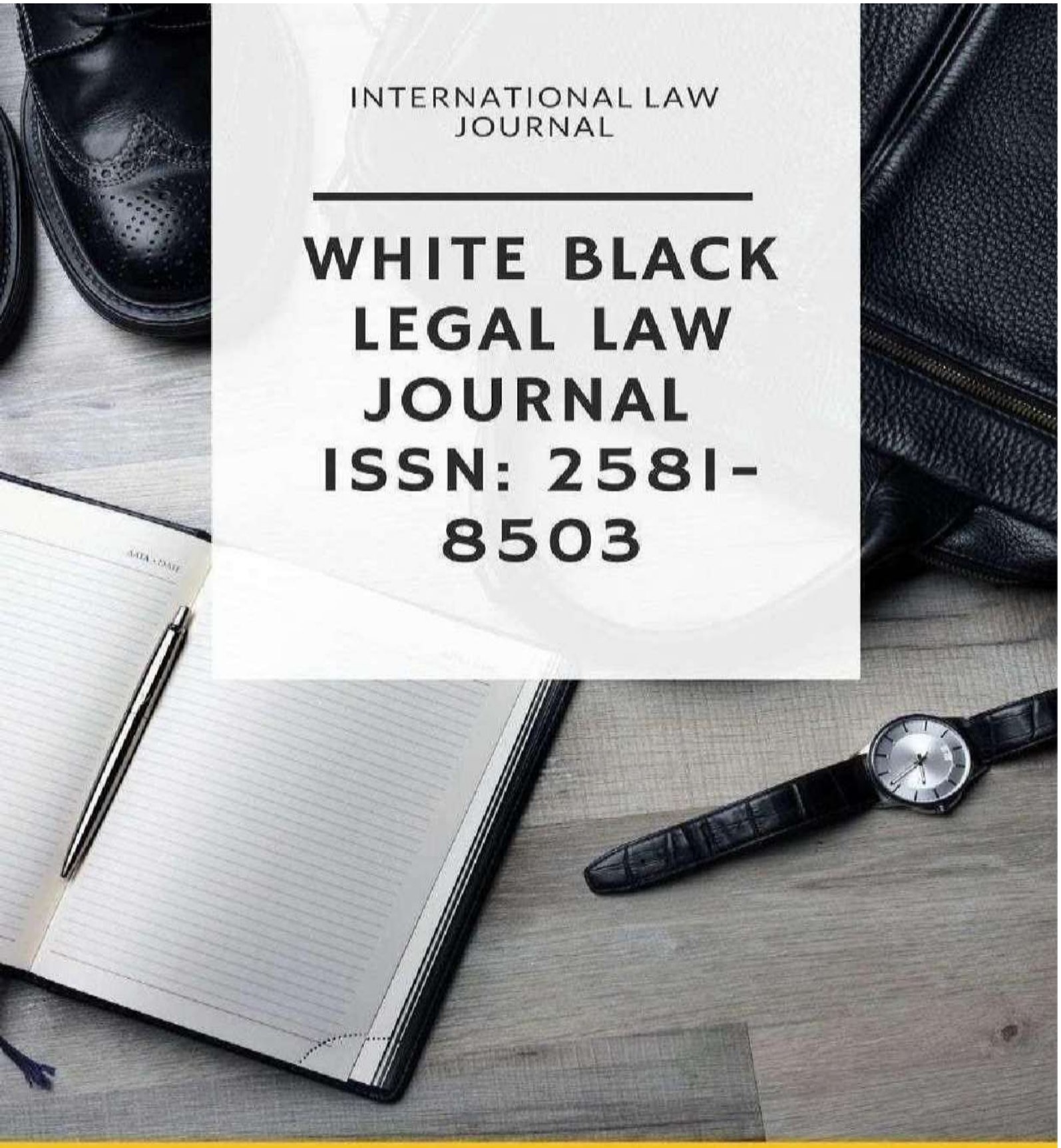

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | April 2025 ISSN: 2581-8503

POST-QUANTUM CRYPTOGRAPHY LAW: PREPARING LEGAL SYSTEMS FOR THE ENCRYPTION ARMS RACE

AUTHORED BY - RISHABH SHARMA

Abstract

Recent advancements in quantum computing have been threatening the cryptographic underpinnings of modern legal and digital systems. At the end of the day, quantum decryption would have serious implications for privacy laws, contractual agreements, and national security frameworks that currently depend on encryption standards susceptible to quantum attacks. Utilizing both interdisciplinary approach, The research demonstrates that algorithms like Shor's or Grover's can undermine popular protocols, including RSA, ECC, and AES, revealing flaws in legal frameworks such as HIPAA, GDPR, or eIDAS. We find existential threats such as the obsolescence of "secure" encrypted data; organizational liability pressures; and state-level surveillance overreach. One recommendation is for legislation on post-quantum cryptography (PQC), noting that national, standards, and treaty action are required to counter the problem — and ethical safeguards are necessary to avoid inequities in adoption. This research serves as a guide for preparing legal systems for the quantum future, synthesising insights from law, computer science, and policy, emphasizing the time-sensitive nature of the work, collaboration, and the role of innovation in provisioning sensitive data for the looming leap in cryptography to come.

