EMERGING POLICY QUESTIONS **FOR QUANTUM ENCRYPTION**

BY DAVID W. OPDERBECK

Professor of Law and Co-Director, Gibbons Institute of Law, Science & Technology and Institute for Privacy Protection, Seton Hall University Law School.

Visit www.competitionpolicyinternational.com for access to these articles and more!

EMERGING POLICY QUESTIONS FOR QUANTUM ENCRYPTION

By David W. Opderbeck

In the not-too-distant future, quantum computing could render today's widely used classical encryption schemes obsolete. Policymakers are already considering how to move public and private infrastructure towards quantum encryption standards that will prove robust in the quantum computing environment. At the same time, security and law enforcement agencies also are strategizing for a future in which large volumes of encrypted information currently inaccessible to them might be opened with quantum computing tools. These coming developments present challenges for cybersecurity policy and civil liberties. This paper surveys those challenges and suggests some questions for further study.

01

THE NEW WORLD OF QUANTUM COMPUTING AND QUANTUM ENCRYPTION

Quantum computing, including quantum encryption and decryption, presents great opportunities for industry and civil society as well as great challenges for national security, law enforcement, and civil liberties. Classical computing uses bits that can hold a value of 0 or 1, corresponding to states of "on" or "off" in a circuit. Quantum computing uses "qubits," which can exist in states of 0 and 1 simultaneously because of the quantum effect of superposition.[2] This allows quantum computers to perform certain computations far more quickly and efficiently than classical computers. Quantum sensors leverage the processing power of quantum computers along with the quantum effect of entanglement, creating highly sensitive sensors effective over potentially vast distances.[3]

02

PREPARING GOVERNMENT FOR QUANTUM ENCRYPTION

Classical encryption algorithms are essentially enormous math problems. The cryptographic key is the solution to the problem. For example, for the RSA 2048 standard, which is used for many of the messages that traverse the Internet, it would take a classical computer trillions of years to solve the cryptographic math problem by brute force. Although researchers are still debating whether quantum computers of feasible scale and cost could crack common standards such as RSA 2048 or AES 129, 192, or 256, some predict that commonly used classical encryption schemes will be broken by quantum computers within twenty years.[4]

The prospect that quantum computers might crack standard cryptography could be a motive behind some current cybersecurity incidents involving parties connected to state actors such as China, Russia, and North Korea. National security officials worry that state actors are warehousing exfiltrated encrypted data for future quantum decryption – "harvest now, decrypt later" attacks.[5] According to a U.S. National Security Memorandum issued in 2022, "a quantum computer of sufficient size and sophistication . . . could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions."[6]

The U.S. has taken initial steps to address these threats with the Quantum Computing Cybersecurity Preparedness Act of 2022 ("QCCPA").[7] The statue requires federal agen-

2 See Europol, *The Second Quantum Revolution: The Impact of Quantum Computing and Quantum Technologies on Law Enforcement* (2023), available at https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Observatory_Report%20-%20The%20Second%20Quantum%20Revolution.pdf. "Superposition" refers to the fact that a quantum system exists in multiple states at the same time until it is measured. Schrödinger's Cat is a famous thought experiment about superposition. *See* Caltech Science Exchange, *What is Superposition and Why is it Important?*, available at https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-superposition.

3 See Charles Q. Choi, *Entangling Quantum Sensors Can Triple Accuracy: "Spooky sensing at a distance" via One Combined Device*, IEEE Spectrum, Dec. 9, 2022, available at https://spectrum.ieee.org/quantum-sensors-entanglement. "Entanglement" refers to the fact that at the quantum scale particles separated by vast distances can be "entangled" such that the observed state of one particle correlates with the observed state of the entangled particle. See Caltech Science Exchange, *What is Entanglement and Why is it Important*, available at https://scienceexchange.caltech.edu/topics/quantum-science-explained/entanglement.

4 Lily Chen, *et al.*, *Report on Post-Quantum Cryptography*, NISTIR 8105, April 2016, at 2, available at https://www.techopedia.com/definition/29703/256-bit-encryption#:~:text=256%2Dbit%20encryption%20is%20refers,by%20even%20the%20fastest%20computers; Michael D. Vermer & Evan D. Peet, *Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption*, Rand Corporation (2020), available at https://www.rand.org/pubs/research_reports/RR3102.html.

