identifiable. However, if there is "no reasonable basis to believe that the information can be used to identify an individual," it is not considered to be individually identifiable.[34] Quantum computing technology would make it easier to re-identify protected health information.[35] The rise of quantum computing "heralds an age when effectively infinite computing power will be available for cracking the world's largest codes."[36] At least one federal court has thus far declined to recognize the security risks associated with re-identified data.[37] However, as quantum computing technology evolves and becomes a more-recognized security threat, the federal judiciary will likely need to reconsider the potential threat of re-identified data. As noted earlier, it is likely that covered entities will need to invest in post-quantum cryptographic systems to maintain their compliance with the requirements enshrined in HIPAA.

COPPA

Enacted in 1998, COPPA sought to give parents control over what information is collected from their children online. COPPA imposes several requirements on operators of commercial websites and online services—including mobile applications—aimed at children. Operators must post a clear privacy policy; obtain parental consent before collecting a child's personal information online; give parents the opportunity to prevent the further use or collection of a child's personal information; maintain the confidentiality, security, and integrity of any information collected; and retain personal information for only as long as is necessary.[38]

Under COPPA, operators must implement "reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[39] With the rise of quantum computing, operators would need to reevaluate their security procedures to make sure they remain "reasonable" in light of technological advances in the field. In particular, to remain in compliance with COPPA, operators should adopt security procedures designed to prevent the re-identification of children's personal information.

August 15, 2018.

[34] Code of Federal Regulations, Title 45, Section 164.514.

[35] Porter, 2008.

[36] Daniel J. Sherwinter, "Surveillance's Slippery Slope: Using Encryption to Recapture Privacy Rights," *Journal on Telecommunications and High Technology Law,* Vol. 5, No. 2, Winter 2007, p. 507.

[37] *IMS Health Inc. v. Ayotte*, 490 F. Supp. 2d 163., New Hampshire, April 30, 2007.

[38] Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions," webpage, July 2020, last updated January 2024.

[39] Code of Federal Regulations, Title 16, Chapter I, Subchapter C, Part 312.3, Regulation of Unfair or Deceptive Acts or Practices in Connection with the Collection, Use, and/or Disclosure of Personal Information from and About Children on the Internet; Code of Federal Regulations, Title 16, Chapter I, Subchapter C, Part 312.8, Confidentiality, Security, and Integrity of Personal Information Collected from Children.

FOIA

Enacted in 1967, FOIA stipulates that "any person" has the right to request access to the records of federal agencies.[40] The rise of quantum computing raises the following questions: First, would a quantum AI be permitted to make a FOIA request? At first glance, it does not seem likely that a quantum AI would be eligible to request a set of records, according to the language of FOIA. The Restatement (Third) of Agency Law provides that a computer program is "not capable of acting as a principal or an agent as defined by the common law."[41] Under FOIA, a quantum AI could request records only if it were treated as a legal person. While at least one legal scholar has argued that this could be possible, it seems unlikely that a quantum AI's FOIA request would be granted.[42] By taking up the question of AI personhood, however, the judicial system will play an important role in facilitating our transition to a world in which quantum computing is pervasive. Second, if the government stores information on a quantum computer, and given that it is impossible to create a copy of quantum memory, what are the FOIA implications? And how much effort is the government required to make to create some representation of the stored information?

---

[40] Public Law 89-487, The Freedom of Information Act, July 5, 1967. This right exists except to the extent that the records are protected from disclosure under any of nine exemptions.

[41] According to Sections 1.01–8.14 of American Law Institute, *Restatement of the Law Third, Agency*, Vol. 1–2, American Law Institute Publishers, 2006,

> [A] computer program is not capable of acting as a principle or an agent as defined by the common law. At present, computer programs are instrumentalities of the persons who use them. If a program malfunctions, even in ways unanticipated by the persons who use them. If a program malfunctions, even in ways unanticipated by its designer or user, the legal consequences for the person who uses it are no different than the consequences stemming from the malfunction of any other type of instrumentality. That a program may malfunction does not create capacity to act as a principal or an agent.

[42] Shawn Bayern, "The Implications of Modern Business-Entity Law for the Regulation of Autonomous Systems," *European Journal of Risk Regulation,* Vol. 7, No. 2, 2016. Bayern envisions a world in which autonomous systems, including AI, have the rights of legal persons.

CHAPTER 6

Challenges in the Global Regulatory Environment

Quantum computing is not just an issue for the civil justice system in the United States. There have been recent discussions on regulating current and emerging computing capabilities in both Europe and China. Those regulatory changes will have consequences for U.S. companies that do business abroad, as well as for legal practitioners who advise U.S. businesses. In this chapter, we first consider the regulatory treatment of quantum computing by the EU, including the implications of the General Data Protection Regulation (GDPR) for quantum computing. Then, we examine the regulatory treatment of quantum computing in China. Finally, we discuss how existing and potential export control regulations may affect quantum computing in the United States.

The European Union

Quantum computing and associated technologies feature prominently in the EU's agenda. While the European Commission has acknowledged the presence of a strong fundamental and applied research community in Europe, the commission is concerned by low levels of industry commitment and an uptick of emerging technologies, especially compared with China and the United States. In particular, there is concern that Europe may fall behind the international competition in a field perceived to encompass one of the key future technologies and that Europe may become dependent on foreign (i.e., non-EU) suppliers for critical components or materials required for quantum computing. Therefore, the EU and its member states have engaged in a variety of national and regional initiatives to increase activity in the academic and research communities (i.e., technology push), increase demand, and ensure that research and development and related products meet European requirements, protect relevant intellectual property, and establish the required quantum infrastructure to turn Europe into a leading quantum technology development ecosystem.[1]

[1] These initiatives were part of the European Quantum Communication Infrastructure (EuroQCI) initiative of 2019 (European Commission, "The European Quantum Communication Infrastructure (EuroQCI) Initiative," webpage, last updated October 22, 2024). See also Quantum Flagship, *Quantum Technologies: Public Policies in Europe*, QuantERA, October 17, 2023b.

In 2018, the EU launched its Quantum Technologies Flagship that aims to expand Europe's scientific leadership and support the development of commercial applications that will provide solutions to real-world challenges.[2] In 2020, the Quantum Flagship Strategic Advisory Board prepared a Strategic Research Agenda that outlines five major strategies the EU should adopt to meet its goal of becoming a leader in the development of quantum technologies:

- Engage all stakeholders across the scientific research, industrial, and governmental sectors to ensure technologies can move swiftly from research to industrial exploitation.
- Build financial capital for sustaining investments in quantum industry.
- Provide the necessary infrastructure that will allow for the successful exploitation of new technologies.
- Create a strategy for intellectual property and the standardization of quantum technologies across all EU states.
- Educate and train a "quantum-aware workforce and society."[3]

In addition, the EU strongly espouses the socioeconomic benefits that investment in quantum computing and related technologies can bring.[4] As part of the EU's wider research and innovation work under the Horizon Europe program, existing quantum technology programs are envisioned as helping Europe produce world-class science, remove barriers to innovation, create jobs, strengthen Europe's global competitiveness, and ensure long-term sustainable and inclusive economic growth.[5]

Technology Investment and Justice System Reform

Since the coronavirus disease 2019 pandemic, the EU has placed significant emphasis on assisting its member states in modernizing their civil justice systems, including investments in digitalization and information and communications technologies (ICT).[6] A large number of member states have ongoing justice-related investment programs. As of 2022, more than 33 of the 46 Council of Europe member states had either adopted or were in the process of negotiating legislative and regulatory activities concerning ICT development in their justice

[2] European Commission, "Quantum Technologies Flagship Kicks Off with First 20 Projects," press release, October 28, 2018.

[3] Quantum Flagship, *Strategic Research Agenda*, European Quantum Flagship, March 2020.

[4] Quantum Flagship, *Strategic Research and Industry Agenda 2030: Roadmap and Quantum Ambitions over This Decade*, 2023a.

[5] European Commission, "Horizon Europe," webpage, undated.

[6] European Commission, "Digitalisation of Justice in the European Union: A Toolbox of Opportunities," memorandum to the European Parliament, the European Council, the European Economic and Social Committee, and the Committee of Regions, December 2020.

systems.[7] Digitization and ICT investment programs have also been the largest recipients of EU structural funds in support of national justice systems.[8]

However, it does not appear that the advent of quantum computing has been actively considered in these investments or that the implications of quantum computing are discussed in the context of the civil justice system in Europe. This is especially important given that investment in and reforms of justice systems typically take several years from inception to adopt. Thus, a failure to address potential security vulnerabilities or the new risks posed by quantum computing technologies early on may jeopardize the long-term security of European national justice systems. However, the fact that the EU does currently have significant programs and expenditures regarding ICT programs for its justice system indicates that the EU will most likely be ready to spend significant amounts of resources to mitigate some of the risks of quantum computing, and most likely before the United States. Therefore, U.S. stakeholders should monitor regulatory and court technology developments in Europe.

General Data Protection Regulation

Enacted in 2018, the GDPR superseded the EU's 1995 Data Protection Directive 95/46/EC.[9] The GDPR represents the most significant EU legislation created thus far to regulate the processing of personal data. The aim of the GDPR is to protect all EU citizens from privacy and data breaches, regardless of where their data reside. The key elements of the GDPR are the following:

- *Increased territorial scope.* The new extraterritorial applicability of the GDPR means that it applies to all companies processing the personal data of subjects residing in the EU, regardless of the company's location (i.e., even if the company is outside the EU).
- *Increased penalties.* In the case of breaches of the GDPR, organizations can be fined up to 4 percent of annual global turnover or 20 million euros (whichever is greater).
- *Mandated consent.* The GDPR mandates that the organizations' required request for consent must be given in an intelligible and easily accessible form.
- New data subject (the individuals whose information may be processed) rights:
  - *Breach notification right.* Breach notifications are now required when a data breach is likely to "result in a risk for the rights and freedoms of individuals," and notifications must be made within the first 72 hours of being made aware of the breach.

---

[7] European Commission for the Efficiency of Justice, *Evaluation Report on European Judicial Systems, Part 1*, Council of Europe, 2020.

[8] Quantum Flagship, 2020.

[9] EU, "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)," *Official Journal of the European Union,* Regulation EU 2016/679, April 27, 2016; European Parliament, Council of the European Union, "On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," Directive 95/46/EC, October 24, 1995.

- *Right to access.* The GDPR includes the right of data subjects to receive information of what personal data are being processed or stored, where, and for what purpose, as well as to be able to receive a copy of those data.
- *Right to be forgotten*. The GDPR also includes the right of data subjects to request that data controllers (the entities that store a person's data) erase their personal data, stop further distributing those data, and possibly have third parties stop processing the data.[10]

Lastly, the GDPR further mandates privacy by design as a legal requirement. *Privacy by design* refers to the process of considering data protection from the outset when creating products and services rather than as an afterthought. In practice, this should mean that the "controller shall . . . implement appropriate technical and organizational measures . . . in an effective way . . . in order to meet the requirements of this [r]egulation and protect the rights of data subjects."[11]

The GDPR has already had wide-ranging implications for data protection, both in the EU and beyond. However, the advent of quantum computing could have further implications for organizations' data protection practices. In addition to the enhanced data subject rights outlined here, the GDPR also requires data controllers to maintain an adequate standard of cybersecurity measures to protect personal data. In the future, the adoption of quantum computing and cryptography may alter what regulators perceive as "adequate" measures of protection, particularly if there are significant quantum implications in relation to current encryption standards. The advent of quantum computing may further change how organizations process, store, and transfer personal data, all of which may have implications for how the GDPR affects data controllers and data subjects.

The significant differences between quantum information and classical information could change how data are perceived and controlled, including how such regulations as the GDPR can practically be implemented. In contrast to digital information, there will be challenges about how quantum information can be moved, copied, stored, and deleted. A practical obstacle to implementing the GDPR in the coming quantum computing era may be, for example, the increased data subject rights brought about by the right to be forgotten. As mentioned earlier, it may not be possible to perfectly delete quantum information.[12] It may also be difficult to copy quantum information in the same way as digital information, which may complicate compliance with the right-to-access principles embodied in the GDPR. If quantum information is transferred through classical optical infrastructure, it will be transferred through *quantum teleportation*, meaning that the quantum information will no longer be available at the source of the communication (i.e., personal data will transfer from the data

[10] EU, 2016, Article 25.

[11] EU, 2016.

[12] Pati and Braunstein, 2000, p. 164.

controller to the data subject without allowing the controller to keep a copy of it).[13] Whereas the current version of the GDPR is fairly technology-neutral, data controllers and regulators alike may face challenges in interpreting and implementing many of its principles and requirements in a quantum future.

China

China is leading global efforts to advance the field of quantum computing. Not only has the State Council of China acknowledged the limits of the current digital revolution, but it also believes that the quantum revolution will have significant social and economic impacts. It recognizes the inevitability of future advances in the field of quantum computing and the potential impacts on economic and social development resulting from these advances. The 14th Five-Year Plan for Economic and Social Development lists the development of quantum information technology as a "priority action" aimed at propelling China to the "frontlines of global science and technology."[14]

Chinese research priorities seem to follow the full spectrum of quantum information sciences and technologies. These include various types of quantum computing systems, quantum communications and information security, quantum simulations, and many of the underlying technologies that promise to become quantum computing enablers.[15]

While there does not seem to be any current efforts to establish new laws related to quantum computing in China, there have been signs of efforts to develop new laws and regulations on AI.[16] The New Generation AI Development Plan (which was developed to build China's first-mover advantage in the development of AI) states: "By 2025 China will have seen the initial establishment of AI laws and regulations, ethical norms and policy systems, and the formation of AI security assessment and control capabilities."[17] By 2030, moreover, "China will have established a number of world-leading AI technology innovation and personnel training centers (or bases), and will have constructed more comprehensive AI laws and regulations,

[13] The EU has provided hints at a solution for this by establishing that trusted repeaters decode and reencode the quantum information to "provide access for lawful intercept, as required by many nation states" (Aymard de Touzalin, Charles Marcus, Freeke Heijman, Ignacio Cirac, Richard Murray, and Tommaso Calarco, "Quantum Manifesto: A New Era of Technology," Quantum Europe Conference, May 17–18, 2016, p. 10).

[14] Johanna Costigan and Graham Webster, eds., "14th Five-Year Plan for National Informatization," DigiChina, 2022.

[15] State Council of the People's Republic of China, "The National Medium- and Long-Term Program for Science and Technology Development (2006–2020): An Outline," 2006.

[16] Theodore J. Karch, Ashwin Kaja, and Yan Luo, "China's Vision for the Next Generation of Artificial Intelligence," *National Law Review*, Vol. 8, No. 84, March 25, 2018.

[17] Graham Webster, Rogier Creemers, Elsa Kania, and Paul Triolo, "Full Translation: China's 'New Generation Artificial Intelligence Development Plan,' (2017)," DigiChina, August 1, 2017.

and an ethical norms and policy system."[18] It is reasonable to expect that if China intends to be a world leader in establishing laws and policies relating to AI, China will also eventually establish new laws and policies relating to quantum computing and quantum AI.

U.S. Export Controls on Quantum Technologies

In recent years, the United States has taken several steps to restrict the export of emerging technologies generally and quantum computing technologies specifically. In 2018, President Donald Trump signed the Export Control Reform Act of 2018 (ECRA).[19] ECRA is the new statutory authority for the existing Export Administration Regulations (EAR).[20] Under ECRA, the U.S. Department of Commerce's Bureau of Industry and Security is charged with leading an interagency process for establishing export controls for "emerging and foundational technologies."[21]

As a general matter, one of the policy objectives of export controls is to maintain the technological leadership of the United States in the world. As applied to emerging technologies, however, export controls may either advance or undermine this goal. The introduction of export controls on quantum computing technologies would have implications for scientific collaboration, manufacturing, and mergers, acquisitions, and investments. U.S. technology leadership in quantum computing relies heavily on foreign expertise because of the global nature of research and development in this field and a global shortage of quantum computing experts. Furthermore, the development of U.S. quantum information science and technology experts is currently insufficient, necessitating reliance on foreign talent who may face visa challenges.

On September 6, 2024, the Bureau of Industry and Security, recognizing that strict export controls would be "devastating to the continued progress of future developments in the quantum field" introduced a general license.[22] The license would require bureau approval for for-

[18] Webster et al., 2017.

[19] On August 13, 2018, President Trump signed the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 (Public Law 115-232, 2018). The NDAA includes ECRA (Pub. L. 115-232, 2018).

[20] Kevin J. Wolf, Thomas J. McCarthy, Andrew R. Schlossberg, "The Export Control Reforms Act and Possible New Controls on Emerging and Foundational Technologies," *Akin*, September 12, 2018. EAR controls the export, reexport, and transfer of sensitive technologies.