Keywords: quantum computing, post-quantum cryptography, encryption laws, data privacy, Shor's algorithm, regulatory frameworks, cybersecurity policy.

Introduction

Imagine this scenario: It's 2030, and a shadowy organization announces in hushed tones a quantum computer that can break RSA-2048, which protects a giant trove of legally sensitive documents. Overnight, decades of encrypted attorney-client communications, intellectual property records and classified national security files are exposed. The assumption that encryption provides permanent confidentiality is blown apart, setting off an earthquake of

litigation and a social one, as well. This is not science fiction; this is a real and present danger that warrants immediate action and attention from legal scholars and policymakers alike.

Quantum computing is emerging by exploiting the principles of quantum mechanics that can transform the computation. Where classical computers are bit-based systems that can be either 0 or 1, qubits in quantum computers can be in superposition between both states simultaneously. This makes possible some algorithms that allow quantum computers to solve on certain problems exponentially faster than the classical ones.[1] This computational power presents a profound risk to classical cryptography, the foundation of contemporary data-driven communication, despite unlocking unparalleled potential in disciplines as diverse as medicine and materials science.[2] Post-quantum cryptographic algorithms running on conventional devices that are secure against the cryptanalytic attacks from both classical and quantum computers are referred to as post-quantum cryptography (PQC), quantum-safe cryptography, or quantum-resilient cryptography.[3] The sophistication of quantum computing makes it imperative to adopt PQC and save such sensitive data.

This is an issue because existing legal structures are not able to address implications of quantum decryption. Legislation such as the Electronic Communications Privacy Act (ECPA), the Health Insurance Portability and Accountability Act (HIPAA)[4], and the EU's electronic Identification, Authentication and Trust Services (eIDAS) Regulation frequently depends on the assumed inviolability of current encryption standards.[5] For example, data breach notification laws often include exceptions from mandatory disclosure for encrypted data, since it is assumed that encryption makes stolen data unusable.[6] But this assumption falls apart under quantum computing. As Kasim Balarabe notes, forward-looking data protection policies and the adoption of post-quantum cryptography are needed.[7] The law recognizes the future threat that quantum decryption poses to federal administrative agencies and orders an examination of the agencies' data. Even quantum learning systems, similar to classical classifiers based on

[1] Kasim Balarabe, Quantum Computing and the law: Navigating the legal implications of a quantum leap, European Journal of Risk Regulation. 1, 1 (2025)
[2] Id. at 2.
[3] National Security Agency, *Quantum Computing and Post-Quantum Cryptography FAQs* (Aug. 2021), https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF.
[4] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).
[5] Phillip Harmon, Data Breach Notification Laws and the Quantum Decryption Problem, 79 Wash. & Lee L. Rev. 475, 477 (2022), https://scholarlycommons.law.wlu.edu/wlulr/vol79/iss1/11/.
[6] Id. at 484.
[7] Kasim. Supra note 1.

classical neural networks, are vulnerable to crafted adversarial examples, independent of whether the input data is classical or quantum.[8]

This report seeks to address the legal vacuum created by the advent of quantum computing by exploring the following research questions:

- How will quantum decryption challenge existing legal principles related to privacy, contract law, and national security?
- What regulatory frameworks can be developed to preempt adversarial quantum hacking and ensure the continued protection of sensitive information in a post-quantum world?

To answer these questions, this report will employ a doctrinal analysis of relevant laws, including ECPA, HIPAA, and eIDAS, examining their implicit assumptions about encryption and their vulnerability to quantum decryption. In addition, case studies, such as the National Institute of Standards and Technology's (NIST) Post-Quantum Cryptography Standardization project, will be analyzed to assess the progress and challenges in developing quantum-resistant cryptographic solutions. NIST announced the three finalists: FIPS 203 is a general encryption standard, and FIPS 204 and 205 are digital signature standards for authenticating users. This analysis will draw upon interdisciplinary research, incorporating insights from computer science, cryptography, and legal theory to provide a comprehensive assessment of the legal landscape. This report aims to offer original insights and analysis, moving beyond mere summarization of existing literature to propose concrete recommendations for preparing legal systems for the encryption arms race of the quantum era.