5 Jeffrey Duran, *Harvest Now, Decrypt Later? The Truth Behind this Quantum Theory*, The Quantum Insider, Feb. 7, 2023, available at https://thequantuminsider.com/2023/02/07/guest-post-harvest-now-decrypt-later-the-truth-behind-this-common-quantum-theory/.

6 *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*, NSM-10, May 4, 2022, available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

7 Public Law 117-260, 117th Congress, Dec. 21, 2022, codified at 6 U.S.C. § 1500 note and 1526 note.

cies to inventory data that might be vulnerable to attack by quantum computers and to establish plans for migration of that data to post-quantum cryptography.[8] The U.S. National Institute of Standards and Technology ("NIST") has initiated a process to identify post-quantum cryptography algorithms, meaning algorithms that are resistant both to classical and quantum encryption.[9]

Nothing in the QCCPA relates to private industry or privately-owned critical infrastructure. It is likely that cybersecurity requirements applicable to private entities under various federal laws will need to be updated to account for the costs and benefits of post-quantum cryptography.[10]

03

LAW ENFORCEMENT: QUANTUM ENCRYPTION, QUANTUM SENSORS, AND PRIVACY

Law enforcement organizations recognize that quantum encryption will present both challenges and opportunities. One challenge mirrors that involving national security: the harvesting and stockpiling of classically encrypted data for later decryption by quantum means. Under U.S and EU law, any access to a protected computer without authorization or in excess of authorization is a crime, even if the accused obtains only encrypted data with unreadable ciphertext, or indeed even if the accused exfiltrates nothing at all.[11] Quantum computing does not present unique challenges for this aspect of computer crimes law, beyond existing problems with interpreting the statutes access provisions, which were first created in an era before the public Internet existed.[12]

A second major challenge is also familiar: user-generated encryption serves vital functions for commerce, personal security, and civil society, but it also enables criminals to "go dark."[13] Quantum computing may weaken security if it proves able to decrypt historical data protected by classical encryption, but it may also enhance security looking forward because it will facilitate a next generation of quantum encryption algorithms that even quantum computers cannot crack. Readily accessible user-generated quantum encryption is probably much further off than the threat of a nation state or large organized criminal actor gaining access to quantum decryption tools for classical encryption because quantum computing platforms are difficult to construct and maintain.[14]

Law enforcement authorities have advocated for encryption "back door" requirements since the clipper chip in the early 1990's – proposals that rightly were resisted in the past, and that should continue to be resisted, as to data in transit.[15] For data at rest, third party storage services that secure user data with encryption already routinely supply plaintext copies to law enforcement in response to lawful process, while courts grapple with whether an individual who has encrypted files on a personal computer or device can be compelled to disclose a decryption key or password.[16] The migration from classical to quantum encryption should not materially change these policy debates. Authoritarian governments, meanwhile, no doubt will continue to require key escrows or use other means to circumvent encryption for data in motion and at rest, including quantum encryption.[17]

8 *Id*., § 4.

9 NIST Post-Quantum Cryptography Standardization page, available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

10 For a discussion of some existing security rules, see David W. Opderbeck, *Cybersecurity and Data Breach Harms: Theory and Reality*, 82 Md. L. Rev. 1001 (2023), Part III.B.

11 U.S. Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.

12 See *Van Buren v. United States,* 141 S. Ct. 1648 (2021).

13 See David W. Opderbeck, *Encryption Policy and Law Enforcement in the Cloud*, 49 Conn. L. Rev. 1657 (2017).

14 Matt Swayne, *What are the Remaining Challenges of Quantum Computing*, The Quantum Insider, March 24, 2023, available at https://thequantuminsider.com/2023/03/24/quantum-computing-challenges/#:~:text=Quantum%20computers%20are%20extremely%20sensitive,degrade%20the%20quality%20of%20computation.

15 See *id.*

16 See David W. Opderbeck, *The Skeleton in the Hard Drive: Encryption and the Fifth Amendment*, 70 Fla. L. Rev. 883 (2018).