[21] U.S. Code, Title 50, Chapter 58, Subchapter I, Section 4817, Requirements to Identify and Control the Export of Emerging and Foundational Technologies.

[22] Bureau of Industry and Security, "Commerce Control List: Additions and Revisions; Implementation of Controls on Advanced Technologies," *Federal Register*, Vol. 89, No. 173, September 6, 2024, p. 72929.

eign persons, with annual reporting requirements to ensure compliance with U.S. national security and foreign policy interests.[23]

While export controls are essential for safeguarding national security, they present significant challenges to the development of quantum computing capabilities. Balancing security concerns with the need for innovation and collaboration will be crucial for maintaining progress. Corporations, policymakers, and researchers will need to work together to navigate these challenges and ensure that the United States can continue to develop advanced quantum computing technologies.

[23] Specifically, the license requirements apply only to foreign persons whose most recent country of citizenship or permanent residency is a destination specified in EAR Country Groups D:1 or D:5. These include such countries as China, Iran, Iraq, Russia, and others that are subject to national security concerns or are under U.S. arms embargos (Bureau of Industry and Security, 2024).

CHAPTER 7

Recommendations

In this report, we considered the new capabilities of quantum computers, how quantum computing differs from traditional digital computing, and how quantum computing may present challenges and opportunities in the context of the civil justice system. We examined how law firms, courts, and liability insurers will need to adapt current practices to these new realities, and we examined the impact of quantum computing on existing regulations. This chapter provides a series of recommendations to address the implications of quantum computing for the civil justice system: the future of encryption, liability, insurance, and privacy in a quantum world.

Securing Sensitive Client Data

The increasing digitization of both information and court proceedings means that law firms, courts, and insurers will have to interface with, process, analyze, and use increasing amounts of information while also keeping it safe. This will require these entities to achieve a potentially higher level of sophistication on cyber threats and digital security than they may currently have and stay informed about the evolving capabilities and risks associated with the proliferation of data and digital systems. If employing in-house technical experts is not financially feasible, law firms, courts, and insurers should consider outsourcing some of the more complex technical aspects of cyber and data risk analysis and security.

Several general security principles can assist insurers, law firms, and courts in safeguarding sensitive client information both now and in the future when quantum computers may have the capability to break current forms of widely used encryption:

- Conduct regular risk assessments to identify sensitive data and determine how long such data may need to be secured.
- Consider keeping highly sensitive or valuable data, such as trade secrets, settlement data, or nonpublic court data, offline to prevent potential unauthorized access.
- Maintain awareness of new encryption standards and identified cyber threats from such authorities as the Cybersecurity and Infrastructure Agency or NIST.
- Develop clear policies and procedures for data breach response, reporting, and notification.

The civil justice system as a whole should invest in acquiring and adopting quantum-secure encryption solutions. While courts, law firms, and insurers may not be among the first adopters of such solutions, they should be ready to transition to quantum-secure systems and have a plan for minimizing the disruption associated with such a transition.

Navigating Liability and Risk Management

The advent of quantum computing will likely introduce new challenges for the civil justice system in how to navigate new or evolving types of liability. As we have discussed, quantum computers are currently incredibly prone to errors and are, by their very nature, difficult, if not impossible, to observe and understand how they arrive at their final computations. These unique characteristics will challenge the traditional legal framework and require the creation of new legal doctrines or the adaptation of existing statutes to ensure that the tort liability system continues to function as it should.

In this report, we identified the following three avenues of potential litigation that law firms, courts, and insurers should begin to think about in the context of the coming quantum age:

- litigation arising from quantum computing–facilitated data breaches
- litigation arising from whether a potential quantum computing–facilitated loss is covered by an existing insurance policy
- litigation arising from product defects caused by manufacturers, programmers, or others involved in the development of a particular quantum computer or process.

Insurers will also need to develop new methods for assessing the risks posed by quantum computers. The insurance industry should be proactive and work closely with the scientific and technical community to understand these risks and quantify their impact. This will enable the insurance industry to create new insurance products for the quantum age.

Insurers should also explore the opportunities that quantum computing offers to improve their overall risk assessment models. Quantum computers will be able to process much larger datasets than traditional computers and have the potential to allow insurers to develop more accurate pricing based on near-real-time adjustments. State insurance regulators will also need to develop sufficient understanding of these risks to design appropriate policy.

Enhancing Privacy Protections

Big data analytics, AI, and ML have already changed how people think about data privacy and the protection of sensitive data. With the advent of quantum computing, understanding of privacy will continue to evolve. The risk of de-anonymizing data will become an integral part of the risk calculus. The civil justice system should prepare to integrate these emerging conceptions of privacy into existing laws and regulations. For example, HIPAA requires that a qualified statistician certify that data have been anonymized. In a quantum future, who will

have the qualifications and expertise to certify the anonymization of data? Will such a certification even be possible? This is just one example of the kind of definitional issue that the civil justice system will have to contend with. The ethical standards for protecting client data will also need to be reworked to reflect the advent of quantum computing. For example, guidelines could require that organizations obtain explicit consent for any activities that require the processing of previously collected and stored client information.

Consider Harmonizing Global Regulation

The development of quantum computers has become a three-way race between the EU, China, and the United States. The fact that this has seemingly become an issue of national pride highlights the pressure national governments feel and the resources that they invest in making quantum computing a reality. The EU, in particular, seems to be preparing policies and regulations to protect and secure future quantum computing, while China intends to show leadership both technologically and in regulating these new capabilities. These actions show the expectations of major players in the technology development and regulation of future developments and their confidence that quantum computing will become a reality in the not-too-distant future. Civil justice stakeholders should make an effort to track further developments in the EU and China and consider whether the U.S. civil justice system should implement similar initiatives.

APPENDIX A

Context for Quantum Computing: History and Timeline

To understand the impact of quantum computing, we need to first understand its history and potential future. Here we briefly discuss the history of quantum computing and its projected timeline. It should be noted that quantum computing is a rapidly expanding area of research and development. As new quantum algorithms are discovered, the variety of tasks that quantum computers can perform will also expand, and the impact on the legal and regulatory systems will change.

A Brief History of Quantum Computing

In 1935, Albert Einstein, Nathan Rosen, and Boris Podolsky published a paper in which they described what is now known as the Einstein-Podolsky-Rosen paradox.[1] The paper described what Einstein later referred to as "spooky action at a distance"—a prediction that two particles could be "entangled" and placed at large distances apart and that the state of the two particles would be intertwined, such that any attempt to measure one would be transmitted instantaneously to the other at arbitrarily large distances.[2] This phenomenon seemed to defy logic, leading researchers to conclude that quantum mechanics must be somehow incomplete.

However, theorists continued to debate the topic, and over time some experimental evidence surfaced that seemed to substantiate the existence of the phenomenon. In the 1980s, researchers began openly discussing the possibility of a quantum computer or a computer that could use quantum phenomena to perform calculations. In 1994, the U.S. mathematician Peter Shor proposed the first practical algorithm demonstrating that a quantum com-

[1] Albert Einstein, Boris Podolsky, and Nick Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" *Physical Review*, Vol. 47, 1935.

[2] See Albert Einstein, *The Born-Einstein Letters: Correspondence Between Albert Einstein and Max and Hedwig Born from 1916–1955, with Commentaries by Max Born*, Macmillan, 1971, p. 158. A *particle* is defined as "any of the basic units of matter and energy (such as a molecule, atom, proton, electron, or photon)" (Merriam-Webster, "Particle," dictionary entry, webpage, undated).

puter, built with entangled particles, could be used to break current encryption systems.[3] By 1998, the first two- and three-entangled particle computers were used to prove that some of the simplest quantum algorithms could actually work.[4] Each particle was referred to as a *qubit*—the quantum analogue of a bit.

Since then, the race to develop a large-scale quantum computer has accelerated. Recent progress in the field suggests that quantum computers may become a reality in the near future. D-Wave, a company in British Columbia, has been at the forefront of this trend. In 2007, the announcement of the first D-Wave 16-qubit quantum annealing–based processor transformed what had previously been only a theory—based on limited experimental work in a few academic labs—into a potentially viable and commercially available capability. Four years later, D-Wave released a 128-qubit chipset. The company subsequently released a 512-qubit quantum computer that was sold to NASA, Lockheed Martin, and Google. In 2017, D-Wave released a 2048-qubit computer; several governmental, industrial, and academic buyers lined up to purchase this computer.[5] Currently, D-Wave's 5000-qubit Advantage computer is being used by numerous businesses to optimize everything from scheduling to asset planning and allocation.[6]

Today, many companies are pursuing their own quantum chip designs, including IBM, Google, Intel, and Microsoft. In 2019, Google announced that it had used its quantum programmable device to achieve *quantum supremacy*—the solution of a mathematical problem that no classical computer can solve.[7] Google's claim of solving a specific mathematical problem in 200 seconds on its quantum device—a feat that would take 10,000 years on the world's fastest supercomputer—was promptly disputed by IBM.[8] IBM argued that an improved digital algorithm could in theory solve the same problem in two-and-a-half days, and ultimately

---

[3] Peter W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, November 20–22, 1994.

[4] Isaac L. Chuang, Neil Gershenfield, and Mark Kubinec, "Experimental Implementation of Fast Quantum Searching," *Physical Review Letters,* Vol. 80, No. 15, April 13, 1998.

[5] One must caveat that this is a quantum *annealing* computer and not a general-purpose quantum computing device (see Appendix B for more information on annealing). It has been criticized for not offering concrete advantages over classical computers other than in very unique circumstances. Nevertheless, D-Wave has initiated a race to commercialize quantum computing. See Universities Space Research Association, "First Quantum Annealing Computer in the U.S. to Have More Than 2000 Qubits Installed and Operational," press release, August 31, 2017; and Luke Graham, "Quantum Computer Worth $15 Million Sold to Tackle Cybersecurity," CNBC, January 27, 2017.

[6] D-Wave, "Quantum Optimization Data Sheet," 2023.

[7] Frank Arute, K. Arya, R. Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Bell, et al., "Quantum Supremacy Using a Programmable Superconducting Processor," *Nature,* Vol. 574, 2019.

[8] Edwin Pednault, John Gunnels, Giacomo Nannicini, Lior Horesh, and Robert Wisnieff, "Leveraging Secondary Storage to Simulate Deep 54-Qubit Sycamore Circuits," arXiv, arXiv:1910.09534, 2019.

they were proven correct.[9] In March 2024, researchers using a D-Wave quantum annealing–based processor claimed to have demonstrated quantum supremacy by simulating nonequilibrium magnetic spin dynamics, which they estimated would have a "hypothetical runtime on the Frontier supercomputer surpassing millions of years with infeasible memory and energy requirements."[10]

Expectations and Timelines for Quantum Computing

Through the National Quantum Initiative Act, the U.S. government has shown that it believes quantum information science—and quantum computing in particular—will be crucial to maintaining U.S. technological superiority in the future.[11]

The natural question to arise is: When exactly will this future become a reality? Predicting when quantum computers will deliver these new capabilities is difficult at best. The key problem in scaling quantum computers to sizes that will allow for breakthrough capabilities is the creation of error-free qubits. As one keeps adding more and more qubits, they become more unstable and prone to errors. One can compensate by combining multiple qubits together to create stable, logical qubits. One needs many physical qubits to create one logical qubit. Scientists are expected to achieve useful results in quantum simulations with fewer than 100 logical qubits, in optimization with fewer than 1,000 qubits, and in breaking encryption with about 4,096 qubits, by some estimates.[12] As of December 2024, Quantinuum holds the record for the largest number of entangled qubits, with 50 logical qubits.[13]

While that sounds low, it is a significant improvement from the breakthrough of 17 qubits in 2017.[14] Considering that it took 17 years to get from five to 17 qubits, there has been measurable, accelerating progress in this field. In 2018, companies were racing to increase the number of entangled qubits. In 2019, however, this changed, with companies beginning to focus on the *quality* (i.e., stability) of their qubits rather than the number of them. As scientists continue to increase both the number and quality of qubits, it is impossible to predict

[9] Adrian Cho, "IBM Casts Doubt on Google's Claims of Quantum Supremacy," *Science*, October 23, 2019; Feng Pan, Keyang Chen, and Pan Zhang, "Solving the Sampling Problem of the Sycamore Quantum Circuits," *Physical Review Letters*, Vol. 129, 2022.

[10] Andrew King, Alberto Nocera, Marek M. Rams, Jacek Dziarmaga, Roeland Wiersama, William Bernoudy, Jack Raymond, Nitin Kaushal, Niclas Heinsdorf, and Richard Harris et al., "Computational Supremacy in Quantum Simulation," arXiv, arXiv:2403.00919v1, March 2024.

[11] Public Law 115-368, National Quantum Initiative Act, December 21, 2018.

[12] Emily Grumbling and Mark Horowitz, *Quantum Computing: Progress and Prospects*, National Academies Press, 2019, p. 98.

[13] Karmela Padavic-Callaghan, "Another Record Has Been Set for the Most Entangled Logical Qubits," *New Scientist*, 2024.

[14] Kyree Leary, "17-Qubit Chips Have Officially Arrived, and So Begins the Quantum Revolution," *Futurism*, November 11, 2017.

how many physical qubits it will take to get a given number of logical qubits. By some estimates, breaking encryption will require a large number of qubits. For quantum simulation and optimization applications, there could be breakthroughs with more modest numbers of qubits. Estimates suggest that encryption will not be broken in the next decade.[15] Indeed, it may take 25 years or more for this to occur (although there could be some intermediate successes). However, quantum simulation and optimization may achieve breakthroughs in the next five years, while quantum-*assisted* AI may see breakthroughs in the next 20 to 30 years—yet the full promise of quantum AI may be farther out. However, there is fierce debate in the literature, and these estimates should be treated as educated guesses.

The following milestones—some of which were already discussed in this report—show the recent development of quantum computing and the logical milestones beyond today:

1. **Establishment of theoretical concepts.** In **1980**, at the first conference on the physics of computation at the Massachusetts Institute of Technology, Paul Benioff and Richard Feynman discussed the possibility of developing quantum computers.[16] At the conference, basic concepts were established, and the utility of such computers was discussed.
2. **Discovery of first application.** In **1994**, Shor developed an algorithm that can be used to break current cryptographic systems.[17] This represented the first proposed use case for a quantum computer that could solve a problem not solvable by classical computers.
3. **Demonstration of technical feasibility.** In **1998**, the first two- and three-qubit computers were demonstrated.[18] Experiments using these computers validated the theory of quantum computation.
4. **Development of commercially available quantum computers.** In **2010**, the D-Wave quantum annealing computer became the first commercially available system.[19] The device was sold to government agencies and corporations, including NASA, Lockheed Martin, and Google. IBM in **2016** and Rigetti in **2017** made their quantum computers available over the internet for researchers to use remotely.[20] In **2019**, IBM announced that it was building the first European quantum computer in Germany and in **2023** unveiled its IBM Quantum System Two.[21] By this

[15] Grumbling and Horowitz, 2019.

[16] Paul A. Benioff, "Quantum Mechanical Hamiltonian Models of Discrete Processes That Erase Their Own Histories: Application to Turing Machines," *International Journal of Theoretical Physics*, Vol. 21, No. 3, 1982.

[17] Shor, 1994.

[18] Chuang, 1998.

[19] Knapp, 2011.

[20] Aron, 2016; Simonite, 2017.

[21] Busvine, 2019; IBM, 2023.

time, researchers and engineers had obtained access to quantum computers and had started developing practical applications.

5. **Demonstration of quantum supremacy.** In **2019**, Google used its quantum computer to solve a problem that it claimed would take classical computers 10,000 years to solve.[22] IBM disputed that claim, arguing that theoretically a classical algorithm could be discovered that could solve the problem in two-and-a-half days.[23] In **2022**, researchers from China were able to run the same problem through a classical computer, solving it in 15 hours, although they claimed a supercomputer using their algorithm could complete the task in 200 seconds.[24] Even though IBM's assessment was accurate, Google demonstrated that a quantum computer could solve a problem orders of magnitude faster than a classical computer. Some have called this phase of development the noisy intermediate scale quantum technology era.[25] During this phase, quantum computers will outperform classical computers in certain tasks, but the qubit noise will limit them in size. Additionally, the supremacy baton will be passed back and forth between quantum and classical computers many times until quantum computers routinely solve problems that classical computers cannot.
6. **Demonstration of the solution of a critical problem.** Quantum supremacy verifies the existence of a problem that is solvable only by quantum computers. The next step is solving a problem of critical importance, such as a molecular simulation, that leads to the discovery of a new material or a new drug—a task that would be impossible to execute on a classical computer.
7. **Demonstration of a full-scale universal quantum computer.** A universal quantum computer would be able to solve a diverse set of critical problems.

This progression of milestones shows how quantum computing evolved, over 18 years, from basic concepts to the first technical demonstration of its capabilities. Another 12 years later, the first commercially available quantum computing system was created. Within the next nine years, quantum computing reached the quantum supremacy milestone. While it is difficult to predict how soon full-scale universal quantum computers will appear, the pace of innovation in the field is relatively high considering that it is a completely new technology with very little past work to build on.

[22] Arute et al., 2019.

[23] Cho, 2019.

[24] Pan, Chen, and Zhang, 2022.

[25] John Preskill, "Quantum Computing in the NISQ Era and Beyond," *Quantum*, Vol. 2, 2018.

APPENDIX B

Principles of Quantum Mechanics and Quantum Computers

Three quantum mechanical principles make computations with qubits possible: superposition, entanglement, and interference.[1] We discuss each briefly below.

Superposition

Superposition is the property that elementary particles have that allows them to be in multiple states at the same time. In other words, if there are two quantum states, they can be added together—or *superimposed*—to create another perfectly valid quantum state that is different from the two original states. An analogy from the current, non-quantum world (i.e., the macroscopic world in which we can see things with our own eyes) might be as follows:

Imagine you have a coin. You place it on a table, and it is either one of two things: heads or tails, zero or one. But what if you throw the coin in the air. Is it heads or tails? It is both. While it is in the air—if it is spinning perfectly—it is both heads and tails. To measure it, you can let it fall onto a surface. Then, you can see it as heads or tails—one or the other. However, imagine if it could remain suspended in the air, and if you could manipulate the coin while it was spinning, you could do computations while it is in this intermediary state of being—both heads and tails.[2] That state corresponds to the microscopic world of quantum computing.

Entanglement

Entanglement is what Einstein referred to as "spooky action at a distance," in which two particles could be entangled and placed at large distances apart, and the state of the two particles would be intertwined such that any attempt to measure one would be transmitted instanta-

[1] There is a fourth quantum mechanical principle used in a special class of quantum computers called *quantum annealing* computers. This principle will be discussed separately in a subsequent section in this appendix.

[2] This is still a metaphor using an analogue of a physical system that people are familiar with. A flipping coin should not be taken as a true representation of a qubit. The direction a coin is pointing at any given time while it is spinning in the air can be calculated. This is not the same as quantum superposition, and a spinning coin cannot be used to execute quantum computations.

neously to the other at arbitrarily large distances.[3] Note that entanglement is defined when measuring the state, because superposition means that particles are always in multiple states until measured. Superposition or entanglement cannot be seen in our macroscopic world, but one way of visualizing either principle is by referencing the coin toss analogy. If two regular coins are tossed in the air, they will each land on heads or tails randomly. In other words, there will be no pattern no matter how many times the experiment is repeated. However, with two entangled coins, every time one comes up heads, the other one would always come up tails. The fates of the two coins are in some way correlated, without there being any physical connection between them.

Interference

The superposition principle states that a particle can be in multiple states at any given time. One consequence of this principle is that a particle can be in different places at any given time. Interference not only means that particles can be in difference places at any given time but also that particles can cross their own paths and interfere with themselves. The way we can verify this property in the microscopic world is by taking a plate with two narrow horizontal slits and placing a photographic plate behind it. We then aim a photon through one of the slits. On the photographic plate, we will see a pattern of multiple lines of light and dark, indicating that another photon interfered with this one. This means that the photon itself also went through the other slit and interfered with itself at the other end of the plate.

How do these principles enable quantum computing? Superposition is what allows for the massive parallelism in the computation. Entanglement allows the computation between the qubits to take place. Interference is what allows us to extract the final result from the output of the calculation.

These quantum mechanical principles have no equivalents in classical physics and, therefore, seem very counterintuitive. Several interpretations have been proposed to explain these quantum phenomena, but the explanations often sound stranger than the phenomena they interpret. For example, the Copenhagen interpretation was developed by Niels Bohn and Werner Heisenberg. In this interpretation, physical entities do not have properties until they are observed, and it is only the observation that gives them defined physical properties.[4] Then again, there is the many-worlds interpretation, which proposes that physical entities have well-defined properties regardless of whether they are observed or not. However, they exist in many different parallel universes, and each property can be measured in each of these parallel worlds.[5]

---

[3] Einstein, 1971, p. 158.

[4] Jan Faye, "Copenhagen Interpretation of Quantum Mechanics," *Stanford Encyclopedia of Philosophy (Summer 2024 Edition)*, May 3, 2002, revised May 31, 2024.

[5] Lev Vaidman, "Many-Worlds Interpretation of Quantum Mechanics," *Stanford Encyclopedia of Philosophy (Fall 2021 Edition)*, March 24, 2002, revised August 5, 2021.

It should be noted that both of these interpretations are exactly equivalent and do not predict anything different when it comes to building and predicting the behavior of quantum systems. However, they show the difficulty of describing the inner workings of a quantum computer to a nonexpert or explaining how and why quantum computers work. Because digital computers exist as part of the macroscopic world that we can see and involve processes that can be explained, it is easier to understand how they work and to trust them; but because quantum computers exist in the microscopic world that we cannot see or understand—as noted, the explanations are counterintuitive—almost all people who will need to rely on quantum computing results will not understand or trust those results.

Types of Quantum Computers

Several different promising types of quantum computers are being developed by large commercial enterprises. Each type takes a slightly different approach, but they all rely on the ability of quantum particles to combine together in a state of entanglement and for these entangled particles to exist in many states simultaneously until they can be measured. Once the quantum particles are measured, superposition and entanglement cease. The final state of each of the particles leads to the quantum calculation.

Standard Quantum Computers

Most companies developing quantum computers are taking a similar approach. These include Google, IBM, Intel, and a sizable number of startups. These companies may use different quantum particles—superconducting loops, trapped ions, or electrons—but regardless of the particle used, the computation is basically the same. Developers initialize the quantum particles, subject them to a variety of quantum operations, and measure their end states. However, it is important to note that unlike a classical digital computer, quantum computers are probabilistic. When a measurement happens, there is some probability that the quantum state will jump to any one of the possible end states. For example, with a classical digital computer, when the output is 0100 in binary form, the final answer is 4. When the output of a quantum computer is 0100, however, the output is also 4, but there is no certainty that the final answer is 4. The quantum computation must be run several—or many—more times to be certain that 4 is the actual answer. The necessity of performing these extra runs adds some time to quantum computations, but this requirement is not among the biggest stumbling blocks of the technology. The main challenge posed by quantum computers is noise.

Because other outside particles could interact with qubits, quantum computers require isolation from the outside world. Interactions with outside particles are problematic because they would not be part of the quantum computation and would therefore throw off the results. This issue is one of the primary challenges of quantum computing. As the number of qubits grows, moreover, the impact of noise on the system also grows. Thus, it is not challenging to

create a quantum computer with many qubits. The challenge is keeping the interference low enough so that a quantum computer with many qubits can be effective.

There are several ways to reduce noise, including reducing the temperature of the qubits to extremely low levels and shielding them from electromagnetic signals. But because this approach is both expensive and cumbersome to operate, a significant amount of effort has been expended on quantum error correction algorithms as a means of reducing noise. These are algorithms that combine qubits together in a way that makes them, as a group, more resilient to noise—even if individually, their bits can be unstable, or their phase can be altered by the noise. This approach shows promise but requires a much higher number of qubits to succeed. However, even with sophisticated quantum error correction algorithms, noise currently limits the ability to scale quantum computers up to the number of qubits that would allow them to surpass the computational power of classical computers. But many in the quantum community expect that this will change soon, especially for a few very specific tasks.

Topological and Photon-Based Quantum Computers: The Promise of Stable Computation at Room Temperature

Topological quantum computing represents a different approach to quantum computing that does not use qubits in the same way. Whereas standard quantum computers address noise-induced errors using error-correcting circuits, topological quantum computers address noise-induced errors by altering the design of the qubits themselves. However, this approach relies on physics that have yet to be fully proven.

There is a type of two-dimensional particle called *a non-Abelian anyon*. States for these particles arise not from the individual particles themselves, but from the topology of the way the particles circle each other. This makes non-Abelian anyons inherently much more resilient to noise. This may all sound esoteric, but many different types of quasi–two-dimensional systems exist. In general, anyons have been proven to exist. In fact, Microsoft is betting big on being able to create and use non-Abelian anyons' insensitivity to noise to create quantum computers that can scale to large numbers of qubits more easily than standard quantum computers.[6] In 2018, Microsoft announced a first big breakthrough by creating a quasiparticle called a *Majorana fermion*, which could be the building block for a topological quantum computer. Further review of the work, however, showed fundamental flaws in the research design, causing the article to be retracted.[7] In 2022, Microsoft again claimed to have made a

[6] To do this, however, Microsoft needs to be able to tie many of these quasiparticles together to exhibit this non-Abelian anyon behavior. While Microsoft claims that it is close to achieving this, it is not known as of this writing whether Microsoft will succeed. If it does, however, Microsoft will have opened a new path toward stable and scalable quantum computers (Zhenghan Wang, "Topological Quantum Computation," *American Mathematical Society*, Vol. 112, April 2010).

[7] Majorana fermions were first conceived in 1937 by theoretical physicist Ettore Majorana. Since then, multiple experiments from multiple parties have attempted to create the theoretical particle (Ryan F. Mandelbaum, "Microsoft Creates Wild Half-Electron Quasiparticle for Its Future Quantum Computer," *Giz-*

similar breakthrough on topological quantum computing, although this breakthrough has also been disputed.[8] If Microsoft or others are ultimately successful, this could quickly scale to a resilient universal quantum computer of sufficient size in a matter of years, with fairly stable qubits at room temperature.

Another approach that promises computational scale at room temperature is photon-based quantum computers. Photons are stable at room temperature, and technologies for manipulating photons are mature and well understood. Entangling photons is a well-known process and can produce a significant number of entangled photons. Handling individual photons traveling at the speed of light does present a challenge, however. Researchers in China have developed a photon-based quantum computer and have claimed that it achieved a calculation significantly faster than a digital computer.[9] In 2024, researchers in South Korea successfully developed a quantum chip capable of controlling photons.[10]

Quantum Annealing Computers

A third type of quantum computer—the first one to become commercially available and currently the only one with a significant installed user base—operates in a very different way from either standard or topological quantum computers. Both standard and topological quantum computers operate similarly to classical computers by using *logic gates*—small electronic devices that process output based on a set of logical rules—to manipulate qubits. However, quantum annealing computers operate by trying to find the minimum energy of a system. Many important practical problems involve calculating minimum values, so quantum annealing is of great practical interest. It has been shown that quantum annealing computers are able to do the same types of calculations as standard and topological quantum computers, though perhaps not at the same rate.[11]

---

modo, March 28, 2018; Davide Castelvecchi, "Evidence of Elusive Majorana Particle Dies—but Computing Hope Lives On," *Nature*, Vol. 591, 2021).

[8] Morteza Aghaee, Arun Akkala, Zulfi Alam, Rizwan Ali, Alejandro Alcaraz Ramirez, Mariusz Andrzejczuk, Andrey E. Antipov, Pavel Aseev, Mikhail Astafev, et al., "InAs-Al Hybrid Devices Passing the Topological Gap Protocol," *Physical Review B*, Vol. 107, June 2023; Richard Hess, Henry F. Legg, Daniel Loss, and Jelena Klinovaja, "Trivial Andreev Band Mimicking Topological Bulk Gap Reopening in the Nonlocal Conductance of Long Rashba Nanowires," *Physical Review Letters*, Vol. 130, No. 207001, 2023.

[9] Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Xing Ding, Yi Hu, Peng Hu, et al., "Quantum Computational Advantage Using Photons," *Science,* Vol. 370, No. 6523, December 2020.

[10] Some believe that photon-based quantum circuits are the most-promising technologies being developed that may lead to a universal quantum computer. See National Research Council of Science and Technology, "Quantum Computing Researchers Develop an 8-Photon Qubit Chip," Phys.org, November 14, 2024.

[11] Dorit Aharonov, Wim van Dam, Julia Kempe, Zeph Landau, Seth Lloyd, and Oded Regev, "Adiabatic Quantum Computation Is Equivalent to Standard Quantum Computation," *SIAM Journal on Computing*, Vol. 37, No. 1, 2007.

Quantum annealing computers start by setting the superposition of their quantum particles to the lowest possible energy state. They then slowly alter the environment so that different configurations of the particles correspond to different energies. This new environment is chosen in such a way that the energies represent a value of interest and might help find the marked item in an unsorted database.[12]

While it is theoretically possible to use a quantum annealing computer to solve problems that would typically be solved by standard quantum computers, current technology is not adequate to achieve that. These types of quantum computers are limited to solving problems related to optimization or that can be formulated as optimization problems. D-Wave has adopted this approach.[13]

---

[12] Tameem Albash and Daniel A. Lidar, "Adiabatic Quantum Computing," *Reviews of Modern Physics,* Vol. 90, 2018.

[13] D-Wave, "How D-Wave Systems Work," webpage, undated.

Abbreviations

ABA	American Bar Association
AI	artificial intelligence
ANN	artificial neural network
CIO	chief information officer
COPPA	Children's Online Privacy Protection Act
EAR	Export Administration Regulations
ECRA	Export Control Reform Act
EU	European Union
FACTA	Fair and Accurate Credit Transactions Act
FCRA	Fair Credit Reporting Act
FOIA	Freedom of Information Act
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
ICT	information and communications technologies
ML	machine learning
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
PII	personally identifiable information

References

Aaronson, Scott, "Read the Fine Print," *Nature Physics*, Vol. 11, No. 4, 2015.

ABA—*See* American Bar Association.

Aghaee, Morteza, Arun Akkala, Zulfi Alam, Rizwan Ali, Alejandro Alcaraz Ramirez, Mariusz Andrzejczuk, Andrey E. Antipov, Pavel Aseev, Mikhail Astafev, et al., "InAs-Al Hybrid Devices Passing the Topological Gap Protocol," *Physical Review B*, Vol. 107, June 21, 2023.

Aharonov, Dorit, Wim van Dam, Julia Kempe, Zeph Landau, Seth Lloyd, and Oded Regev, "Adiabatic Quantum Computation Is Equivalent to Standard Quantum Computation," *SIAM Journal on Computing*, Vol. 37, No. 1, 2007.

Albash, Tameem, and Daniel A. Lidar, "Adiabatic Quantum Computing," *Reviews of Modern Physics*, Vol. 90, 2018.

Ambrogi, Robert, "Another State Adopts Duty of Technology Competence for Lawyers, Bringing Total to 40," *LawSites* blog, March 24, 2022.

American Bar Association, "Securing Communication of Protected Client Information," Formal Opinion 477R, revised May 22, 2017.

American Bar Association, *Model Rules of Professional Conduct*, 1983, last updated August 2023.

American Bar Association, "Ensuring Security: Protecting Your Law Firm and Client Data," *Law Technology Today*, 2024.

American Bar Association Center for Professional Development, "Encryption for Lawyers: Fulfilling Your Ethical Duties," continuing legal education training, American Bar Association Law Practice Division, September 28, 2016.

American Law Institute, *Restatement of the Law Third, Agency*, Vol. 1–2, American Law Institute Publishers, 2006.

Arghire, Ionut, "Law Firm Orrick Reveals Extensive Data Breach, Over Half a Million Affected," *SecurityWeek*, January 5, 2024.

Aron, Jacob, "Try Your Hand at Programming IBM's Online Quantum Computer," *NewScientist,* May 4, 2016.

Arute, Frank, K. Arya, R. Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Bell, et al., "Quantum Supremacy Using a Programmable Superconducting Processor," *Nature*, Vol. 574, 2019.

Balz, Suzan Dionne, and Olivier Hance, "Privacy and the Internet: Intrusion, Surveillance and Personal Data," *International Review of Law, Computers and Technology*, Vol. 10, No. 2, 1996.

Bayern, Shawn, "The Implications of Modern Business—Entity Law for the Regulation of Autonomous Systems," *European Journal of Risk Regulation*, Vol. 7, No. 2, 2016.

Beer, Kerstin, Dmytro Bondarenko, Terry Farrelly, Tobias J. Osborne, Robert Salzmann, Daniel Scheiermann, and Ramona Wolf, "Training Deep Quantum Neural Networks," *Nature Communications,* Vol. 11, No. 808, 2020.

Benioff, Paul A., "Quantum Mechanical Hamiltonian Models of Discrete Processes That Erase Their Own Histories: Application to Turing Machines," *International Journal of Theoretical Physics*, Vol. 21, No. 3, 1982.

Benjamin, Louise M., "Privacy, Computers, and Personal Information: Toward Equality and Equity in an Information Age," *Communications and the Law*, Vol. 3, No. 2, 1991.

Blaustein, Stacey, Melinda L. McLellan, and James A. Sherer, "Digital Direction for the Analog Attorney—Date Protection, E-Discovery, and the Ethics of Technological Competence in Today's World of Tomorrow," *Richmond Journal of Law and Technology*, Vol. 22, No. 4, 2016.

Bookman, Samantha, "15 Huge Supercomputers That Were Less Powerful Than Your Smartphone," *The Clever*, April 18, 2017.

Briggs, Bill, Khalid Kark, Peter Vanderslice, Anthony Abbattista, George Collins, David Sisk, David Schmitz, Andy Dacher, Tom Galizia, Prashanth Ajjampur, et al., "Tech Trends 2015: The Fusion of Business and IT—An Insurance Industry Perspective," Deloitte, 2015.

Bureau of Industry and Security, "Commerce Control List: Additions and Revisions; Implementation of Controls on Advanced Technologies," *Federal Register*, Vol. 89, No. 173, September 6, 2024.

Busvine, Douglas, "IBM, Fraunhofer Partner on German-Backed Quantum Computing Research Push," Reuters, September 10, 2019.

California State Bar Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179, 2010.

Carey, Joseph, "Star Wars the Last Jedi: Is 'the Force' of Kylo Ren and Rey REAL? Quantum Science Reveals," *Express*, December 17, 2017.

Castelvecchi, Davide, "Evidence of Elusive Majorana Particle Dies—but Computing Hope Lives On," *Nature*, Vol. 591, 2021.

Cho, Adrian, "IBM Casts Doubt on Google's Claims of Quantum Supremacy," *Science*, October 23, 2019.

Chuang, Isaac L., Neil Gershenfeld, and Mark Kubinec, "Experimental Implementation of Fast Quantum Searching," *Physical Review Letters*, Vol. 80, No. 15, April 13, 1998.

Code of Federal Regulations, Title 16, Commercial Practices; Chapter I, Federal Trade Commission; Subchapter C, Regulations Under Specific Acts of Congress; Part 312.3, Regulation of Unfair or Deceptive Acts or Practices in Connection with the Collection, Use, and/or Disclosure of Personal Information from and About Children on the Internet.

Code of Federal Regulations, Title 16, Commercial Practices; Chapter I, Federal Trade Commission; Subchapter C, Regulations Under Specific Acts of Congress; Part 312.8, Confidentiality, Security, and Integrity of Personal Information Collected from Children.

Code of Federal Regulations, Title 45, Public Welfare; Subtitle A, Department of Health and Human Services; Subchapter C, Administrative Data Standards and Related Requirements; Part 164, Security and Privacy; Part 160, General Administrative Requirements; Subpart A, General Provisions; Section 160.103, Definitions.

Code of Federal Regulations, Title 45, Public Welfare; Subtitle A, Department of Health and Human Services; Subchapter C, Administrative Data Standards and Related Requirements; Part 164, Security and Privacy; Subpart C, Security Standards for the Protection of Electronic Protected Health Information; Section 164.306, Security Standards: General Rules.

Code of Federal Regulations, Title 45, Public Welfare; Subtitle A, Department of Health and Human Services; Subchapter C, Administrative Data Standards and Related Requirements; Part 164, Security and Privacy; Subpart C, Security Standards for the Protection of Electronic Protected Health Information; Section 164.514, Other Requirements Relating to Uses and Disclosures of Protected Health Information.

Costigan, Johanna, and Graham Webster, eds., "14th Five-Year Plan for National Informatization," DigiChina, 2022.

Cross, Tim, "After Moore's Law," *The Economist Technology Quarterly*, March 11, 2016.

D-Wave, "How D-Wave Systems Work," webpage, undated. As of March 11, 2025: https://www.dwavequantum.com/learn/quantum-computing/

D-Wave, "Quantum Optimization Data Sheet," 2023.

de Touzalin, Aymard, Charles Marcus, Freeke Heijman, Ignacio Cirac, Richard Murray, and Tommaso Calarco, "Quantum Manifesto: A New Era of Technology," Quantum Europe Conference, May 17–18, 2016.

DeWitt, Bryce S., "Quantum Mechanics and Reality," *Physics Today*, Vol. 23, No. 9, 1970.

Duggal, Pavan, *Quantum Computing Law*, Cyberlaw University, 2018.

Einstein, Albert, *The Born-Einstein Letters: Correspondence Between Albert Einstein and Max and Hedwig Born from 1916–1955, with Commentaries by Max Born*, Macmillan, 1971.

Einstein, Albert, Boris Podolsky, and Nick Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" *Physical Review*, Vol. 47, 1935.

Elliott, Marc N., Kirsten Becker, Megan K. Beckett, Katrin Hambarsoomian, Philip Pantoja, and Benjamin Karney, "Using Indirect Estimates Based on Name and Census Tract to Improve the Efficiency of Sampling Matched Ethnic Couples from Marriage License Data," *Public Opinion Quarterly,* Vol. 77, No. 1, 2013.

Ethics and Practice Guidelines Committee, "RE: Ethics Opinion 11-01," memorandum to Iowa State Bar Association executive director, Iowa State Bar Association, September 9, 2011.

EU—*See* European Union.

European Commission, "Horizon Europe," webpage, undated. As of March 5, 2025: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

European Commission, "Quantum Technologies Flagship Kicks Off with First 20 Projects," press release, October 28, 2018.

European Commission, "Digitalisation of Justice in the European Union: A Toolbox of Opportunities," memorandum to the European Parliament, the European Council, the European Economic and Social Committee, and the Committee of Regions, December 2020.

European Commission, "The European Quantum Communication Infrastructure (EuroQCI) Initiative," webpage, last updated October 22, 2024. As of February 27, 2025: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

European Commission for the Efficiency of Justice, *Evaluation Report on European Judicial Systems, Part 1*, Council of Europe, 2020.

European Parliament, Council of the European Union, "On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," Directive 95/46/EC, October 24, 1995.

European Union, "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)," *Official Journal of the European Union,* Regulation EU 2016/679, April 27, 2016.

Everett, Hugh, *Theory of the Universal Wave Function*, Princeton University, 1956.

Ezekiel, Alan W., "Hackers, Spies, and Stolen Secrets: Protecting Law Firms from Data Theft," *Harvard Journal of Law and Technology*, Vol. 26, No. 2, Spring 2013.

Faye, Jan, "Copenhagen Interpretation of Quantum Mechanics," *Stanford Encyclopedia of Philosophy (Summer 2024 Edition)*, May 3, 2002, revised May 31, 2024.

Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions," webpage, July 2020, last updated January 2024. As of February 20, 2025:
https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions

Ferro, David, "The Unbelievable Bug of the 21st Century," editorial, *Standard-Examiner*, March, 25, 2020. As of February 20, 2025:
https://www.standard.net/news/2020/mar/25/
dr-david-ferro-the-unbelievable-bug-of-the-st-century/

Feynman, Richard P., "Simulating Physics with Computers," *International Journal of Theoretical Physics*, Vol. 21, 1982.

Giovannetti, Vittorio, Seth Lloyd, and Lorenzo Maccone, "Quantum Random Access Memory," *Physical Review Letters*, Vol. 100, April 2008.

Giuffrida, Iria, Frederick Lederer, and Nicolas Vermerys, "A Legal Perspective on the Trials and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law," *Case Western Reserve Law Review*, Vol. 68, No. 3, 2018.

Graham, Luke, "Quantum Computer Worth $15 Million Sold to Tackle Cybersecurity," CNBC, January 27, 2017.

Greig, Jonathan, "U.S. Court System Demands Massive Changes to Court Documents After Solarwinds Hack," *TechRepublic*, February 12, 2021.

Grumbling, Emily, and Mark Horowitz, *Quantum Computing: Progress and Prospects*, National Academies Press, 2019.

Harrow, Aram W., Avinatan Hassidim, Seth Lloyd, "Quantum Algorithm for Solving Linear Systems of Equations," *Physical Review Letters*, Vol. 103, No. 15, October 2009.

Hess, Richard, Henry F. Legg, Daniel Loss, and Jelena Klinovaja, "Trivial Andreev Band Mimicking Topological Bulk Gap Reopening in the Nonlocal Conductance of Long Rashba Nanowires," *Physical Review Letters*, Vol. 130, No. 207001, 2023.

Hill, Louise Lark, "Cloud Nine or Cloud Nein: Cloud Computing and Its Impact on Lawyers' Ethical Obligations and Privileged Communications," *Journal of the Professional Lawyer*, 2013.

Hofmann v. Jerico Pictures, Inc., 0:24-cv-61383, Southern District of Florida, August 1, 2024.

IBM, "IBM Debuts Next-Generation Quantum Processor: IBM Quantum System Two, Extends Roadmap to Advance Era of Quantum Utility," December 4, 2023.

IMS Health Inc. v. Ayotte, 490 F. Supp. 2d 163, New Hampshire, April 30, 2007.

Johnson, Walter G., "Governance Tools for the Second Quantum Revolution," *Jurimetrics Journal*, Vol. 59, February 2019.

Kalai, Gil, "The Argument Against Quantum Computers," in Meir Hemmo and Orly Shenker, eds., *Quantum, Probability, Logic: Itamar Pitowsky's Work and Influence*, Springer, 2020.

Karch, Theodore J., Ashwin Kaja, and Yan Luo, "China's Vision for the Next Generation of Artificial Intelligence," *National Law Review,* Vol. 8, No. 84, March 25, 2018.

King, Andrew, Alberto Nocera, Marek M. Rams, Jacek Dziarmaga, Roeland Wiersama, William Bernoudy, Jack Raymond, Nitin Kaushal, Niclas Heinsdorf, Richard Harris, et al., "Computational Supremacy in Quantum Simulation," arXiv, arXiv:2403.00919v1, March 2024.

Knapp, Alex, "D-Wave Sells Quantum Computer to Lockheed Martin," *Forbes*, May 25, 2011.

Leary, Kyree, "17-Qubit Chips Have Officially Arrived, and So Begins the Quantum Revolution," *Futurism,* November 11, 2017.

Magee, Peder, "Privacy and Identity Protection from the Fair Credit Reporting Act to Big Data," *Antitrust*, Vol. 29, No. 1, 2014.

Mandelbaum, Ryan F., "Microsoft Creates Wild Half-Electron Quasiparticle for Its Future Quantum Computer," *Gizmodo*, March 28, 2018.

Marchant, Gary E., Douglas J. Sylvester, and Kenneth W. Abbott, "What Does the History of Technology Regulation Teach Us About Nano Oversight?" *Journal of Law, Medicine, and Ethics*, Vol. 37, No. 4, Winter 2009.

Martin, Karen, "Waiting for Quantum Computing: Why Encryption Has Nothing to Worry About," *TechBeacon*, August 15, 2018.

Merriam-Webster, "Particle," dictionary entry, webpage, undated. As of March 11, 2025: https://www.merriam-webster.com/dictionary/particle

National Institute of Standards and Technology, *Status Report on the Third Round of NIST Post-Quantum Cryptography Standardization Process*, update 1, IR 8413, 2022.

National Research Council of Science and Technology, "Quantum Computing Researchers Develop an 8-Photon Qubit Chip," Phys.org, November 14, 2024.

National Security Agency, "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ," September 7, 2022.

NIST—*See* National Institute of Standards and Technology.

O'Connell, Cathal, "Quantum Computing for the Qubit Curious," *Cosmos,* July 5, 2019.

Okuda, Michael, Denise Okuda, and Debbie Mirek, *The Star Trek Encyclopedia*, Pocket Books, 1994.

Orzel, Chad, "What the Many-Worlds Interpretation of Quantum Physics Really Means," *Forbes*, January 5, 2016.

Padavic-Callaghan, Karmela, "Another Record Has Been Set for the Most Entangled Logical Qubits," New Scientist, 2024.

Pan, Feng, Keyang Chen, and Pan Zhang, "Solving the Sampling Problem of the Sycamore Quantum Circuits," *Physical Review Letters*, Vol. 129, 2022.

Pati, Arun Kumar, and Samuel L. Braunstein, "Impossibility of Deleting an Unknown Quantum State," *Nature*, Vol. 404, No. 6774, 2000.

Pednault, Edwin, John Gunnels, Giacomo Nannicini, Lior Horesh, and Robert Wisnieff, "Leveraging Secondary Storage to Simulate Deep 54-Qubit Sycamore Circuits," arXiv, arXiv: 1910.09534, 2019.

Porter, C. Christine, "De-Identified Data and Third Party Data Mining: The Risk of Re-Identification of Personal Information," *Washington Journal of Law, Technology and Arts*, Vol. 5, No. 1, 2008.

Powell, Nathan, "Electronic Ethics: Lawyers' Ethical Obligations in a Cyber Practice," *Georgetown Journal of Legal Ethics*, Vol. 29, No. 4, 2016.

Preskill, John, "Quantum Computing in the NISQ Era and Beyond," *Quantum*, Vol. 2, 2018.

Public Law 89-487, The Freedom of Information Act, July 5, 1967.

Public Law 106-102, Gramm-Leach-Bliley Act, November 12, 1999.

Public Law 115-232, John S. McCain National Defense Authorization Act for Fiscal Year 2019, August 13, 2018.

Public Law 115-368, National Quantum Initiative Act, December 21, 2018.

Puiszis, Steven M., "Perspective: Technology Brings a New Definition of Competency," Bloomberg Law, April 12, 2016.

Quantum Flagship, *Strategic Research Agenda*, European Quantum Flagship, March 2020.

Quantum Flagship, *Strategic Research and Industry Agenda 2030: Roadmap and Quantum Ambitions over This Decade*, 2023a.

Quantum Flagship, *Quantum Technologies: Public Policies in Europe*, QuantERA, October 17, 2023b.

Shankar, A. J., "Ransomware Attackers Take Aim at Law Firms," *Forbes*, March 12, 2021.

Sherwinter, Daniel J., "Surveillance's Slippery Slope: Using Encryption to Recapture Privacy Rights," *Journal on Telecommunications and High Technology Law*, Vol. 5, No. 2, Winter 2007.

Shor, Peter W., "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, November 20–22, 1994.

Simonite, Tom, "The Quantum Computer Factory That's Taking on Google and IBM," *Wired*, June 20, 2017.

Solove, Daniel J. "A Brief History of Information Privacy Law," in Kristen J. Matthews, ed., *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, 2nd edition, Practicing Law Institute, January 7, 2017.

Soma, John T., and Richard A. Wehmhoefer, "A Legal and Technical Assessment of the Effect of Computers on Privacy," *Denver Law Review*, Vol. 60, No. 3, 1983.

State Council of the People's Republic of China, "The National Medium- and Long-Term Program for Science and Technology Development (2006–2020): An Outline," 2006.

Tupper, Stephen L., "The View from the GC's Desk: Security and Privacy Issues That Keep General Council Up at Night," *Michigan State Journal of International Law,* Vol. 16, No. 1, 2007.

Universities Space Research Association, "First Quantum Annealing Computer in the U.S. to Have More Than 2000 Qubits Installed and Operational," press release, August 31, 2017.

U.S. Code, Title 5, Section 552a, Records Maintained on Individuals.

U.S. Code, Title 15, Chapter 41, Subchapter III, Section 1681, Disclosures to Consumers.

U.S. Code, Title 50, Chapter 58, Subchapter I, Section 4817, Requirements to Identify and Control the Export of Emerging and Foundational Technologies.

U.S. Department of Justice, *Overview of the Privacy Act of 1974 (2020 Edition)*, 2020.

Vaidman, Lev, "Many-Worlds Interpretation of Quantum Mechanics," *Stanford Encyclopedia of Philosophy (Fall 2021 Edition)*, March 24, 2002, revised August 5, 2021.

Volkswagen Group, "Where Is the Electron and How Many of Them?" *Global Energy World,* November 6, 2019.

Wang, Zhenghan, "Topological Quantum Computation," *American Mathematical Society*, Vol. 112, April 2010.

Washburn, Pat, "Electronic Journalism, Computers and Privacy," *Computer Law Journal*, Vol. 3, No. 1, 1981.

Webster, Graham, Rogier Creemers, Elsa Kania, and Paul Triolo, "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)," August 1, 2017. As of March 10, 2025:
https://d1y8sb8igg2f8e.cloudfront.net/documents/translation-fulltext-8.1.17.pdf

White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," May 4, 2022.

Wolf, Kevin J., Thomas J. McCarthy, and Andrew R. Schlossberg, "The Export Control Reforms Act and Possible New Controls on Emerging and Foundational Technologies," *Akin,* September 12, 2018.

Wootters, William K., and Wojciech H. Zurek, "A Single Quantum Cannot Be Cloned," *Nature*, Vol. 299, No. 5886, 1982.

Zalka, Christoff, "Grover's Quantum Searching Algorithm is Optimal," *Physical Review A*, Vol. 60, No. 4, 1999.

Zhong, Han-Sen, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Xing Ding, Yi Hu, Peng Hu, et al., "Quantum Computational Advantage Using Photons," *Science*, Vol. 370, No. 6523, December 2020.