The Quantum Threat to Legal Encryption

The rapid advancement of quantum computing presents a looming threat to the foundations of modern cryptography, with profound implications for legal systems worldwide. However, quantum computers, based on the principles of quantum mechanics, have the potential to break existing encryption algorithms. As quantum computing technology develops, the need to understand and counter the quantum threat to the legal encryption community is acute. This report looks at how quantum computers will shatter existing encryption, the legal systems yet to be migrated, and the timeline for this transition. Fortune Business Insights predicts that annual quantum computing revenue will reach $12.6 billion by 2032, underscoring the growing

[8] Sirui Lu et al., Quantum Adversarial Machine Learning, 2 Phys. Rev. Res. 033212, 1 (2020), https://doi.org/10.1103/PhysRevResearch.2.033212.

importance of this field.[9]

How Quantum Computers Break Current Encryption

Classical cryptography relies on the computational difficulty of certain mathematical problems, such as integer factorization and discrete logarithms. However, quantum algorithms offer dramatically faster solutions to these problems, rendering many widely used encryption methods vulnerable.[10]

Shor's Algorithm vs. RSA/ECC

Shor's algorithm, a quantum algorithm formulated by Peter Shor in 1994 that can factor large numbers efficiently into their prime factors.[11] This is a direct threat to the RSA (Rivest-Shamir-Adleman) encryption (based on the difficulty of factoring large numbers).[12] Likewise, Shor's algorithm can also efficiently compute discrete logarithms, which breaks the security of Elliptic Curve Cryptography (ECC) and Diffie-Hellman key exchange. These algorithms are critical to secure communications protocols like TLS, SSL, and VPNs, and their compromise would have global ramifications. Factoring a 1024-bit RSA key takes approximately 10 days with a 1024 qubit quantum computer, while factoring a 2048-bit RSA key takes approximately 8 hours with a 20 million qubit quantum computer.[13]

Grover's Algorithm vs. Symmetric Keys

Grover's algorithm, in contrast to Shor's, targets symmetric-key algorithms like AES (Advanced Encryption Standard).[14] While it doesn't break symmetric keys entirely, Grover's algorithm provides a quadratic speedup in brute-force attacks, reducing the effective key length by half. For example, AES-128, which classically requires $O(2^{128})$ operations to brute-force, would only require $O(2^{64})$ operations with Grover's algorithm. Similarly, cryptographic hash functions like SHA-256, which classically require $O(2^n)$ operations to find a preimage, are

[9] Joe Panettieri, Quantum Computing Timeline: What's Coming, When Will It Arrive, And Why Quantum Matters, Sustainable Tech Partner (Mar. 21, 2025), https://sustainabletechpartner.com/news/quantum-computing-timeline-whats-coming-when-will-it-arrive-and-why-quantum-matters/.
[10] Daniel J. Bernstein, Introduction to Post-Quantum Cryptography, in *Post-Quantum Cryptography* 1, 1–14 (Daniel J. Bernstein et al. eds., 2009), https://doi.org/10.1007/978-3-540-88702-7_1.
[11] Aryan Sahni & Ridhima Sahni, Decrypting the Future: Quantum Computing and The Impact of Grover's and Shor's Algorithms on Classical Cryptography, EasyChair Preprint No. 14978, at 1 (Sept. 21, 2024), https://easychair.org/publications/preprint/NJCx.
[12] Id.
[13] Id at 8.
[14] Id.

reduced to $O(2^{(n/2)})$ with Grover's algorithm. While doubling the key size can mitigate this threat, it necessitates a transition to algorithms like AES-256, which then becomes AES-128 in terms of quantum resistance.[15]

The following table summarizes the impact of Shor's and Grover's algorithms:

Algorithm	Target	Classical Security	Quantum Security	Impact	Mitigation
Shor's	RSA, ECC, Diffie-Hellman	Factoring Difficulty	Efficient Factoring	Breaks public-key cryptography; compromises digital signatures	Transition to Post-Quantum Cryptography (PQC)
Grover's	AES, SHA	Brute-Force	Quadratic Speedup	Reduces effective key length; weakens symmetric-key and hash fun€ctions	Increase key size

Timeline Estimates

Estimating the timeline for the arrival of quantum computers capable of breaking current encryption is challenging. The intelligence community recognized the quantum threat as early as 2015, with the NSA announcing plans to transition National Security Systems (NSS) to quantum-resilient cryptography.[16] In contrast, industry projections from companies like Google suggest commercial quantum computing applications may emerge within five years.[17]

The US government has also formalized its approach, with White House memos mandating that federal agencies prepare for a transition to Post-Quantum Cryptography (PQC).[18] This

[15] Id
[16] US Government Quantum Timeline, QuSecure (Jan. 3, 2024), https://www.qusecure.com/us-government-quantum-timeline/.
[17] Joe Panettieri, Quantum Computing Timeline: What's Coming, When Will It Arrive, And Why Quantum Matters, Sustainable Tech Partner (Mar. 21, 2025), https://sustainabletechpartner.com/news/quantum-computing-timeline-whats-coming-when-will-it-arrive-and-why-quantum-matters/.
[18] QuSecure, supra note 18.

includes the National Quantum Initiative Act (NQI)[19] which has funded initiatives focused on advancing quantum technologies. NIST has already released final versions of its first three Post Quantum Crypto Standards in 2024.[20] These differing perspectives highlight the uncertainty surrounding the timeline, but the consensus is that proactive measures are necessary to prepare for the quantum threat.

Legal Systems at Risk

The vulnerability of current encryption algorithms to quantum computers poses significant risks to various legal systems that rely on secure data transmission and storage.

Data Privacy Laws: HIPAA, GDPR

Data privacy laws, such as HIPAA (Health Insurance Portability and Accountability Act) in the United States and GDPR (General Data Protection Regulation)[21] in the European Union, mandate the protection of sensitive personal data. If quantum computers can break the encryption protecting this data, it could lead to severe breaches of privacy and violations of these laws. For example, pseudonymized data, which is often used to comply with GDPR, could be re-identified if the underlying encryption is compromised. The Council Decision (EU) 2016/920, an agreement between the US and EU, establishes a framework for data protection principles and safeguards for personal information transferred for criminal law enforcement purposes.[22] This agreement, and related directives, could be undermined if quantum computers compromise the encryption protecting this data.

Digital Contracts: Blockchain Smart Contracts, e-signatures (eIDAS)

Digital contracts, including blockchain smart contracts and e-signatures governed by regulations like eIDAS (electronic Identification, Authentication and Trust Services), also face significant risks.

These cryptographic techniques are the keys to preventing fraud and ensuring the integrity of

[19] National Quantum Initiative Act, Pub. L. No. 115-368, 132 Stat. 5092 (2018).
[20] NIST Releases First 3 Finalized Post-Quantum Encryption Standards, Nat'l Inst. of Standards & Tech. (Aug. 13, 2024), https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.
[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[22] Council Decision 2016/920, 2016 O.J. (L 154) 1 (EU).

agreements, thus heavily leaning on algorithms such as RSA and ECC.[23] The algorithms can be broken by Shor's algorithm, which will help attackers to fake digital signatures, change smart contract code, and lose trust in network transactions.[24] The eIDAS 2 (EU Digital Identity Regulation) which, by offering secure digital identity wallets, is to serve all EU citizens also requires quantum resilience for the cryptographic solutions to succeed. Three post-quantum encryption standards have been finalized and approved by NIST and FIPS standards.[25] These actions are fundamental to the sustained security of digital identity and trust services against quantum attacks.

National Security: Classified Communications, FISA Implications

National security is also at risk, as classified communications and data protected by encryption could be decrypted by quantum computers. This has implications for intelligence gathering, military operations, and diplomatic communications. The US government is taking steps to address this threat, with agencies like DISA (Defense Information Systems Agency) and NIST releasing roadmaps to prepare for the transition to PQC.[26] The Quantum Computing Cybersecurity Preparedness Act[27] encourages federal government agencies to adopt technology that will protect against quantum computing attacks. However, the potential for adversaries to "harvest now, decrypt later" poses a long-term risk, as encrypted data intercepted today could be decrypted once quantum computers become powerful enough.[28]

Legal encryption faces a crisis, as quantum computing continues to advance at an alarming rate, outstripping the predictions of many experts. Going further, quantum computers can be able to break existing encryption algorithms, compromising the security of data privacy laws, digital contracts, and national security. Although it is difficult to predict when quantum computing will enable the breaking of existing encryption, we need to be forward thinking to ensure a smooth transition during the changeover. Such measures comprise the investment in post-quantum cryptography research and development, the establishment and implementation

[23] Sahni & Sahni, supra note 13, at 9.
[24] Sahni & Sahni, supra note 13, at 10.
[25] NIST Releases First 3 Finalized Post-Quantum Encryption Standards, Nat'l Inst. of Standards & Tech. (Aug. 13, 2024), https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.
[26] QuSecure, supre note 18.
[27] Quantum Computing Cybersecurity Preparedness Act, Pub. L. No. 117-260, 136 Stat. 2389 (2022).
[28] Joe Panettieri, Quantum Computing Timeline: What's Coming, When Will It Arrive, And Why Quantum Matters, Sustainable Tech Partner (Mar. 21, 2025), https://sustainabletechpartner.com/news/quantum-computing-timeline-whats-coming-when-will-it-arrive-and-why-quantum-matters/.

of novel standards and regulations, and the promotion of awareness among legal professionals and policymakers. Through these measures, the legal sector is able to lessen the quantum threat and maintain the security of sensitive data and messages in the quantum age.

Legal and Regulatory Gaps

To surmount the challenge, the importance of quantum computing will undoubtedly require the evolution of laws and regulations to better protect sensitive data with respect to the vulnerabilities of quantum. Important substantive issues involve spying law, responsibility for quantum weaknesses, and global splintering.

Post-Quantum Surveillance Law

Quantum computers pose a particular challenge to surveillance laws. In a kind of "backdoor" workaround, quantum decryption could enable governments to circumvent conventional encryption and access communications and data that were previously secure. This capability has significant free speech implications as they relate directly to the right to be free from unreasonable search and seizure.

There are cases like Apple vs FBI[29] which usually are encryption backdoors debate. Quantum decryption capabilities might worsen this tension, providing Governments access to encrypted data on an unprecedented scale. So the challenge is: How do legal systems evolve to address national security requirements while still upholding the constitutional rights of citizens in a world where quantum decryption is real?

In addition, concerns about the scope and duration of surveillance activities are heightened by the ability of governments to store encrypted data for later decryption (also known as "store now, decrypt later"). Legal frameworks that are clear on the conditions under which such data collection is appropriate and what safeguards are in place to prevent abuse are needed.

Liability for Quantum Vulnerabilities

The transition to post-quantum cryptography (PQC) also raises questions about liability for organizations that fail to adequately protect their data. Can companies be sued for using pre-quantum encryption methods if their data is compromised by quantum attacks? This issue

[29] In re Apple, Inc., No. ED 15-0451M (C.D. Cal. Feb. 16, 2016), https://www.eff.org/document/court-order-compelling-apple-assist-law-enforcement-agents-search.

introduces the potential for negligence claims against organizations that do not take reasonable steps to mitigate quantum risks.

Several factors will likely influence the determination of liability, including:

- **Industry standards:** What constitutes reasonable security practices in the context of quantum threats?
- **Foreseeability:** Was the risk of quantum attacks reasonably foreseeable at the time of the breach?
- **Availability of PQC solutions:** Were PQC solutions readily available and feasible to implement?

The SEC's new cybersecurity rules, effective September 5, 2023, mandate that public companies disclose material cybersecurity incidents and provide periodic disclosures about their processes for assessing, identifying, and managing cybersecurity risks.[30] These rules underscore the importance of proactive cybersecurity risk management and board oversight. Failure to comply with these regulations could expose companies to enforcement actions and potential liability.

Cyber insurance also plays a crucial role in mitigating the financial impact of cyber incidents, covering risks such as data breaches, ransomware attacks, and legal liabilities.[31] As quantum computing advances, organizations will need to assess their cyber insurance policies to ensure they adequately address the emerging risks.

The financial penalties for failing to protect personal data can be substantial. India's Digital Personal Data Protection Act, 2023, prescribes penalties of up to INR 250 crore for failure to take reasonable security safeguards and up to INR 200 crore for failure to notify the relevant authorities and affected parties in the event of a data breach.[32]

[30] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896 (Aug. 4, 2023) (to be codified at 17 C.F.R. pts. 229, 232, 239, 240, and 249).
[31] Tejas Jain, Understanding India's Cybersecurity Compliance Laws: How Can Cyber Insurance Help?, BimaKavach (Jan. 20, 2025), https://www.bimakavach.com/blog/understanding-india-cybersecurity-compliance-laws-and-how-cyber-insurance-helps/.
[32] Digital Personal Data Protection Act, No. 37 of 2023, sec. 8(5)-(6), 2023 Gazette of India, pt. I, sec. 1.

The following table summarizes the potential liabilities and risk mitigation strategies:

Liability	Risk Mitigation Strategies
Negligence claims for data breaches	Implement PQC solutions, conduct regular risk assessments, comply with industry standards and regulations (e.g., SEC/SEBI rules), maintain adequate cyber insurance coverage
Regulatory fines for non-compliance	Adhere to data protection laws (e.g., GDPR, DPDPB), implement robust cybersecurity policies and procedures, provide employee training on data security best practices
Reputational damage	Develop a comprehensive incident response plan, communicate transparently with stakeholders in the event of a breach, invest in reputation management and public relations
Financial losses due to business interruption	Implement business continuity and disaster recovery plans, invest in cyber insurance coverage for business interruption losses

3.3 International Fragmentation

The global landscape of quantum technology is characterized by increasing fragmentation, driven by differing national interests, technological capabilities, and regulatory approaches. This fragmentation poses challenges to international cooperation and hinders the development of harmonized standards and norms.

Export controls on quantum-resistant technologies, often classified as dual-use, further complicate the landscape. Countries like the US and China are implementing export restrictions to protect their national security interests and maintain a competitive edge in quantum technology.[33] However, disagreements on technical details and commercial interests undermine the effectiveness of these controls.

[33] Antonia Hmaidi & Jeroen Groenewegen-Lau, MERICS China Tech Observatory Quantum Report 2024, Mercator Inst. for China Stud. 6 (Dec. 2024), https://merics.org/sites/default/files/2024-12/MERICS%20China%20Tech%20Observatory%20Quantum%20Report%202024.pdf.

The US Department of Commerce added 37 Chinese entities to the Entity List in May 2024, restricting their access to items listed under the Export Administration Regulations (EAR). Twenty-two of these entities were added for their participation in China's quantum technology advancements.[34]

Differing standards between the EU, US, and China also contribute to international fragmentation. China is heavily investing in quantum technology and is using a state-led approach.[35] As of 2022, China's investments totalled $15.3 billion, more than the European Union and the United States combined.[36] This has led to concerns about fair competition and the potential for technological dominance. The US National Quantum Initiative Advisory Committee (NQIAC) urges more investment for the US to maintain leadership across all quantum technologies.[37]

The political objectives for controlling quantum technologies today take on a broader view of national security than those of the past, aiming to maintain the "largest possible lead" in foundational technologies, including quantum, rather than just maintaining a "relative advantage".

Post-quantum cryptography thus represents a legal and regulatory gap with complex, multifaceted implications. Filling these gaps will require proactive work on surveillance law, liability frameworks, and international cooperation. With the evolution of quantum computing, there is a need for legal systems to keep pace with these changes to protect individuals, encourage responsible innovation, and maintain a trusted digital ecosystem. Not doing so would risk privacy, security and economic stability.

Policy Solutions and the Road Ahead

Modern encryption could be broken down by the emergence of quantum computing, which poses a serious risk to information confidentiality, integrity, and authenticity across unsecured networks.[38] Traditional cryptographic algorithms like RSA, AES, and ECC that spent decades

[34] Additions of Entities to the Entity List, 89 Fed. Reg. 41886 (May 14, 2024).
[35] Hmaidi & Groenewegen-Lau, supra note 34.
[36] Hmaidi & Groenewegen-Lau, supra note 34, at 6.
[37] National Quantum Initiative Advisory Committee, Quantum Networking: Findings and Recommendations for Growing American Leadership, Quantum.gov 3 (Sept. 6, 2024), https://www.quantum.gov/wp-content/uploads/2024/09/NQIAC-Report-Quantum-Networking.pdf.
[38] Anand Ramachandran, Future-Proofing Digital Security: Architecting, Designing, and Implementing PQC

as the gold standard are becoming vulnerable to quantum computers that can employ Shor's algorithm to rapidly factor large integers and solve discrete logarithms for ECC.[39] While it may seem a distant prospect, the racing threat calls for pre-emptive action to ready legal systems for the arms race of encryption, most crucially through the deployment of post-quantum cryptography (PQC). This section discusses policy solutions & the way forward, including legislative changes, global governance, and ethical issues.

Legislative Reforms

Legislative reforms are essential in making the transition to PQC in sensitive sectors. One key step is to require PQC in areas critical to national security and economic stability.

- **Mandating PQC in Critical Sectors:** Mandate for PQC in Critical Sectors: Governments can mandate the adoption of PQC in critical infrastructures, financial institutions, healthcare, and other sectors dealing with sensitive data. This mandate shall comply with the National Institute of Standards and Technology (NIST) 2024 standards[40], with algorithms such as CRYSTALS-Kyber for key encapsulation, as well as the CRYSTALS-Dilithium, FALCON, and SPHINCS+ algorithms for digital signatures. In August 2024, for example, NIST released the initial set of formalized Federal Information Processing Standards (FIPS) for post-quantum cryptography: FIPS 203, FIPS 204, and FIPS 205.[41] FIPS 203 defines standards for Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM), prioritizing efficiency, resistance to side-channel attacks, and compatibility with existing public key infrastructure (PKI).[42] FIPS 204 provides guidelines for Module-Lattice-Based Digital Signature Algorithm (ML-DSA), ensuring data authenticity and integrity, mitigating risks of forged digital certificates, and scalability for large-scale deployment. FIPS 205 defines standards for Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), focusing on long-term security and minimal reliance on complex mathematical assumptions, suited for systems requiring long-term data security and applications with strict memory constraints.[43]

(Post-Quantum Cryptography) Systems, LinkedIn (Nov. 26, 2024), https://www.linkedin.com/pulse/future-proofing-digital-security-architecting-pqc-anand-ramachandran-wnpue.

[39] Id.

[40] Id.

[41] NIST, supra note 22.

[42] Ramachandran, supra note 39.

[43] Ramachandran, supra note 39.

- **Safe Harbor Provisions for Early Adopters:** To encourage early adoption of PQC, governments should establish safe harbor provisions that offer legal protection to organizations that proactively implement PQC measures. These provisions would provide an affirmative legal defense against lawsuits following a security incident, protecting from tort claims alleging a lack of reasonable cybersecurity controls. Several states in the U.S. have already implemented cybersecurity safe harbor laws. For example, Ohio's Data Protection Act of 2018 offers an affirmative defense to organizations that implement reasonable information security controls. Similarly, the HIPAA Safe Harbor Act incentivizes the use of cybersecurity standards in the healthcare industry by offering lower fines and shorter audits for covered entities following recognized security practices. Other states, like Connecticut, Iowa, Tennessee and Utah, have also enacted safe harbor laws with varying requirements and protections.[44]
- **Incentives and Subsidies**: Offer tax breaks, grants, or other financial incentives to organizations that invest in PQC infrastructure and training. This can help offset the costs associated with upgrading systems and adopting new cryptographic standards.

Global Governance

The transition to PQC requires international cooperation and the establishment of global standards to ensure seamless and secure communication across borders.

- **Model Laws for PQC Migration:** International organizations such as the International Telecommunication Union (ITU), the United Nations (UN), or the Organisation for Economic Co-operation and Development (OECD) can play a crucial role in developing model laws for PQC migration.[45] These model laws would provide a framework for countries to develop their national legislation, ensuring consistency and interoperability across different legal systems. International Telecommunications Union's Technical Report provides an overview of standardization activities on hybrid approaches for migration towards quantum-safe algorithms or protocols.[46] The

[44]Joe Köller, US Cybersecurity Safe Harbor Laws by State: All Current Legislation, Tenfold Security (Dec. 20, 2023), https://www.tenfold-security.com/en/cybersecurity-safe-harbor-laws/.
[45] Commission Recommendation (EU) 2024/2393 of 11 April 2024 on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, 2024 O.J. (C 2393) 1, https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography.
[46] International Telecommunication Union, XSTR-HYB-QKD: Overview of Hybrid Approaches for Key Exchange with Quantum Key Distribution, ITU-T Technical Report (May 20, 2022),

European Commission recommends Member States develop a comprehensive strategy for adopting PQC, defining clear goals, milestones, and timelines, resulting in a joint PQC Implementation Roadmap.[47]

- **Treaties Restricting Quantum Cyberattacks:** Given the potential for quantum computers to be used for malicious purposes, there is a need for international treaties that restrict quantum cyberattacks. These treaties could be modeled after existing agreements such as the Chemical Weapons Convention (CWC) and the Nuclear Non-Proliferation Treaty (NPT).[48] The Tallinn Manual 2.0, which provides an analysis of how international law applies to cyber operations, can serve as a foundation for developing these treaties.[49] The treaties should also address the challenges of defining "cyberattack" and attributing attacks, as highlighted in the Harvard National Security Journal article.[50]
- **International Standards and Certifications**: Promote the development and adoption of international standards for PQC algorithms and implementations. Encourage the establishment of certification programs to ensure that PQC products and services meet these standards. NIST's Cryptographic Module Validation Program (CMVP) is an example of such a certification program.[51]

Ethical and Equity Concerns

The implementation of PQC raises ethical and equity concerns that must be addressed to ensure a fair and inclusive transition.

- **Digital Divide:** One of the primary concerns is whether PQC will widen the digital divide. The cost and complexity of implementing PQC may disproportionately affect smaller organizations and developing countries, leaving them vulnerable to

https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2022-1-PDF-E.pdf.
[47] EU, supra note 46.
[48] Dominic Rota, A Quantum Leap in International Law on Cyberwarfare: An Analysis of International Cooperation with Quantum Computing on the Horizon, Harv. Nat'l Sec. J. (Nov. 8, 2018), https://harvardnsj.org/2018/11/08/a-quantum-leap-in-international-law-on-cyberwarfare-an-analysis-on-the-need-for-international-cooperation-with-quantum-computing-on-the-horizon/.
[49] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael N. Schmitt ed., Cambridge Univ. Press 2017), https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N._Schmitt_-_Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press__2017_.pdf.
[50] Id.
[51] GSM Association, Post Quantum Cryptography – Guidelines for Telecom Use Cases, Version 2.0 (Oct. 4, 2024), https://www.gsma.com/newsroom/wp-content/uploads/PQ.03-Post-Quantum-Cryptography-Guidelines-for-Telecom-Use-Cases-v2.0-2.pdf.

cyberattacks. To mitigate this risk, governments and international organizations should provide resources and support to help these entities adopt PQC.[52]

- **Open-Source vs. Proprietary PQC Solutions:** This consideration stems from the fact that the type of encryption we will be using after future quantum computers come useful against traditional encryption will be either open-source or proprietary PQC solutions. Open-source solutions encourage transparency and collaboration but might not have the resources to provide continuous maintenance and support. While proprietary solutions tend to provide better support and security, they come at a higher cost and lack transparency. The overarching need is to establish a balanced framework that incentivizes both open-source and proprietary innovation in PQC development, leading to a well-rounded and diverse ecosystem.[53]
- **Data Ownership and Control**: Because of its highly powerful processing capabilities, quantum computing raises questions of data ownership and control associated with the copious amounts of personal data. Governments are growing more and more concerned with the effects of quantum computing on national security, economic competitiveness, and society and are developing policies geared towards regulating its development and deployment. This requires the implementation of laws that will protect the personal information of the user against quantum computers.
- **Environmental Impact**: Address the environmental impacts of PQC implementations with energy-efficient architectures and lifecycle management. Encourage sustainability in the development and deployment of PQC technologies.

The transition to post-quantum cryptography is a complex and multifaceted challenge that requires proactive policy solutions and international cooperation. By mandating PQC in critical sectors, establishing safe harbor provisions for early adopters, developing model laws for PQC migration, and addressing ethical and equity concerns, legal systems can be effectively prepared for the encryption arms race. The road ahead requires a collaborative effort between governments, industry, academia, and international organizations to ensure a secure, equitable, and sustainable transition to a post-quantum world.

[52] Quantum News, The Ethics of Quantum Computing: Considerations and Challenges, Quantum Zeitgeist (Sept. 14, 2024), https://quantumzeitgeist.com/the-ethics-of-quantum-computing-considerations-and-challenges/.
[53] Id.

Conclusion

The advent of quantum computing heralds a transformative era in technology, but it also poses unprecedented challenges to the legal and cryptographic frameworks that underpin modern data security. As this research has demonstrated, the ability of quantum computers to break widely used encryption algorithms—such as RSA, ECC, and AES—threatens the confidentiality, integrity, and authenticity of sensitive information across sectors, from healthcare and finance to national security and digital contracts. The implications for privacy laws, contractual agreements, and surveillance frameworks are profound, necessitating urgent and coordinated action from policymakers, legal scholars, and technologists.

Key Findings and Implications

1. **Vulnerability of Current Encryption**: Quantum algorithms like, Shor's and Grover's, can break down classical cryptographic systems, undermining the security assumptions on which laws such as HIPAA, GDPR, and eIDAS are based. This vulnerability has repercussions on blockchain technologies, digital signatures, and classified communications, creating cascading effects on trust and compliance.
2. **Legal and Regulatory Gaps**: Current legal frameworks are insufficient to mitigate quantum decryption threats. These systems have not included provisions on how to mitigate "harvest now, decrypt later" attacks, or how to define accountability for quantum-era breaches, including surveillance laws, liability standards, and international regulations. This building of walls between jurisdictions creates greater challenges in developing unified approaches to common problems.
3. **Policy Solutions**: To achieve this secure transition, we must be proactive too, through legislation (e.g., mandating the PQC wherever possible, providing safe harbor provisions), the establishment of global governance (e.g., model laws, treaties), and ethical considerations (e.g., bridging the digital divide) NISTs PQC standards (FIPS 203–205) are an initiatory map, but their deployment requires execution and international uniformity.

The Path Forward

Direct quantum danger isn't something hypothetical in the future; it's an imminent reality. To ready legal systems for this paradigm shift requires:

Partnerships: Governments, industry, and academia working together across sectors to speed

up the adoption of PQC and reach consensus around standards.

Education: Educating legal practitioners and firms on quantum risks and their mitigation.

Innovation: Maintaining immunization and the development of quantum-resistant, open-source, and sustainable solutions.

In conclusion, The quantum era encryption arms race is a clarion call. Through grounding the transition in legal stability, driving international collaboration, and promoting ethical equity, society can forge a stronger future throughout this demanding evolution. It's now or never, Before quantum advances outstrip our preparedness and expose critical systems in a post-quantum world.