17 Valentin Weber & Joss Wright, *(Quantum) Encryption: Europeans Need to Come Down in Favor*, German Council on Foreign Relations, June 20, 2023, available at https://dgap.org/en/research/publications/quantum-encryption-europeans-need-come-down-favor.

Law enforcement thought leaders also see potential opportunities with quantum computing, all of which raise challenging questions for civil liberties. One intriguing possibility is the use of quantum computers to decrypt evidence protected by classical encryption in cold cases.[18] An individual no doubt has a reasonable expectation of privacy in data they have encrypted with classical encryption. If the government has seized evidence, such as computer hard drives, pursuant to a search warrant, then probable cause existed for the government to review the data if it was available in plaintext. Presumably the government would not need to obtain an additional warrant to use quantum computing techniques on historical classically encrypted data that had been lawfully seized, but perhaps additional process should be required.

This question is somewhat analogous to the use of contemporary DNA techniques on archived cold case evidence.[19] Some privacy advocates have been alarmed at warrants that require providers of commercial genealogy services such as GEDmatch and 23 and Me to turn over information to law enforcement authorities working on live or cold cases.[20] Other privacy advocates are investigating law enforcement access to genetic data collected from newborn infants for genetic disease screening purposes.[21] But many of these DNA cases involve third parties who collected their customers' DNA under contractual or legal obligations of privacy before large scale genomic databases existed. The privacy issue is not so much that the DNA can be "read" as that the government has ready access to enormous privately curated genomic databases for comparisons. In contrast, the ability to crack conventional encryption employed on collected cold case data files with a new technology seems like less of a general mass surveillance tool. Nevertheless, the notion that the government might stockpile presently uncrackable evidence to be examined when quantum decryption tools become available seems problematic.

An even more challenging question from a civil liberties perspective is the possibility of quantum decryption of data in motion.[22] Quantum computing could render classical end-to-end encryption techniques obsolete, giving law enforcement a window onto communications that are now opaque. This would break all current versions of Internet security, including the security protocols used for ecommerce, as well as secure messaging apps. The U.S. Justice Department has argued for many years that the "going dark" problem requires some form of decryption backdoor, which quantum computing may provide unless secure quantum encryption protocols are developed.[23]

> ***An even more challenging question from a civil liberties perspective is the possibility of quantum decryption of data in motion***

Quantum computing may also provide new avenues for fault injection attacks, which could be used by law enforcement to corrupt or disable systems used by cybercriminals, including those used to distribute child sexual abuse material ("CSAM").[24] Law enforcement already uses malware to surveil and disrupt allegedly criminal enterprises, such as botnets and CSAM servers.[25] The Federal Rules of Criminal Procedure were amended in 2016 to al-

18 Europol, *The Second Quantum Revolution*, at 18.

19 See Sarah H. Katsanis, *Pedigrees and Perpetrators: Uses of DNA and Genealogy in Forensic Investigation*, 21 Annual Review of Genomics and Human Genetics 535 (2020), available at https://www.annualreviews.org/doi/10.1146/annurev-genom-111819-084213; U.S. Department of Justice, Using DNA to Solve Cold Cases, NCJ 194197, July 2002, available at https://www.ojp.gov/pdffiles1/nij/194197.pdf; Jordan Smith, Police are Getting DNA Data From People Who Think They Opted Out, The Intercept, August 18, 2023, available at https://theintercept.com/2023/08/18/gedmatch-dna-police-forensic-genetic-genealogy/.

20 See Kashmir Hill & Heather Murphy, "Your DNA Profile is Private? A Florida Judge Just Said Otherwise," New York Times, Nov. 5, 2019, available at https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html.

21 See Crystal Grant, "Police Are Using Newborn Genetic Screening to Search for Suspects, Threatening Privacy and Public Health," ACLU News and Commentary, July 26, 2022, available at https://www.aclu.org/news/privacy-technology/police-are-using-newborn-genetic-screening.

22 Europol, *The Second Quantum Revolution*, at 17.

23 See Opderbeck, *Encryption Policy and Law Enforcement in the Cloud, supra* note 3; NIST Post-Quantum Encryption Standardization Page, *supra* note 9.

24 *Id.* at 23.

25 See *FBI, Partners Dismantle Qakbot Infrastructure in Multinational Cyber Takedown*, Aug. 29, 2023, available at https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown; *Justice Department Announces Court-Authorized Disruption of the Snake Malware Network Controlled by Russia's Federal Security Service*, May 9, 2023, available at https://www.justice.gov/usao-edny/pr/justice-department-announces-court-authorized-disruption-snake-malware-network; *'Playpen' Creator Sentenced to 30 Years*, May 5, 2017, available at https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years.

low Magistrate Judges to issue warrants for remote access tools ("RATs").[26]

RATs are essentially malware tools that allow authorities to surveil, control, and disable affected computers. A local Magistrate can issue a RAT warrant for out-of-district computers if "(A) the district where the media or information is located has been concealed through technological means; or … (B) in an investigation of a violation of [a section of the Computer Fraud and Abuse Act] the media are protected computers that have been damaged without authorization and are located in five or more districts."[27]

RAT warrants thereby greatly expand the geographic scope of any individual Magistrate's power to issue warrants, which ordinarily must be restricted to persons or property within the Magistrate's district or that are within the district but might move outside the district before the warrant is issued.[28] These are historically important restrictions, rooted in concepts of jurisdiction meant to facilitate local accountability over judicial power. This controversial amendment recognizes that information readily travels and is stored across district borders in the cloud computing era. The property of quantum entanglement demonstrates that, when information is the commodity in question, geographical boundaries are even less meaningful than imagined. With the advent of quantum computing, it might become impossible to specify "where" a piece of information is located, pushing the territorial limitations on search warrants beyond the breaking point.

Quantum computing and the property of quantum entanglement will also produce advanced quantum sensors, which are already in development.[29] Quantum sensors will be smaller and more precise than classical sensors and will be able to communicate over vast distances, with very little light, across densely populated areas, and regardless of solid barriers.[30] Combined with breakthroughs in artificial intelligence, quantum surveillance may inch the world closer to the world of Philip K. Dick's *Minority Report*, in which police can predict crimes before they occur.[31] In the *Carpenter* case, the Supreme Court limited the third party doctrine and held that a person has a reasonable expectation of privacy in cell site location data collected by telecommunications providers.[32] The *Carpenter* Court's effort to square the Fourth Amendment with contemporary cell phone technology likely will appear quaint over the coming decades.

04
CONCLUSION

The quantum computing revolution could prove as disruptive as the Internet and AI revolutions. In fact, quantum computing could dissolve the Internet's existing security protocols and supercharge AI's predictive and surveillance capabilities. The United States has taken some initial steps to prepare for quantum cryptography. Industry leaders likewise should begin preparing plans for a world in which classical encryption is no longer sufficient. Lawmakers and lawyers should also begin thinking about how the potential for quantum technologies in law enforcement should be balanced against civil liberties concerns, both within the U.S. and internationally. ■

"Quantum computing and the property of quantum entanglement will also produce advanced quantum sensors, which are already in development

26 F.R. Crim. Pro. 41(b)(6).

27 *Id.*

28 F. R. Crim. Pro. 41(b)(1)-(2). Out of district warrants can also be issued in terrorism cases, for tracking devices, and for searches and seizures in certain locations not subject to the jurisdiction of any state or district. F. R. Crim. Pro. 41(b)(3)-(5).

29 Europol, *The Second Quantum Revolution*, at 44.

30 Allison Snyder, "Quantum Sensing Readies to be the 21st Century's Surveillance Leap," Axios, February 16, 2023, available at https://www.axios.com/2023/02/16/quantum-sensing-military.

31 See Philip K. Dick, *The Minority Report and Other Classic Stories* (Citadel Reprint Ed. 2016); Jonathan Reichental, "Quantum Artificial Intelligence is Closer Than You Think," Forbes, November 20, 2023, available at https://www.forbes.com/sites/jonathanreichental/2023/11/20/quantum-artificial-intelligence-is-closer-than-you-think/?sh=36ce453c4818.

32 *Carpenter v. United States*, 138 S.Ct. 2206 (2018).

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL