Washington and Lee Law Review

Volume 79 | Issue 1 Article 11

Winter 2022

Data Breach Notification Laws and the Quantum Decryption Problem

Phillip Harmon
Washington and Lee University School of Law, harmon.p22@law.wlu.edu

Data Breach Notification Laws and the Quantum Decryption Problem

Phillip Harmon*

Abstract

In the United States, state data breach notification laws protect citizens by forcing businesses to notify those citizens when their personal information has been compromised. These laws almost universally include an exception for encrypted personal data. Modern encryption methods make encrypted data largely useless, and the notification laws aim to encourage good encryption practices.

This Note challenges the wisdom of laws that place blind faith in the continued infallibility of encryption. For decades, Shor's algorithm has promised polynomial-time factoring once a sufficiently powerful quantum computer can be built. Competing laboratories around the world steadily continue to march toward this end. Once quantum computers become strong enough, classical encryption will no longer remain secure.

Ramifications of quantum decryption would reverberate through all aspects of security and society. This Note focuses only on the interplay of this development with data breach notification laws. While these laws cannot prevent technological progress, a federal data breach notification law could encourage adoption of a quantum-secure classical encryption method. This

* J.D. Candidate, Washington and Lee University School of Law; B.A. Washington and Lee University. The author is grateful to Alexandra Clark, T.J. Benedict, and Mitch McCloy for their comments on early drafts. Special thanks to Joshua Fairfield, for his guidance and mentorship, and to Cooper Baird, for his insights on the nuances of quantum algorithms and all things relating to computer engineering. This article would not have been completed without support and feedback from Ellie Bradach and MacKenzye Leroy.

would dampen the harm quantum decryption causes by limiting the relevance of newly useful encrypted data.

Table of Contents

INTRODUCTION

Oh, the horrors of calculus! At some point, nearly everyone has struggled to get through a tough math class. Many people are not wired for numbers, and even a gold-star mathematician will eventually come to a problem that she cannot immediately comprehend. The frustration inherent in grappling with a hard math problem is nearly universal. But challenging problems are not all bad. Some calculations are so difficult that even

computers cannot readily solve them.[1] Practical uses of those problems can result. Indeed, complex math problems form the backbone of encryption, a huge facilitator for modern human interaction.[2]

What happens when a technological breakthrough makes a near impossible problem suddenly straightforward to solve? Rapidly approaching innovations in quantum technology promise a quick solution to the classically difficult math problems underlying encryption.[3] Unfortunately, our society is built around, and our laws implicitly assume, the continued infallibility of those hard problems.

This Note focuses on data breach notification laws, which require data holders to tell people if someone has stolen data containing their private personal information. To start, Part I will introduce encryption and explain how difficult math problems have been manipulated to secretly convey information. Part II will closely examine existing data breach notification laws. Particular attention will be given to the ways in which various jurisdictions address encryption. Most do not require any alert in instances in which encrypted data was taken, because the encrypted data is assumed to be unusable.[4] Part III of this Note will examine the development of quantum technologies and how Shor's algorithm will render current encryption methods insecure. Existing data breach notification laws will be revisited in Part IV to see if they could continue to properly function as that development approaches. Finally, Part V will propose a new data breach notification framework that

1. *See* David Grossman, *After 65 Years, Supercomputers Finally Solve this Unsolvable Math Problem*, POPULAR MECHS. (Sept. 9, 2019), https://perma.cc/XL3U-K9V3 (detailing how supercomputers needed over a million hours of computing power to solve the Diophantine equation for the integer forty-two).

2. *See Encryption 101: What It Is, How It Works, and Why We Need It*, TREND MICRO (July 24, 2015), https://perma.cc/TPP9-CKR9 (noting that the mathematical algorithms underlying encryption provide security in "activities we can no longer live without").

3. *See infra* Part III.

4. *See* Mark Burdon et al., *Encryption Safe Harbours and Data Breach Notification Laws*, 26 COMPUT. L. & SEC. REV. 520, 528 (2010) (asserting that, in United States data breach notification laws, "encryption equates to security").

would better protect personal data as the quantum-decrypting horizon approaches.

I. IDENTITY THEFT AND ENCRYPTION

Over the past few decades, the internet has enormously impacted how society functions.[5] Most people can quickly list numerous ways that they use it on a daily basis: online shopping is commonplace;[6] banks allow us to manage our money remotely;[7] and social media platforms let us connect and interact with friends around the world.[8] With increased reliance on the internet for these services, private information has become widely digitalized.[9] Every online interaction conveys some information—be it a name, an address, or a credit-card number—that might be saved or otherwise used to create a record.[10] If compiled, this information could harm individuals by

5. *See* Marianna Diomidous et al., *Social and Psychological Effects of the Internet Use*, 24 ACTA INFORMATICA MEDICA 66, 66 (2016) (crediting computers and the internet with bringing about a "revolution in human daily life").

6. *See* Claire Hansen, *Consumers Continue a March Toward Online Shopping*, U.S. NEWS & WORLD REP. (Oct. 16, 2020, 5:05 PM), https://perma.cc/E8XW-NSSP (reporting that online retail sales constituted 16.1 percent of total sales during the second quarter of 2020 and that three-quarters of shoppers intend to do some online shopping for the holidays); Matt Rosoff, *Amazon Will Be the Most Important Company of the 2020s*, CNBC (Dec. 13, 2019, 8:59 AM), https://perma.cc/5X7B-KXUC (detailing how Amazon, the largest online retailer in the United States, increased its e-commerce revenues by sevenfold in the 2010s).

7. *See Manage My Bank Account*, USAA, https://perma.cc/5RLU-BCBV (providing options for wire transfers, depositing checks by taking pictures of them, and transferring money between bank accounts, all online); *Sign-In*, BANK OF AM., https://perma.cc/JH52-82AG (offering online management of finances and bank accounts).

8. *See About Meta*, META, https://perma.cc/C5WH-ALF6 ("At Meta, we are constantly . . . working together to connect people all over the world."); *About Instagram*, INSTAGRAM, https://perma.cc/8GS5-SR77 ("We bring you closer to the people and things you love.").

9. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198 (1998) ("[W]e increasingly speak, listen, and act through cyberspace. And such activity generates records, dutifully recorded, sorted, saved, and exchanged by computers.").

10. *Id.*

painting a full picture of their lives with sufficient information to imitate them in a digital context.[11]

The proliferation of digital commerce has resulted in widespread fraud, theft of private information, and identity theft.[12] A few examples of large data breaches illustrate the magnitude of this problem. In 2018, hackers compromised the personal information of 147 million consumers held in a database owned by Equifax, a credit reporting company.[13] In 2014, the discovery of a computer programming error known as the "Heartbleed Bug" incited widespread fear because the bug rendered passwords and private information from an estimated half-million websites insecure.[14] In a 2013 breach of Adobe, hackers stole credit-card numbers from roughly three million customers along with the login information of thirty-eight million users.[15] Incidents like these have occurred repeatedly throughout the past couple of decades.[16] This begs the question: what prevents nefarious actors from stealing information and money every time someone engages in a personal transaction online?

The answer is encryption. Cryptography is the process of scrambling messages so that only desired parties can unscramble and discern their meanings by using secret keys.[17]

---

11. *See id*. at 1199 (discussing how data generated from cyber activity can strip a person of his privacy when compiled into a detailed profile).

12. *See* S. REP. NO. 111-290, at 3–4 (2010) (expressing concern and detailing the dangers of fraud and identity theft associated with data breaches); *We Are Privacy Rights Clearinghouse*, PRIV. RTS. CLEARINGHOUSE, https://perma.cc/P2TQ-A76J (reporting over 11.7 billion breached records since 2005).

13. Tara Siegel Bernard, *Equifax Breach Affected 147 Million, But Most Sit Out Settlement*, N.Y. TIMES (Jan. 22, 2020), https://perma.cc/GES7-GWXQ.

14. *See* Jane Wakefield, *Heartbleed Bug: What You Need to Know*, BBC NEWS (Apr. 10, 2014), https://perma.cc/4AN2-VGJ5 (reporting on the Heartbleed bug and its dangers); *The Heartbleed Bug*, HEARTBLEED, https://perma.cc/TDG5-572S (providing detailed information about the bug and how it could be fixed for domain owners amid the Heartbleed crisis).

15. *See* Brian Krebs, *Adobe Breach Impacted at Least 38 Million Users*, KREBS ON SEC. (Oct. 29, 2013), https://perma.cc/RF82-HLAE.

16. *See* Michael Hill & Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (July 16, 2021, 2:00 AM), https://perma.cc/ZS5M-WLYA (recounting results and damages of multiple enormous data breaches).

17. *See* LYNN MARGARET BATTEN, PUBLIC KEY CRYPTOGRAPHY 2 (2013) (defining cryptography).

There are two categories of encryption schemes—symmetric encryption and asymmetric encryption (also known as private-key encryption and public-key encryption, respectively).[18] Symmetric encryption relies on two parties using one key, which only they know, to scramble their messages.[19] Visualize this form of encryption as two friends mailing each other secret messages by mail inside of a locked box, where each of the two friends owns one of the only two keys to the box.[20] Unfortunately, private-key encryption is only secure to the extent that the key is kept and distributed secretly.[21] It would seem that the best way to safely establish the private key is to pick one together in person, an impossibility when private communication with a new person is urgent or there are large geographical divides.[22]

Public-key encryption solves the key-distribution problem.[23] Under a public-key protocol, there are two keys. The first key, accessible to the world, can be used to encrypt information but cannot decrypt a message once it has been scrambled.[24] The second key can decrypt the data but is closely held by its owner to ensure security.[25] Here, imagine someone

18. *See* Dustin Taylor Vandenberg, Note, *Encryption Served Three Ways: Disruptiveness as the Key to Exceptional Access*, 32 BERKELEY TECH. L.J. 531, 532–34 (2017) (drawing distinctions between these two encryption methods).

19. *See* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 426 (2012) (explaining how private-key encryption works).

20. *See* Zainul Franciscus, *What Is Encryption, and How Does It Work?*, HOW-TO GEEK, https://perma.cc/XPN2-VW4V (archived Dec. 12, 2020) (providing the above metaphor as an illustration of symmetric encryption between Alice and Bob, the two traditional named parties in cryptography).

21. *See* Swire & Ahmad, *supra* note 19, at 426 ("The critical element in this approach is to generate and share the key securely.").

22. *See* BATTEN, *supra* note 17, at 3 (highlighting the impracticability of symmetric encryption and how it historically created trouble during war).

23. *See* Swire & Ahmad, *supra* note 19, at 428 ("[T]he public key approach directly addresses the most glaring weakness of the private-key approach. It allows people to send messages to each other without first having to securely share a secret key.").

24. *See id.* at 427 (explaining the functions of keys in a public-key encryption method).

25. *Id.*

sending their friend a padlock in the mail.[26] The recipient then writes a message, locks it in a box with the padlock, and returns the box to the padlock sender.[27] If the padlock only has one key and the box comes back locked, the original party will know that no one has read the letter in the box.[28] Typically in online interactions, asymmetric encryption is only used to establish a shared private key because symmetric encryption has an advantage in computational efficiency, and hence speed.[29] Together, public-key and private-key encryption allow for the security and secrecy necessary to make electronic commerce possible.[30]

Without exploring the intricacies of the underlying mathematics,[31] it is important to note that asymmetric key encryption hinges on two mathematical challenges: factoring and the discrete logarithm problem.[32] Consider this: if asked to factor the number 21,534,283, most people would throw their hands up in defeat after trying and failing to divide the number by small, readily-recognized primes such as two, three, five, and seven. However, most could multiply the prime numbers 881 and 24,443 relatively easily (with the help of a calculator) and would find an answer of 21,534,283. As the size of inputs increases, the computational difficulty of factoring is believed to

---

26. *See* Franciscus, *supra* note 20 (suggesting this metaphor for an asymmetric key encryption protocol between Alice and Bob).

27. *Id.*

28. *Id.*

29. *See* BATTEN, *supra* note 17, at 6 ("All known public key schemes are far more computationally intensive than symmetric key schemes. . . . For this reason, public key schemes are traditionally used only for small messages such as secret keys, whereas symmetric key schemes are retained for sending large messages.").

30. *See* Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 718–25 (1995) (providing multiple examples of ways in which encryption is critical to the success of electronic commerce, including the use of digital signatures).

31. *See generally* R.L. Rivest et al., *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, 26 COMMC'NS ACM 96 (1978) (detailing the mathematical basis for a public-key encryption system with rigor).

32. *See* ELEANOR RIEFFEL & WOLFGANG POLAK, QUANTUM COMPUTING: A GENTLE INTRODUCTION 172 (William Gropp & Ewing Lusk eds., 2011) ("In fact, all standard public key encryption systems and digital signature schemes are based on either factoring or the discrete logarithm problem.").

be greater than that of multiplication.[33] In fact, when numbers grow very large there is no known way to reliably factor quickly with a computer.[34] That is not to say that decrypting material encrypted with public-key encryption is impossible without access to the private key.[35] Rather, the massive number of possible keys renders it highly improbable that educated or even lucky guessing would thwart security of the information in any meaningful amount of time.[36]

The discrete logarithm problem is much more difficult to illustrate, but functions similarly to factoring in that it becomes increasingly difficult with large inputs.[37] Security of online transactions depends on the well-founded notion that mathematicians might never discover an efficient method for computers to solve these problems.[38]

Still, a reasonable person might retain some hesitancy about the safety of communicating information over the internet. Why should we assume that companies are doing their due diligence by encrypting all communications? How would we

---

33. *See* William L. Hosch, *P Versus NP Problem*, ENCYC. BRITANNICA (Aug. 11, 2009), https://perma.cc/WU8Y-APZ9 (last updated Jan. 9, 2020) (identifying multiplication as an example of a relatively easy problem but noting that factoring is an extremely difficult problem). A problem of polynomial time ("P") difficulty can be solved by an algorithm with steps bounded by a polynomial. *Id.* While multiplication is a P problem, no such algorithms are known for factoring or solving the discrete logarithm problem with a computer. *Id.* It follows that there is currently no guaranteed method of decrypting messages that were scrambled using public-key encryption with a computer in any reasonable amount of time. *Id.*

34. *See Computer Scientists Set New Record for Cryptographic Challenge*, U.C. SAN DIEGO (Apr. 21, 2020), https://perma.cc/44JS-PJTB (reporting that a team of six researchers spanning multiple continents finally solved a challenge, issued to the world in 1991, to factor a specified 250-digit number).

35. *See* Swire & Ahmad, *supra* note 19, at 429 (emphasizing that all forms of encryption are subject to attack and not completely invulnerable).

36. *See id.* at 430 (pointing out that longer keys mathematically increase resistance to brute force attacks); Andrew Braun, *How Secure Is Your Stolen Encrypted Data?*, MAKETECHEASIER (Mar. 26, 2019), https://perma.cc/SAT5-ZY6S (estimating that using brute computational force to attack AES-256 encryption would currently take up to three sexdecillion years, a very long time).

37. *See supra* note 33 and accompanying text.

38. *See* Hosch, *supra* note 33 ("The discovery of an efficient algorithm for factoring large numbers would break most modern encryption schemes.").

even know if our information was stolen in an unencrypted form?

II. DATA BREACH NOTIFICATION LAWS AND ENCRYPTION EXCEPTIONS

State legislatures have taken steps to address these concerns. In 2002, California enacted a statute requiring any owner of licensed computerized data to notify state residents whose "personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[39] Other jurisdictions quickly followed suit, and now all fifty states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands each have some form of "data breach notification" law.[40] While the specifics of these laws vary, they all tend to focus on defining what types of personal-information data merit heightened protection and the conditions under which data holders must tell individuals about possible theft or breach of that sensitive information.[41] Data breach notification laws have the dual purpose of protecting private citizens and holding data owners accountable.[42] If a person knows that a malicious party might have stolen her private information, she can take protective steps such as freezing her credit or monitoring account balances with heightened scrutiny.[43] The notification

39. Assemb. B. 700, 2001–2002 Sess. (Cal. 2002).

40. *See Data Breach Notification in the United States and Territories*, PRIV. RTS. CLEARINGHOUSE (Dec. 10, 2018) https://perma.cc/B7EG-5JYT (providing basic information about every data breach notification law in the United States).

41. *See* Sara A. Needles, Comment, *The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law*, 88 N.C. L. REV. 267, 273–80 (2009) (explaining that data breach notification laws generally define what constitutes personally identifiable data, what events constitute data breaches, and how or whether a data holder must notify people if their personally identifiable data has been compromised).

42. *See* David Thaw, *Data Breach (Regulatory) Effects*, 2015 CARDOZO L. REV. DE-NOVO 151, 158 (2015) ("The stated purpose of most jurisdictions' breach notification statutes is to enable consumers to take steps to protect themselves by requiring custodians of this information to inform consumers when those custodians have lost control of this information.").

43. *See* Seena Gressin, *The Equifax Data Breach: What to Do*, FTC (Sept. 8, 2017), https://perma.cc/6BGE-ZWA8 (last updated Oct. 5, 2017) (suggesting different ways people might protect themselves from identity theft or fraud following the Equifax breach).

also informs individuals that they might be entitled to compensation from the negligent party that lost their data.[44] Requiring data custodians to report breaches encourages them to take greater precautionary measures because public knowledge of a breach will financially damage the custodian.[45]

The reporting mechanism differs by jurisdiction. Some jurisdictions require data holders to report potential breaches directly to the affected parties.[46] Others require an additional report to a state actor with authority to later publish information about the breach at the state actor's discretion.[47] One common provision requires the data holder to check with law enforcement and potentially delay issuing notices to ensure that the notices do not interfere with any ongoing criminal investigation.[48] Surprisingly, there is no federal data breach notification statute despite the piecemeal protections enacted in each of the states.[49] While data breach notification requirements

44. *See* Siegel Bernard, *supra* note 13 (discussing a settlement following the Equifax breach that allowed parties to reclaim money lost because of the data breach); Scottie Andrew, *Yahoo Could Pay You $358 for its Massive Data Breach Settlement. Here's How to Claim It*, CNN, https://perma.cc/RM2S-RJRM (last updated Oct. 15, 2019, 10:08 AM) (urging eligible consumers who received notification of a data breach at Yahoo to file for their share of a class action settlement).

45. *See IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years*, MKTS. INSIDER (July 23, 2019, 12:00 AM), https://perma.cc/HXX5-SRDZ (reporting on an IBM study, which found that on average a data breach will cost a company $3.92 million).

46. *See, e.g.*, 9 GUAM CODE ANN. § 48.30 (2022) (requiring disclosure of a data breach directly to affected residents unless a law enforcement agency requests delay).

47. *See, e.g.*, 815 ILL. COMP. STAT. 530/10 (2022) ("Upon receiving notification from a data collector of a breach of personal information, the Attorney General may publish the name of the data collector that suffered the breach, the types of personal information compromised in the breach, and the date range of the breach.").

48. *See, e.g.*, MO. REV. STAT. § 407.1500 (2022) ("The notice required by this section may be delayed if a law enforcement agency informs the person that notification may impede a criminal investigation or jeopardize national or homeland security . . . .")

49. A bill introduced in the Senate at the end of 2017 that would have created a federal data breach notification law for personally identifiable information never reached a vote. Data Security and Breach Notification Act, S. 2179, 115th Cong. (2017).

reach across jurisdictional boundaries,[50] standardized requirements at the federal level would encourage greater uniformity.

As previously acknowledged, theft of encrypted data presents very little danger if the malicious party lacks a decryption key.[51] In fact, legislators would likely want to exclude encrypted information from data breach notification laws out of fear that unnecessary warnings would dilute the efficacy of urgent ones in a boy-who-cried-wolf effect.[52] Sure enough, practically all jurisdictions with data breach notification laws include an encryption haven, or encryption exception.[53] This means data custodians do not need to tell citizens that their encrypted data has been stolen.[54] When the California legislature drafted the first data breach notification law, it intended for the statute to act as an incentive for companies to practice better data hygiene by encrypting their data to avoid potentially embarrassing notifications of breach.[55] This Note will consider different ways in which the various jurisdictions enacted encryption havens and compare their effectiveness.

---

50. Typically, notification is required if any resident of a jurisdiction is affected by a breach, so the location of the data holder is irrelevant. *See, e.g.*, N.M. STAT. ANN. § 57-12C-6 (2022) (requiring that a data owner "provide notification to each New Mexico resident whose personal identifying information is reasonably believed to have been subject to a security breach").

51. *Supra* notes 35–36 and accompanying text.

52. In *The Boy Who Cried Wolf*, a child repeatedly lied to his village about the approach of a dangerous wolf. Consequently, the village did not believe him when he authentically tried to warn it about a real wolf. *The Boy Who Cried Wolf*, FABLES OF AESOP, https://perma.cc/4WNS-X4SJ (last updated Oct. 5, 2020). This classic fable illustrates why the absence of an encryption haven could create harmful apathy toward notifications that carry real significance.

53. *See* Jill Joerling, Note, *Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data*, 32 WASH. U. J.L. & POL'Y 467, 475 (2010) (explaining that states have encrypted data safe harbors in their data breach notification laws, which means that no notification is required if compromised data was encrypted).

54. *Id.*

55. *See Personal Information: Privacy: Hearing on SB 1386 Before the Assembly Committee on Business and Professions*, 2001–2002 Sess. 3 (Cal. 2002) ("In practice, this bill will create incentives for organizations seeking to simplify their legal requirements to encrypt their personal information data.").

A. *West Virginia*

In West Virginia, data breaches are explicitly defined so that they do not include any instance in which encrypted information has been taken.[56] Other jurisdictions indirectly exclude compromised encrypted data from their definition of a data breach in a similar way by excluding information found in an encrypted form from the definition of personal information (the loss of which constitutes a breach).[57] In total, twenty-eight different jurisdictions have data breach notification laws that exclude all encrypted data from the definition of a breach.[58] This Note refers to the exclusion of all encrypted information from the definition of data breach as the "West Virginia model" for ease of identification.

B. *South Dakota*

Although the West Virginia model provides incentives for data owners to ensure that all data remains encrypted, statutes

---

56. *See* W. VA. CODE § 46A-2A-101(1) (2022) (defining a security breach as "the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information").

57. *See* OHIO REV. CODE ANN. § 1347.12(A)(2)(a) (West 2022) (recognizing a data breach in instances in which personal information has been taken); OHIO REV. CODE ANN. § 1347.12(A)(6)(a) (West 2022) (requiring certain data elements to be unencrypted for information to constitute "personal information").

58. *See* ARIZ. REV. STAT. ANN. § 18-551 (2022) (Arizona); ARK. CODE ANN. § 4-110-103 (2022) (Arkansas); CONN. GEN. STAT. § 36a-701b (2022) (Connecticut); D.C. CODE § 28-3851 (2022) (District of Columbia); FLA. STAT. § 501.171 (2022) (Florida); GA. CODE ANN. § 10-1-911 (2022) (Georgia); 9 GUAM CODE ANN. § 48.20 (2022) (Guam); IDAHO CODE § 28-51-104 (2022) (Idaho); KAN. STAT. ANN. § 50-7a01 (2022) (Kansas); KY. REV. STAT. ANN. § 365.732 (West 2022) (Kentucky); LA. STAT. ANN. § 51:3073 (2022) (Louisiana); ME. STAT. tit. 10 § 1347 (2022) (Maine); MD. CODE ANN. COM. LAW § 14-3501 (West 2022) (Maryland); MISS. CODE. ANN. § 75-24-29 (2022) (Mississippi); MO. REV. STAT. § 407.1500 (2022) (Missouri); MONT. CODE. ANN. § 30-14-1704 (2022) (Montana); NEV. REV. STAT. § 603A.040 (2022) (Nevada); N.J. STAT. ANN. § 56:8-161 (West 2022) (New Jersey); N.D. CENT. CODE § 51-30-01 (2022) (North Dakota); OHIO REV. CODE ANN. § 1347.12 (West 2022) (Ohio); OKLA. STAT. tit. 24, § 162 (2022) (Oklahoma); P.R. LAWS ANN. tit. 10, § 4052 (2022) (Puerto Rico); S.C. CODE ANN. § 39-1-90 (2022) (South Carolina); UTAH CODE ANN. § 13-44-102 (West 2022) (Utah); VT. STAT. ANN. tit. 9, § 2430 (2022) (Vermont); V.I. CODE ANN. tit. 14, § 2208 (2022) (Virgin Islands); W. VA. CODE § 46A-2A-101 (2022) (West Virginia); WIS. STAT. § 134.98 (2022) (Wisconsin).

of this kind do not mention encryption keys in determining what constitutes a breach,[59] despite the fact that anyone with the proper key can easily read encrypted data.[60] To eliminate any possible loophole concerning discovery of confidential keys, the South Dakota legislature defined data breaches to include stolen encrypted data if the corresponding key was also acquired.[61] Twenty-two jurisdictions have adopted data breach notification laws that define data breaches to include the theft of encrypted data only when the confidential key was also stolen or otherwise available to the stealing party.[62] This Note will refer to encryption havens of this kind as the "South Dakota model."

While the South Dakota model appears to give stronger protection to some data breach victims than the West Virginia model, explicitly identifying encryption keys as a mode of breach is likely only a semantic difference. Although this exact issue has never been litigated, a deciding court could reasonably find the leak of encrypted data with a key to constitute a breach of

59. *See, e.g.*, OHIO REV. CODE ANN. § 1347.12(A)(4) (West 2022) (acknowledging that access to a confidential key facilitates decryption but failing to incorporate the existence of such keys into the definition of what constitutes a breach).

60. *See* Swire & Ahmad, *supra* note 19, at 426 (likening cryptographic keys to physical keys capable of quickly opening their corresponding locks).

61. *See* S.D. CODIFIED LAWS § 22-40-19(1) (2022) (defining "breach of security system" as "the unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the information holder").

62. *See* ALA. CODE § 8-38-2(b)(2) (2022) (Alabama); ALASKA STAT. § 45.48.090 (2022) (Alaska); COLO. REV. STAT. § 6-1-716(2)(a.4) (2022) (Colorado); DEL. CODE. ANN. tit. 6, § 12B-101 (2022) (Delaware); HAW. REV. STAT. § 487N-1 (2022) (Hawaii); 815 ILL. COMP. STAT. 530/5 (2022) (Illinois); IND. CODE § 24-4.9-2-2 (2022) (Indiana); IOWA CODE § 715C.1 (2022) (Iowa); MASS. GEN. LAWS ch. 93H § 1 (2022) (Massachusetts); MINN. STAT. § 325E.61(e) (2022) (Minnesota); NEB. REV. STAT. § 87-802 (2022) (Nebraska); N.H. REV. STAT. ANN. § 359-C:19 (2022) (New Hampshire); N.M. STAT. ANN. § 57-12C-2(D) (2022) (New Mexico); N.Y. GEN. BUS. LAW § 899-aa (McKinney 2022) (New York); N.C. GEN. STAT. § 75-61(14) (2022) (North Carolina); OR. REV. STAT. § 646A.602 (2022) (Oregon); 73 PA. CONS. STAT. § 2303 (2022) (Pennsylvania); 11 R.I. GEN. LAWS § 11-49.3-3 (2022) (Rhode Island); S.D. CODIFIED LAWS § 22-40-19 (2022) (South Dakota); TENN. CODE ANN. § 47-18-2107 (2022) (Tennessee); TEX. BUS. & COM. CODE ANN. § 521.053 (West 2022) (Texas); VA. CODE ANN. § 18.2-186.6 (2022) (Virginia).

unencrypted information under the West Virginia model.[63] After all, any person possessing the proper key can read encrypted data as though they were written in plain text.[64] Holding otherwise would run contrary to the explicit purpose of these laws: to notify people when any unauthorized party has accessed or taken their personal information.[65] It follows that a court would likely rule in favor of notification in borderline cases. While more jurisdictions currently ascribe to the West Virginia model, some legislatures have started flipping to the South Dakota model, finding no drawbacks to the explicit clarification.[66]

Query then how a temporal element would affect this analysis. Suppose a company found that a hacker tried to steal personal data, but the company was confident that only encrypted personal information was taken. Would the company have any obligation to notify those parties whose encrypted information was taken if the corresponding key was stolen a few years later?

Presumably, the answer would still be yes under both the West Virginia and South Dakota models. As a standalone incident, a malicious party taking encrypted data does not constitute a data breach in any of the jurisdictions with encryption havens in their data breach notification laws.[67] Even under the South Dakota framework, the initial theft of the encrypted data would not have constituted a breach because "encrypted computerized data and the encryption key" were not

63. *See, e.g.*, *In re* Equifax Inc. Sec. Litig., 357 F. Supp. 3d 1189, 1208 (N.D. Ga. 2019) (listing Equifax's practice of putting encryption keys on a public server as an egregious security error and equating it to instances in which the data Equifax owned was left unencrypted entirely).

64. *See* Swire & Ahmad, *supra* note 19, at 426.

65. *See* Mark Burdon, *Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws*, 27 SANTA CLARA COMPUT. & HIGH TECH. L.J. 63, 78 (2010) ("First, the law primarily seeks to formally recognize that an individual has a 'right to know' about unauthorized misuse of his or her personal information and notice of the incident enables mitigation of subsequent identity theft.").

66. For example, Illinois narrowed its encryption haven to exclude instances in which encrypted information was compromised along with the associated key in 2016. H.B. 1260, 99th Gen. Assemb., Reg. Sess. (Ill. 2016) (enacted).

67. *See, e.g.*, MISS. CODE. ANN. § 75-24-29(2) (2022) (excluding encrypted information from the definition of a data breach).

taken together.[68] In spite of this statutory language, the theft of a key alone would probably force the data holder to notify all people whose personal information had been encrypted by the compromised code of the potential breach. Encryption remains effective only to the extent that the keys remain private.[69] Any hacker with the skills to discern a confidential key would only have done so with intent to decrypt related information.[70] The data custodian must assume that all encrypted information has been breached in addition to the key, because any of the data could have been compromised. Alternatively, someone with inside knowledge of the key, like a disgruntled employee, could compromise key integrity by going rogue, but such a party would also already have had known access to the encrypted data in the first place.[71] Either way, loss of the key would constitute a breach, independently requiring notification to the parties whose encrypted information had been previously taken.

C. *California*

A third type of encryption exception more explicitly addresses this scenario. California's data breach notification law does not define what constitutes a security breach in relation to whether data was encrypted, but rather makes notification conditional based on the encryption status of the stolen data.[72] In the above example, under California law, there would have been a breach the moment that the information holder learned that encrypted data was stolen, but the statute

68. S.D. CODIFIED LAWS § 22-40-19(1) (2022).

69. *See* Swire & Ahmad, *supra* note 19, at 426.

70. *See* Braun, *supra* note 36 ("Attackers are well aware that encrypted data is useless without keys, so what do they go after? The keys.").

71. *See Rogue Postbank Employees Steal Master Encryption Key; Make Off with $3.2 Million*, FINEXTRA (June 19, 2020), https://perma.cc/C945-VG7L (reporting on the devastating effects of an inside data breach); Sooraj Shah, *The Rise of Employees Stealing Data: How Do Businesses Stop This from Happening?*, INFORMATIONAGE (Mar. 28, 2019), https://perma.cc/EVJ9-8RGR (detailing the increasing potential for data breaches by companies' employees).

72. *See* CAL. CIV. CODE § 1798.82(a) (West 2022) (requiring notification when "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person," or a key and encrypted information have been taken, giving the trustee "a reasonable belief that the encryption key or security credential could render that personal information readable or usable").

does not call for the holder to report the breach until someone compromised the key.[73] Although interpretation of the West Virginia and South Dakota encryption exceptions would likely result in the same outcome, this formulation better handles temporal breach issues by broadening the definition of a breach and narrowing the conditions for notification. Presumably, that difference would simplify any potential litigation and increase the likelihood of a finding in favor of notification. Michigan and Washington join California as the only states to have adopted what this Note will refer to as the "California model" for legislating encryption havens.[74]

D. *Tennessee*

Two additional treatments of encryption in data breach notification laws merit some attention. First, a jurisdiction could decide that any breach of personal information requires notice. While no data breach notification laws in the United States currently ignore encryption practices this way,[75] Tennessee adopted this rigid approach for roughly eight months in 2016 and 2017.[76] Starting from a West Virginia model, the state legislature removed the encryption exception from its definition of a data breach.[77] Senator Bill Ketron, the leading proponent of the change, appeared largely motivated by a desire to provide greater security and information to constituents, and perhaps in part by a misunderstanding of the relative security that

---

73. *Id.*

74. *See* CAL. CIV. CODE § 1798.82 (West 2022) (California); MICH. COMP. LAWS § 445.72 (2022) (Michigan); WASH. REV. CODE § 19.255.010 (2022) (Washington).

75. *See Data Breach Notification in the United States and Territories*, PRIV. RTS. CLEARINGHOUSE (Dec. 10, 2018) https://perma.cc/B7EG-5JYT (documenting the treatment of encryption in every data breach notification law in the United States).

76. *See* Thomas Ritter, *Tennessee Amends Its Breach Notification Law (AGAIN) and Reinserts the Encryption Safe Harbor*, THOMPSON BURTON (Mar. 29, 2017), https://perma.cc/3EAK-Y3A3 (reporting that Tennessee abandoned its encryption haven for about eight months).

77. *Compare* TENN. CODE ANN. § 47-18-2107 (2015), *with* TENN. CODE ANN. § 47-18-2107 (2016) (changing the definition of a security breach from "unauthorized acquisition of unencrypted computerized data" in 2015 to "unauthorized acquisition of computerized data" in 2016).

encryption provides.[78] Regardless, after heavy lobbying from data holders the state quickly reversed course to include an encryption exception, this time in alignment with the South Dakota model.[79] Within a short window, the legislature realized that ubiquitous and often unnecessary notifications would impose unreasonable costs on information holders.[80] Additionally, the state wanted to promote responsible encryption practices, an original purpose of data breach notification laws.[81] Although Tennessee's legislature had noble intentions in its attempt to protect consumers, an encryption exception proved more practical.

Still, excluding an encryption exception provides some benefit because not all encryption is created equally. For example, in a groundbreaking 2013 article, the *New York Times* reported that the National Security Agency (NSA) had circumvented common encryption practices and was invading citizen privacy.[82] A follow-up report revealed that the NSA accomplished this by building a backdoor into a standard

78. *See Hearing on S.B. 2005 Before the S. Com. & Lab. Comm.*, 109th Gen. Assemb. at 1:09:12 (Tenn. 2016) (statement of Sen. Bill Ketron), https://perma.cc/JB4X-TQXJ ("This bill will also include encrypted. And the reason for including the encrypted is that encrypted data is now being stolen almost as easily as the unencrypted. So, we felt like that [sic] we should include that.").

79. *Compare* TENN. CODE ANN. § 47-18-2107 (2016), *with* TENN. CODE ANN. § 47-18-2107 (2017) (amending the statute to clarify that a breach of system security includes only the acquisition of unencrypted data or encrypted data with a key as opposed to the previous provision, which considered loss of all personal information a data breach).

80. *See Hearing on S.B. 547 Before the S. Com. & Lab. Comm.*, 110th Gen. Assemb. at 1:06:45 (Tenn. 2017) (statement of Sen. Bill Ketron), https://perma.cc/ZPF5-RHNH ("The language will eliminate the burden of reporting encrypted data that does not threaten the integrity of personal information maintained by the information holder, conserving both time and expenses.").

81. *See Hearing on H.B. 545 Before the H. Consumer & Hum. Res. Subcomm.* at 1:51 (Tenn. 2017) (statement of Rep. Courtney Rogers), https://perma.cc/DS75-9Z2Q ("All encrypted data is not created equal, and by just having it all up together we kind of created a disincentive for companies to encrypt their data. And so, we're going to rectify that with further clarifying.").

82. *See* Nicole Perlroth et al., *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES (Sept. 5, 2013), https://perma.cc/5MV7-E7VP (detailing efforts by the NSA to skirt around encryption through the Bullrun program).

algorithm used to generate the random large prime numbers necessary for encryption.[83] That standard algorithm was immediately reevaluated and discarded.[84] In theory, however, a data holder could still rely on encryption that applied this standard, which is known to be breakable. Encryption exceptions employed by other statutes might allow such a data holder to avoid reporting requirements. By excluding encryption havens entirely, Tennessee forcefully, albeit temporarily, rejected this prospect.

E. *Wyoming*

Wyoming provides a better example of how data breach notification laws can function without an encryption haven. Wyoming's data breach notification statute completely excludes any mention of encryption.[85] Instead, the acquisition of select personal identifying information may be excluded from the definition of a breach to the extent that some digits of numerical data have been redacted.[86] Rather than requiring notification following the discovery of a breach, the statute gives each data owner the discretion to "conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal identifying information has been or will be misused."[87] This lack of treatment with respect to encryption still allows data trustees not to report the theft of encrypted data when they immediately and reasonably decide that no malicious party can misuse the data (as long as the key remains secure).[88] It also differs from the failed Tennessee experiment because Wyoming does not have the same legislative history explicitly establishing

83. *See* Nicole Perlroth, *Government Announces Steps to Restore Confidence on Encryption Standards*, N.Y. TIMES (Sept. 10, 2013, 7:02 PM), https://perma.cc/TT86-7QRR (explaining how the NSA pushed the compromised Dual EC DRBG standard).

84. *See id.*

85. WYO. STAT. ANN. § 40-12-501 (2022).

86. *See id.* § 40-12-501(a)(vii) (defining personal information as a name coupled with unredacted information like a credit-card or social-security number); *id.* § 40-12-501(a)(viii) (establishing that in this context, redacted means altered or truncated so that no more than five digits are accessible).

87. *Id.* § 40-12-502(a).

88. *See id.*

legislative intent for companies to send a notification of every encrypted data breach.[89]

Of course, self-regulation with respect to the notification decision could have serious drawbacks. In borderline cases, a company might seek to avoid the heavy financial burdens associated with the public knowledge of a data breach by choosing not to notify the affected parties.[90] That said, experts have provided reasoned arguments both for and against self-regulation.[91] Given the security of normal encrypted data, the Wyoming statute will almost certainly never lead to more notification than a data breach notification law using the California model because reasonable data trustees would never choose to report the theft of encrypted information unless they had a concern about the key or encryption mechanism.

Suffice it to say, jurisdictions around the United States have adopted a multitude of varying data breach notification laws to combat information theft crimes. These statutes largely function with the dual purpose of notifying people when someone has compromised their sensitive personal information and encouraging data holders to encrypt their data.[92] Implicitly, data breach notification laws rely on the principle that the mathematical complexities underlying encryption render it impervious to traditional computing attacks.[93] This assumption is necessary because there is no known, better way to efficiently facilitate secure online interactions, and researchers have found

89. *See supra* notes 77–78 and accompanying text.

90. *See IBM Study Shows Data Breach Costs on the Rise*, *supra* note 45 (demonstrating the tremendous expenses of a data breach).

91. *See* Alexander Pfaff & Chris William Sanchirico, *Big Field, Small Potatoes: An Empirical Assessment of EPA's Self-Audit Policy*, 23 J. POL'Y ANALYSIS & MGMT. 415, 426 (2004) (suggesting that self-policed EPA violation reports might act as red herrings to distract from major unreported violations); Jodi L. Short & Michael W. Toffel, *Coerced Confessions: Self-Policing in the Shadow of the Regulator*, 24 J. L. ECON. & ORG. 45, 62–63 (2008) (finding that self-policing becomes much more common with frequent inspection and greater threat of enforcement action). *But see* Neil Malhotra et al., *Does Private Regulation Preempt Public Regulation?*, 113 AM. POL. SCI. REV. 19, 34–35 (2019) (determining that industries might self-regulate to acknowledge a problem and act on it in efforts to preempt legal obligations that could be more expensive, more onerous, and less effective).

92. *See supra* notes 42–44, 51–55 and accompanying text.

93. *See supra* notes 34–38 and accompanying text.

no evidence that the mathematical premise is false.[94] However, a looming technological advancement soon promises to throw the current state of private communications and informational data storage into chaos.

III. QUANTUM COMPUTING

Toward the end of the twentieth century, scientists combined information theory with quantum physics to reimagine computation and the physics of its underlying mechanisms.[95] Quantum computing developed as a result.[96] At the most basic level, classical computers rely on binary—a base-two counting system visualized with strings of ones and zeros—to create complex commands and perform intricate operations.[97] The smallest unit of binary, a bit, will take on a value of either zero or one depending on the presence or absence of an electrical signal.[98]

Unlike the binary units used by classical computers, quantum bits (commonly referred to as "qubits")—the building blocks of quantum computing—exist as a continuum, or superposition, of possible values.[99] Whereas a bit must take on a single value of either zero or one, any given qubit simultaneously holds both values (along with every number in between).[100] When someone measures the value of a qubit on a binary basis, the state of the qubit changes into one of the binary options.[101] That measurement value is probabilistically

94. *See supra* note 32 and accompanying text.

95. *See* ELEANOR RIEFFEL & WOLFGANG POLAK, QUANTUM COMPUTING: A GENTLE INTRODUCTION 1–2 (William Gropp & Ewing Lusk eds., 2011) (explaining how information theory allowed for discussion of computation abstracted from underlying mechanics and scientists then applied these concepts to a system of computation utilizing quantum measurement).

96. *Id.*

97. *See* Anthony Heddings, *What Is Binary, and Why Do Computers Use It?*, HOW-TO GEEK (Oct. 1, 2018, 6:40 AM), https://perma.cc/9264-NPRU (describing binary and how it works).

98. *Id.*

99. *See* Kevin Bosner & Jonathan Strickland, *How Quantum Computers Work*, HOW STUFF WORKS (Dec. 8, 2000), https://perma.cc/DTP6-LC9V (providing a brief description of the qubit).

100. *Id.*

101. *See* RIEFFEL & POLAK, *supra* note 95, at 16–17 (explaining superpositions and the effects of single-qubit measurement). To illustrate this

dependent on the fixed initial superposition of the qubit.[102] Because measurement changes the state of a qubit, each qubit has the capability to hold exactly one bit of classical computing information.[103] That said, a quantum property known as entanglement mysteriously allows multiple qubits to yield the same random results upon measurement.[104] While intricacies of the underlying theory far exceed the scope of this Note, mathematicians have taken advantage of entanglement to produce non-intuitive results and build an understanding of the operations that a computer built on entangled qubits could carry out.[105]

For many problems and tasks, researchers have not yet found quantum algorithms that are provably more efficient than the fastest known classical analog.[106] However, some quantum

---

phenomenon, consider the polarization of a beam of light. *Id.* at 10–13. Photons will only pass through a polaroid film with probabilities based on their amplitudes relative to the polarity of the film. *Id.* If a photon does pass through the film, it is now polarized in the direction of the film, and its initial polarity along with information about it has been lost. *Id.*

102. *See id.*

103. *See* RIEFFEL & POLAK, *supra* note 95, at 17–18

> [T]he properties of quantum measurement severely restrict the amount of information that can be extracted from a qubit. . . . [E]ven though a quantum bit can be in infinitely many different superposition states, it is possible to extract only a single classical bit's worth of information from a single quantum bit.

104. *See id.* at 60–62 (discussing this phenomenal behavior and the corresponding paradox of why particles separated by such a large distance will behave in the exact same random way every time, and how scientists have no explanation for this natural wonder); A. Einstein et al., *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, 47 PHYSICAL REV. 777, 780 (1935) (concluding that our understanding of quantum physics as it relates to reality is incomplete in this area).

105. *See* RIEFFEL & POLAK, *supra* note 95, at 2–4 (detailing a brief history of the development of quantum computing).

106. *See, e.g.*, Peter Høyer et al., *Quantum Complexities of Ordered Searching, Sorting, and Element Distinctness*, 34 ALGORITHMICA 429, 447 (2002) (determining that quantum algorithms cannot provide a meaningful advantage in sorting over classical algorithms). *But see* Peter W. Shor, *Why Haven't More Quantum Algorithms Been Found?*, 50 J. ACM 87, 88–89 (2003) (suggesting that mathematicians have not discovered more quantum algorithms improving on classical computing processes in part because they have focused on superpolynomial speedups to difficult problems rather than focusing on discovering polynomial time improvements to already relatively fast classical algorithms). In fact, the discovery of a seemingly faster quantum

algorithms have the capacity to more efficiently address challenges that would take significant amounts of time for even the strongest classical computers to reliably solve.[107] In 1994, applied mathematician Peter Shor generated wide interest in quantum computing when he discovered the first quantum algorithm with meaningful practical significance.[108] Shor's algorithm, which still excites the imagination today, would allow a quantum computer to factor and solve the discrete algorithm problem in polynomial time.[109] Effectively, using Shor's algorithm, a quantum computer of sufficient complexity would have the capability to thwart the current methods of public-key encryption discussed above in Part I.[110]

---

algorithm has, at times, spurred classical innovation because researchers will attempt to prove that no classical alternative exists that could operate at the quantum algorithm's speed, but instead find a more efficient classical algorithm. *See* Kevin Hartnett, *Major Quantum Computing Advance Made Obsolete by Teenager*, QUANTA MAG. (July 31, 2018), https://perma.cc/8WES-VWGC (discussing the discovery of a classical algorithm able to solve the recommendation problem with similar efficiency as a quantum algorithm that experts previously understood as an example of quantum advantage); Ariel Bleicher, *Quantum Algorithms Struggle Against Old Foe: Clever Computers*, QUANTA MAG. (Feb. 1, 2018), https://perma.cc/C2DX-TQQE ("Paradoxically, reports of powerful quantum computations are motivating improvements to classical ones, making it harder for quantum machines to gain an advantage.").

107. *See generally* Lov K. Grover, *Quantum Mechanics Helps in Searching for a Needle in a Haystack*, 79 PHYSICAL REV. LETTERS 325 (1997) (detailing a quantum search algorithm that would provide a quadratic improvement over the most efficient possible classical algorithm); Esma Aïmeur et al., *Quantum Speed-Up for Unsupervised Learning*, 90 MACH. LEARNING 261 (2012) (demonstrating how quantum computing could facilitate faster unsupervised machine learning).

108. *See* Davide Castelvecchi, *Quantum-Computing Pioneer Warns of Complacency Over Internet Security*, NATURE (Oct. 30, 2020), https://perma.cc/3RXT-QC5L ("The news spread amazingly fast . . . . All sorts of people were asking me for my paper before I had even finished writing it, so I had to send them an incomplete draft." (quoting Peter Shor)).

109. *See generally* Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, 41 SIAM REV. 303 (1999).

110. *See generally* Craig Gidney & Martin Ekerå, *How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits*, ARXIV 1905.09749 (May 23, 2019), https://perma.cc/PEM4-HMCJ (PDF) (last updated Apr. 13, 2021) (combining multiple different optimizations to demonstrate how a twenty million-qubit quantum computer could decrypt popular forms of public-key encryption in a matter of hours).

Of course, the mere existence of Shor's algorithm means nothing unless quantum computers with the capacity to run it become a physical reality. Although physics does not preclude the possibility of creating such a machine, constructing one has proven to be a considerable engineering challenge.[111] Among other problems, entangled states are highly susceptible to outside influences such as temperature changes and vibrations, so engineers need to find clever solutions to prevent outside interference and create the stable environments necessary to house the qubits of a quantum computer.[112]

Researchers first developed a two-qubit quantum computer in 1998.[113] But this mode of construction could not scale into a system with significantly more qubits, so researchers have continued to search for other solutions.[114] Today, rivaling

111. *See* Kevin McCaney, *Quantum Computing: 'Physicist's Dream' or 'Engineer's Nightmare'?*, GOV'T CIO (Mar. 23, 2018, 4:00 PM), https://perma.cc/LK96-2N63 ("The thing driving the hype is the realization that quantum computing is actually real . . . . It is no longer a physicist's dream—it is an engineer's nightmare." (quoting MIT professor Isaac Chuang)).

112. *See* Dashveenjit Kaur, *IBM 'Super-Fridge' Aims to Solve Quantum Computer Cooling Problem*, TECH HQ (Dec. 15, 2020), https://perma.cc/CMF2-5H8N (reporting on IBM's plans to build a giant refrigerator named "GoldenEye" capable of housing a future large qubit system at a temperature of –459 degrees Fahrenheit); *Atoms Make Better Quantum Computers*, IONQ, https://perma.cc/C97W-BD84 (explaining how IonQ uses "a collection of laser-based techniques called *resolved-sideband cooling* to produce qubits so cold that they are almost perfectly still at an atomic level" and then places the qubits in an extremely strong vacuum to prevent any possible collisions with other matter).

113. *See* John Markoff, *Quantum Computing Is Becoming More than Just a Good Idea*, N.Y. TIMES (Apr. 28, 1998), https://perma.cc/BXD6-ED2D (reporting on the creation of the first quantum computer and the potential promise of this technology); Neil Gershenfeld & Isaac L. Chuang, *Quantum Computing with Molecules*, SCI. AM., https://perma.cc/UPV2-C52S (explaining the methods used to construct this primitive quantum computer).

114. *See* Gershenfeld & Chuang, *supra* note 113

> A basic limitation of the chloroform computer is clearly its small number of qubits. The number of qubits could be expanded, but n could be no larger than the number of atoms in the molecule employed. . . . [T]o create still larger computers, other techniques, such as optical pumping, would be needed to 'cool' the spins.

governments,[115] academic laboratories,[116] and major technology companies[117] are still competing to develop effective quantum computers in a quest to attain quantum supremacy on a host of practical problems.[118] Increasingly, it appears that scientists are on the brink of a quantum future. In late 2019, Google published a paper in which it claimed to have achieved quantum supremacy on a specific random sampling task.[119] For the first

115. *See* Michael Kratsios & Chris Liddell, *The Trump Administration Is Investing $1 Billion in Research Institutes to Advance Industries of the Future*, WHITEHOUSE (Aug. 26, 2020), https://perma.cc/U75C-GVP6 (announcing a $625 million investment in quantum information, to include quantum computing, at five Department of Energy research centers); Jeffrey Lin & P.W. Singer, *China Is Opening a New Quantum Research Supercenter*, POPULAR SCI. (Oct. 10, 2017, 4:00 PM), https://perma.cc/C8BE-D4NA (discussing China's $10 billion research center for quantum computing).

116. *See, e.g.*, Miranda Volborth, *'More Possibilities than There Are Particles in the Universe'*, DUKESTORIES (Nov. 12, 2020), https://perma.cc/6M5Q-MJ9D (advertising the aggregation of multiple experts to form a super team of quantum researchers working toward building stronger quantum computers at a Duke lab); *About the Institute for Quantum Computing*, UNIV. WATERLOO, https://perma.cc/NJW9-SCH9 (detailing the success of a research institute in Canada that is completely dedicated to quantum information research and has produced 1,869 publications since 2002); *About HQI*, HARV. QUANTUM INITIATIVE, https://perma.cc/56PC-VV5S (promoting Harvard's quantum research community).

117. *See* Jay Gambetta, *IBM's Roadmap for Scaling Quantum Technology*, IBM (Sept. 15, 2020), https://perma.cc/3PHB-BBQ3 (revealing IBM's plans to build a 1,121 qubit computer by 2023 and a one-million qubit computer in the next decade); Paul Smith-Goodson, *Google's Top Quantum Scientist Explains in Detail Why He Resigned*, FORBES (Apr. 30, 2020, 10:31 AM), https://perma.cc/4AMB-UQ2S ("The Google plan is roughly to build a million-qubit system in about ten years, with sufficiently low errors to do error correction. Then at that point you will have enough error-corrected logical qubits that you can run useful, powerful algorithms that you now can't solve on a classical supercomputer." (quoting former Google lead quantum scientist John Martinis)).

118. *See* Bernard Marr, *What Is Quantum Supremacy and Quantum Computing? (And How Excited Should We Be?)*, FORBES (Aug. 17, 2020 12:19 AM), https://perma.cc/3XJQ-75UP (defining quantum supremacy as the ability of a quantum computer to perform a task that a classical computer could not, or that would take a classical computer an incredibly long time to complete).

119. *See* Frank Arute et al., *Quantum Supremacy Using a Programmable Superconducting Processor*, 574 NATURE 505, 505 (2019) ("Our Sycamore processor takes about 200 seconds to sample one instance of a quantum circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years."). *But see* Edwin Pednault et al., *On "Quantum Supremacy"*, IBM (Oct. 21, 2019), https://perma.cc/9NEW-TFL8 (*"[A]n ideal simulation of the*

time, a quantum computer had carried out an operation that classical computers could not.[120] One year later, researchers in China announced that they had built a quantum computer capable of Gaussian boson sampling one hundred trillion times faster than would be possible using a classical system.[121] Although nobody can predict exactly when it will happen, the next large quantum computing milestone could be the construction of a quantum computer capable of factoring large numbers.[122] Scientists have already built a scalable model capable of factoring small numbers, so regardless of the timeline, eventual development appears inevitable.[123]

---

same task can be performed on a classical system in 2.5 days and with far greater fidelity. This is in fact a conservative, worst-case estimate, and we expect that with additional refinements the classical cost of the simulation can be further reduced.").

120. *See* Jeffrey Kluger, *Google Has Achieved 'Quantum Supremacy.' Just What the Heck Is That?*, TIME (Oct. 23, 2019, 12:01 PM), https://perma.cc/KJM6-SQSG (last updated Oct. 24, 2019, 9:24 AM) ("[T]here's no denying that a hinge-point in computer history has been turned. . . . [T]he fact is, the quantum world has always existed. The news—the huge news—is that now we've arrived there, too.").

121. *See* Han-Sen Zhong et al., *Quantum Computational Advantage Using Photons*, 370 SCIENCE 1460, 1460 (2020) ("The photonic quantum computer, *Jiuzhang*, generates up to 76 output photon clicks, which yields an output state-space dimension of 10^{30} and a sampling rate that is faster than using the state-of-the-art simulation strategy and supercomputers by a factor of ~10^{14}."). Currently there are no known practical applications of this technique beyond demonstrating quantum supremacy. Hamish Johnston, *Quantum Advantage Demonstrated Using Gaussian Boson Sampling*, PHYSICS WORLD (Dec. 3, 2020), https://perma.cc/U8YA-YDLN (noting the lack of concrete practical applications to Gaussian boson sampling but remaining optimistic that it could help future research efforts).

122. *See* Volborth, *supra* note 116 ("[T]he Duke team agrees that getting close enough to grab the golden ring—breaking public-key cryptography—is still at least a decade away."); Jon R. Lindsay, *Why Is Trump Funding Quantum Computing Research but Cutting Other Science Budgets?*, WASH. POST (Mar. 13, 2020), https://perma.cc/F4UP-7S7M ("It may take decades to clear all the engineering hurdles."); Cecelia Smith-Schoenwalder, *What to Know About 'Quantum Supremacy'*, U.S. NEWS (Oct. 22, 2019, 4:17 PM), https://perma.cc/A7JL-WRA6 (noting that quantum computers capable of breaking encryption systems are a long way off, while simultaneously quoting technology analyst Brian Hopkins as saying that "[t]here are a number of breakthroughs that could take a lot less time than we think . . . . It could change very quickly").

123. *See* Jennifer Chu, *The Beginning of the End for Encryption Schemes?*, MIT NEWS (Mar. 3, 2016), https://perma.cc/HK6L-WSZ6 (reporting on a

With such developments lurking on the horizon, lawmakers need to think critically about whether society is prepared for the quantum future, and if not, what new laws and adjustments to existing laws they need to enact. Interplay between the current encryption exceptions of state data breach notification laws and quantum decryption deserves some attention on this front. Will the construction of a computer capable of quantum decryption require data holders to alert everyone whose personal information they have ever held of a potential breach? What does the role of data breach notification laws look like for newly collected or generated data beyond that threshold? Finally, what future consequences do current encryption exceptions hold because of their implicit assumption that common asymmetric encryption mechanisms promise indefinite security?

IV. SHOR'S ALGORITHM AS A TRIGGER FOR CURRENT DATA BREACH NOTIFICATION LAWS

Once scientists realize a quantum computer capable of factoring with Shor's algorithm, not only will public-key encryption methods fail moving forward, but also any stockpiled encrypted data will no longer remain protected.[124] Because state data breach notification laws are intended to protect people if their personal data become insecure, intuitively one might expect to receive a notification if all of her private information became accessible at once.[125] However, encryption exceptions muddy this water. If the laws do not require any action by the data holder with respect to lost encrypted information, perhaps they convey no duty here. To address that inquiry, this Note will revisit the various groupings of encryption havens provided in the different states' data breach notification laws to discern

---

quantum computer factoring the number fifteen and its creator's belief that the machine will be "straightforwardly scalable").

124. *See Quantum Computing and Cybersecurity*, THALES (Oct. 23, 2019), https://perma.cc/TT7J-PZRX (cautioning that "encrypted data can be saved and decrypted at a later point in time" with a quantum computer); Arthur Herman, *Booz Allen Sounds the Alarm on China's Coming Quantum Harvest*, FORBES (Dec. 9, 2021, 11:48 AM), https://perma.cc/9SPV-BT69 (specifically identifying a concerted Chinese plan of stealing data with the intention to decrypt that information in the future with technology the country is actively developing).

125. *See supra* notes 42–44 and accompanying text.

whether they would mandate notification for all data that could possibly be compromised by quantum factoring.

A. *The Tennessee Model Revisited*

In a hypothetical state using the abandoned Tennessee encryption treatment, data holders would constantly issue breach notifications regardless of whether taken information had been encrypted.[126] Theoretically, people would already have been warned that their encrypted personal information was insecure prior to the emergence of quantum decryption.[127] Data holders could reasonably argue that they had already met their statutory duty and hold no responsibility to issue further warning.[128] Unfortunately, the original alerts would likely have fallen on deaf ears. Because this framework vastly overstates the current dangers of identity theft, citizens might have become numb to the repeated alerts.[129] Further, at the time people received the original notice, they would have no reason to take it seriously given common trust in the power of standard encryption.[130] Quantum decryption would create a drastic swing in the relative accessibility of personal information for which the Tennessee model would already have provided a premature notification. By issuing data breach notifications too soon, this statute would convey danger as ineffectively as if no notification had been provided at all.

B. *The West Virginia Model Revisited*

Jurisdictions following the West Virginia model would also likely fail to address the danger of quantum factoring to consumers through their data breach notification laws. A law-abiding data trustee would have no reason to report, or even keep track of, instances in which potentially malicious parties accessed encrypted personal information under a statutory

126. *See* Rosemarie Lally, *Tennessee Strengthens Data Security Breach Notification Law*, SHRM (May 5, 2016), https://perma.cc/M3MB-6GU2 (noting that the old Tennessee data breach notification law would require immediate notification of a breach even if it only contained encrypted data).

127. *Id.*

128. *See supra* note 78.

129. *See supra* note 52 and accompanying text.

130. *See supra* notes 31–38 and accompanying text.

regime that excludes encrypted information from the definition of a breach.[131] The texts of these statutes simply do not contain a temporal element to mandate notification when unusable data previously compromised is presently rendered useful by an outside force (in this case, by quantum computing making asymmetric encryption insecure).[132] In fact, most of these statutes call for sending notifications as quickly as possible following the discovery of a breach.[133] Delayed notices for known breaches that originally seemed harmless would conflict with those provisions.

Recall that if an encryption key was stolen in one of the West Virginia model jurisdictions, subjects of previously compromised personally identifying data would likely be notified because loss of the key would constitute a fresh breach.[134] The same rationale does not apply as easily to the use of quantum processes for decryption. In the original scenario, a "breach" would presumably have occurred because the fraudster stole essentially unencrypted data to the extent that the key made it easily readable.[135] Those whose encrypted data had previously been compromised would get pulled into the requisite notification as a precautionary consequence.[136] A fraudster using Shor's algorithm has everything she needs as soon as she accessed the encrypted information.[137] She never needs to steal "unencrypted" data from the data holder, so there is never a breach to trigger notification.[138] As such, the West Virginia model would not require data holders to notify people that their

131. *See, e.g.*, W. VA. CODE § 46A-2A-101(1) (2022) (defining a data breach to include only compromised unencrypted data).

132. *Id.*

133. *See, e.g.*, MICH. COMP. LAWS § 445.72(4) (2020) (specifying that notification should be made without "unreasonable delay," seemingly tied to initial discovery of a breach).

134. *See supra* notes 69–71 and accompanying text.

135. *See* Swire & Ahmad, *supra* note 19, at 426 (illustrating how keys facilitate easy encryption and decryption of data).

136. *See supra* notes 70–71 and accompanying text.

137. *See Quantum Computing and Cybersecurity*, *supra* note 124 https://perma.cc/TT7J-PZRX ("[E]ncryption must be secured against Quantum Computers even before these exist, as encrypted data can be saved and decrypted at a later point in time.").

138. *Id.*

encrypted data had been previously taken once quantum technology makes that data readable.

In fact, as legislators have currently worded the West Virginia model encryption havens, theft of encrypted data might not even trigger notification for future breaches that occur after quantum computers capable of breaking standard public-key encryption have emerged. That would depend heavily on whether the definitional understanding of the word "encryption" evolves. For example, "encrypt" can mean "encode."[139] That definition would not require notification because stolen encrypted data would still be encoded; a hacker would simply have the requisite mathematical tools to discern the confidential key used for encoding. Alternatively, its meaning could be tied to federally established encryption standards.[140] If such standards are adjusted to address the threat of quantum decryption, then it is conceivable that the asymmetric mathematical operations we currently consider "encryption" could fall out of the term's definition. Most data breach notification statutes do not provide precise mathematical definitions of what "encryption" means.[141] Those jurisdictions that have stated what encryption means in more concrete terms currently have the benchmark fixed in a place that would present no obstacle to quantum decryption.[142] Some states might have circumvented this problem by specifying unreadability as an additional condition for the encryption exception to kick in, but even this might not provide assurance

139. *Encrypt*, MERRIAM-WEBSTER DICTIONARY, https://perma.cc/M7DC-QFZM.

140. *See* Ross Thomas, *Advanced Encryption Standard (AES): What It Is and How It Works*, HASHEDOUT (Apr. 23, 2020), https://perma.cc/SDP2-ZAWM (explaining the use of AES, the NIST established encryption standard).

141. *See, e.g.*, W. VA. CODE § 46A-2A-101 (2022) (defining encryption as "transformation of data through the use of an algorithmic process to into a form in which there is a low probability of assigning meaning without use of a confidential process or key"). The West Virginia definition is unhelpful because encryption would still yield low probability of assigning meaning without the confidential key, but Shor's algorithm would make it impossible to fully protect the confidential keys from parties with advanced technological capabilities.

142. *See, e.g.*, 11 R.I. GEN. LAWS § 11-49.3-3 (2022) ("'Encrypted' means the transformation of data through the use of a one hundred twenty-eight (128) bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key.").

of post-quantum notifications.[143] In most cases, it appears that for the statutes of West Virginia model jurisdictions to require notification when what we currently understand as encrypted data has been compromised in a post-quantum world, their definitions of what constitutes "encryption" need to be revised.

C. *The South Dakota Model Revisited*

Current South Dakota model laws would similarly fail to mandate notifications around quantum-decryption breaches. Like under the West Virginia model, these statutes have no concrete temporal element that would require data trustees to tell people that their encrypted personally-identifying information was compromised in a distant breach once quantum decryption renders that data insecure.[144] Further, use of a quantum computer capable of decrypting encrypted information still appears to skirt around the South Dakota notification requirements because encrypted data would fall under the encryption havens.[145]

In fact, the expanded definition of a breach under these statutes could make it more likely that quantum decryption would not require notification moving forward.[146] By explicitly enumerating an exception to the encryption haven notification shield, these laws preclude the judiciary from inferring additional exceptions.[147] By clarifying that compromise of a key

143. *See* WIS. STAT. § 134.98 (2022) (specifying that loss of personal information requisite for a breach must contain an element that is "not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable"). Of course, pressing this as a reason for post-quantum notifications could spur debate about what readability means. When untouched, encrypted information would remain largely meaningless, but more people would have the technological capabilities to revert the data back into its coherent form.

144. *See* S.D. CODIFIED LAWS § 22-40-19 (2020) (making no mention of the data holder's responsibilities to keep track of potentially leaked encrypted data in case a key later becomes compromised); *see also supra* notes 134–138 and accompanying text.

145. *See supra* notes 139–142 and accompanying text.

146. *See* S.D. CODIFIED LAWS § 22-40-19 (2022) (including encrypted information taken with an encryption key in the definition of a security breach).

147. *See* Andrus v. Glover Constr. Co., 446 U.S. 608, 616–17 (1980) ("Where Congress explicitly enumerates certain exceptions to a general

with encrypted data constitutes a breach, these jurisdictions have implicitly endorsed the position that encryption status depends not on data readability, but rather on whether mathematical operations have scrambled the information. That level of legislative specificity ultimately impairs the efficacy of these laws in a post-quantum world by preventing an evolving interpretation of "encryption" that would require notification whenever personally identifiable information has been breached in a readily accessible format.

D. *The California Model Revisited*

The California model addresses some of these problems, but still would not necessitate widespread notification as a result of quantum decryption. By excluding language about encryption from the definition of a data breach, but instead adding it to notification requirements, these statutes are more likely to allow delayed notification when formerly taken encrypted data becomes compromised by the development of quantum factoring.[148] This follows the same rationale that would require notification in California should someone steal an encryption key corresponding to encrypted data that had been compromised years earlier.[149] Of course, the issue of how to interpret "encryption" would persist.[150] Presumably these jurisdictions would not require notification because they tend to specify cut-outs for stolen encrypted data combined with access to the corresponding keys.[151] Again, current data breach notification laws appear likely to fail at protecting consumers once effective quantum decryption becomes possible.

---

prohibition, additional exceptions are not to be implied, in the absence of evidence of a contrary legislative intent.").

148. *See* CAL. CIV. CODE § 1798.82 (West 2022) (requiring notification of a breach to residents whose unencrypted personal information was taken during the breach).

149. *See supra* notes 72–74 and accompanying text.

150. *See supra* notes 139–143, 146–147 and accompanying text.

151. *See* CAL. CIV. CODE § 1798.82 (West 2022) (requiring notification of a breach to a person "whose encrypted personal information was . . . acquired by an unauthorized person and the encryption key or security credential was . . . acquired").

E. *The Wyoming Model Revisited*

Curiously, Wyoming's data breach notification law might have the greatest potential to force meaningful notifications about compromised personal information once quantum decryption becomes possible. Excluding all mentions of encryption removes the notification exception that could plague other jurisdictions' untouched data breach laws once quantum computers can decrypt.[152] Once a breach has been discovered, "a reasonable and prompt investigation to determine the likelihood that personal identifying information has been or will be misused" could certainly point toward notification if a company determined that the hacker of encrypted data also had the technological capabilities to decrypt with quantum computing.[153] When data holders become aware of the danger posed by quantum decryption, they will need to acknowledge a real risk of misuse should malicious parties access any encrypted data moving forward.

The Wyoming statute still would not necessarily mandate retroactive reporting for encrypted data taken before quantum decryption because investigations start as soon as the data trustee "becomes aware of a breach of the security of the system."[154] Presumably, most prior investigations would have quickly closed given encryption's strong current security, and the law does not require reexamination. Still, unlike most jurisdictions, the Wyoming data breach notification law would almost certainly require notifications following the development of quantum decryption. This differs from the abandoned Tennessee model, because the relevant change in quantum capabilities would create an increase in notifications, making the heightened danger of data theft more noticeable to consumers.

While the many different data breach notification laws have their unique nuances, it appears that they will collectively fail to require meaningful notifications about theft of encrypted personal information once quantum computers have decryption

152. *See* WYO. STAT. ANN. § 40-12-501 (2022) (defining a security breach as "unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal identifying information").

153. WYO. STAT. ANN. § 40-12-502 (2022).

154. *Id.*

capacities. Certainly, these statutes set only a lower bound for data holder responsibility, and the data trustees might independently rise to the occasion and choose to issue nonmandatory notices.[155] But betting on companies to act in a manner that might be against their best interest could certainly backfire.[156] Changes to the national data breach notification law landscape must be considered and enacted in anticipation of quantum decryption to minimize its potential harm.

V. A PROPOSED FEDERAL DATA BREACH NOTIFICATION FRAMEWORK BETTER SITUATED TO HANDLE QUANTUM ENCRYPTION

Because the emergence of quantum encryption would pose a security threat to the personal information of all American citizens, a federal data breach notification statute might provide the most efficient and effective means to address holes in the current state-law patchwork. Roughly fifteen years passed between California adopting the first data breach notification law and Alabama, the last holdout, passing its own.[157] Such a prolonged timeline on these laws' inductions indicates that individual adjustments to every jurisdiction's statute would move far too slowly to adequately address the problem. Of

155. A commitment to notify people about the security of company-owned data could be construed as falling under the broad umbrella of corporate social responsibility (CSR). *See* Brian Edmondson, *What Is Corporate Social Responsibility?*, BALANCE, https://perma.cc/89V3-22EL (last updated Oct. 20, 2021) ("Corporate social responsibility can refer to any effort to improve a company's eco-friendliness and increase its social impact."). Evidence supports the notion that engaging in CSR can benefit companies, so generous reporting might be a wise business decision. STEVE ROCHLIN ET AL., PROJECT ROI 17–20 (2015), https://perma.cc/JQ7X-SFZ2 (documenting various benefits of CSR including customer satisfaction, employee satisfaction, and higher sales volumes).

156. *See, e.g.*, *IBM Study Shows Data Breach Costs on the Rise*, *supra* note 45 (finding that companies face steep financial consequences when they report a data breach).

157. *See* Elizabeth Larson, *New Legislation to Strengthen Data Breach Notification Law*, LAKE CNTY. NEWS (Feb. 25, 2019, 12:42 AM), https://perma.cc/J973-38C6 (highlighting that California passed the first data breach notification law in 2003); *Data Breach Notification Effective June 1 in Alabama*, ALA. RETAIL (Mar. 28, 2018), https://perma.cc/2B8N-FYRL (proclaiming passage of Alabama's data breach notification law in 2018, and recognizing it as the fiftieth state to codify one).

course, every jurisdiction should still attempt to fix any weaknesses within its own laws, but a blanket nationwide data breach notification that answers to concerns about under-notification due to quantum decryption would provide much needed protection to constituents of jurisdictions that drag their feet in implementing desirable updates.

Although no federal data breach notification law currently exists, federal legislators have periodically expressed interest in passing one.[158] Historically, debate over whether a federal law would preempt state data breach notification laws has created a point of contention and prevented necessary congressional consensus.[159] Some have argued that preemption is necessary because implementing a single data breach notification statute would create simplicity and help data holders with limited financial capacity comply with numerous confusing legal reporting requirements.[160] Others worry that a federal body would not willingly adopt stronger data breach notification protections than already-existing local equivalents.[161] For some

158. *See* S. REP. NO. 111-290, at 1 (2010) (providing the Senate Committee on the Judiciary's recommendation to pass Senate Bill 139 which would have codified a federal data breach notification law); Data Security and Breach Notification Act, S. 2179, 115th Cong. (2017) ("A [b]ill [t]o protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a breach of security.").

159. *See* Grant Gross, *Lawmakers Push for Federal Data Breach Notification Law*, PC WORLD (July 18, 2013, 12:42 PM), https://perma.cc/9RLR-MJ4N ("The debate over whether a national law should preempt state laws . . . has held up a national breach notification bill in Congress for years . . . .").

160. *See* Cameron F. Kerry & John B. Morris, Jr., *Preemption: A Balanced National Approach to Protecting All Americans' Privacy*, BROOKINGS (June 29, 2020), https://perma.cc/DP2T-VR5D (acknowledging that selective or incomplete preemption would undermine "the goal of a national standard for privacy practices, compliance systems and consumer expectations").

161. *See* Letter from the Nat'l Ass'n of Att'ys Gen. to Congress (July 7, 2015), https://perma.cc/MXT4-PXVQ (asserting the concern of forty-seven state attorneys general that "[p]reempting state law would make consumers less protected than they are right now" and that "[i]f states are limited by federal legislation, [they] will be unable to respond to [consumer] concerns"); *Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?: Hearing Before the Subcomm. on Com., Mfg., & Trade of the H. Comm. on Energy & Com.*, 113th Cong. 3 (2013) (statement of Janice D. Schakowsky, Ill. Rep.), https://perma.cc/AH54-JTBR ("[M]y view is that any federal law should not weaken strong State laws. In addition, any federal response should

citizens, preemption by a weaker federal statute would mark an undesirable step in the wrong direction.[162] Indeed, the idea that federal preemption can permit actors to engage in bad behavior that local jurisdictions have already curtailed is not new in the sphere of cyber regulation.[163]

Because this Note primarily focuses on the issue of whether data breach notification laws adequately protect against the impending threat of quantum decryption, concerns about the current costs of differing state laws take a backseat. With over fifty different data breach notification laws already in effect, adding one more in the form of a non-preemptive federal statute would not create complexity issues so much as it would fail to address them. In an ideal world, a federal data breach notification law would provide far stronger protections than any state equivalent. In that scenario, preemption would have no drawbacks and emerge as the obvious choice. Recognizing the improbability of such action, a federal data breach notification law that supersedes its state counterparts only if the local statute affords less protection would provide the greatest opportunity to address the quantum decryption problem.

Beyond the advantage of universal coverage, a federal data breach notification law would provide greater protection against quantum decryption because a singular federal decisionmaker empowered to make determinations about the dangers presented by quantum computing would likely have the best access to guiding information. Specifically, state officials or individual data holders will not be able to as effectively evaluate when public-key encryption will no longer provide adequate protection, triggering alerts under hypothetically updated data breach notification laws. As a threshold matter, laypeople might have difficulty identifying if a quantum computer capable of compromising encryption has been made, particularly because

---

establish a baseline so that every American can be assured some level of data protection, not just notification after the fact."); *id.* at 6 (statement of Henry A. Waxman, Cal. Rep.) ("[F]ederal legislation must not move backward by undermining those States with strong breach notification laws.").

162. *Id.*

163. *See generally* OpenRisk, LLC v. MicroStrategy Servs. Corp., 876 F.3d 518 (4th Cir. 2017) (determining that the federal Copyright Act preempts state conversion and computer fraud claims under the Virginia Computer Crimes Act).

other competitors in the quantum race will want to cast doubt on potential successes of their rivals.[164] A central authority might have stronger expertise to sift through conflicting accounts. Such an actor would also be better situated to access information about quantum developments that are not made available to the American public. Intelligence on the developments of hostile foreign powers, or even within domestic government labs might not be widely circulated.[165]

Once a quantum computer capable of factoring is recognized to have been built, decisionmakers would still need to determine at what point it actually threatens personal information and merits notification required by law. Developers of a quantum computer will surely be familiar with the classic science fiction trope examining the moral concerns and horrible outcomes of humans developing technology that society is not prepared for.[166] To that end, the developers of a factoring quantum computer might not willingly choose to share their machine after contemplating its ethical implications.[167] Are data breach notifications necessary for a technological advancement contained to a single lab? Perhaps not.

---

164. *See* Marr, *supra* note 118 (documenting an instance in which Google claimed to have made a significant advance with its quantum computing program and IBM immediately pushed back by casting doubt on the validity of Google's assertion).

165. The United States and China have invested heavily in quantum development. *See supra* note 115 and accompanying text. Indeed, quantum development has been likened to a modern space race. *See* Walter G. Johnson, Comment, *Governance Tools for the Second Quantum Revolution*, 59 JURIMETRICS J. 487, 489–92 (2019) (discussing the race for quantum developments and the corresponding concern about potential harm it could present to national security). Suffice it to say, government actors will pay close attention as this unfolds. *Id.* at 497–98 (noting NSA interest in quantum decryption, and leak of that information by Edward Snowden).

166. *See, e.g.*, EX MACHINA (Universal Pictures 2014) (examining how advanced AI could challenge the notion of what it means to be human and demonstrating what could go wrong if human-like AI is developed before that question is answered); MINORITY REPORT (20th Century Fox 2002) (imagining a world in which advanced technology results in false criminal convictions for innocent people).

167. *See* David B. Resnik & Kevin C. Elliott, *The Ethical Challenges of Socially Responsible Science*, 23 ACCOUNTABILITY RSCH. 31, 38–39 (2016) (advocating for socially responsible dissemination of scientific discovery and providing examples of how virology research is vetted over concerns that it might be used for terrorism before release).

But that begs the follow-up question, what is the threshold at which quantum computing has spread enough to demand these notifications? The answer to that concern is murky now, and unlikely to become clear even as technology develops. If widespread access and use of quantum computers maps onto the proliferation of classical computers, decades might pass between the creation of a factoring quantum machine and its presence in most households.[168] However, classical computers grew more powerful at an exponential clip for decades.[169] Viewed as the natural extension of classical computing, one might expect rollout of quantum computers to occur at a prodigious rate.[170] Quantum decryption could also become widely available on a much shorter timeline than it took for public access to classical computers because of cloud computing—the act of outsourcing storage of data or expensive computations to powerful machines via the internet.[171] Some pioneers in the industry have already developed a business model around allowing interested businesses to purchase cloud access to their quantum computers.[172] Theoretically, a malicious party could rent quantum computing capacity to decrypt stockpiled data.

Regardless of the actual threat timeline, if individual data holders or states must independently assess when quantum decryption has developed or access to it has spread enough to

168. *See* Timothy Williamson, *History of Computers: A Brief Timeline*, LIVE SCI. (Dec. 1, 2021), https://perma.cc/JGS6-93WW (demonstrating the prolonged timeline over which people conceived the idea of a computer, first models were built, and computers became commonplace).

169. *See* Carla Tardi, *Moore's Law*, INVESTOPEDIA, https://perma.cc/U5M7-BCT8 (last updated Feb. 23, 2021) (defining Moore's Law as the "perception that the number of transistors on a microchip doubles every two years," and noting that it has roughly held true since Moore first contemplated it in 1965).

170. *See id.* (acknowledging that physical impediments to continued advancements of processing power might be quickly approaching and suggesting quantum physics as a potential path forward).

171. *See* Eric Griffith, *What Is Cloud Computing?*, PC MAG., https://perma.cc/4K4H-ZP93 (last updated June 29, 2020) (providing a basic overview of how cloud computing works and various ways in which it is currently used).

172. *See* Stephen Shankland, *Microsoft Opens Its Azure Quantum Computer Cloud Service to the Public*, CNET (Feb. 1, 2021, 12:00 PM), https://perma.cc/K87F-EQRV (last updated Feb. 3, 2021, 9:59 AM) (reporting on Microsoft's public commercialization of a quantum-computing cloud with Azure Cloud, and how it has joined Amazon, Google, and IBM, which also all provide quantum services over the cloud).

require notification under varying data breach notification laws, they will inevitably reach different conclusions. Empowering an actor at the federal level to unilaterally decide when quantum decryption has become an issue would provide the benefit of a uniform interpretation made by an actor with access to the expertise and information needed to adequately evaluate the problem. The National Institute of Standards and Technology (NIST) currently "develops and disseminates the standards that allow technology to work seamlessly and business to operate smoothly," making it a prime candidate to assume these duties.[173]

To sufficiently address quantum decryption, a federal data breach notification law would need to provide notifications for personal data that had not been compromised prior to quantum advancement but will become readable afterwards. That would require data holders to be prepared to tell people what personal information quantum decryption could potentially compromise. To address that issue, this Note proposes that the statute define a breach of personal information without mention of encryption or any other exclusion, like in the California model.[174] It should also require data owners to hold some record of what personal information they have held about a person for a fixed number of years. Finally, the statute should contain provisions that require notification, both forward- and backward- facing, at tiered thresholds based on readability in alignment with concrete technological milestones.

Keeping the definition of what constitutes a breach separate from any reporting exclusion helps ensure that a possibility for future notifications is not foreclosed by a present exclusion that could become obsolete. As discussed previously, many current state data breach notification laws define a breach such that none has occurred if only encrypted data was stolen.[175] This method fails to register the possibility of future technological developments rendering that encrypted data readable.[176] In such instances, issuing a notification would be desirable, but it is impossible to point to any "breach" that could

173. *Standards: Overview*, NIST, https://perma.cc/JVR4-W5CX.

174. *See supra* Part II.C.

175. *See supra* notes 56–62 and accompanying text.

176. *See supra* notes 134–138, 145–148 and accompanying text.

form the basis of the alert.[177] A federal data breach notification statute aiming to curb the harm of quantum decryption should separate any reporting exception from the definition of a breach to avoid this problem.

Next, the statute must require data owners to keep record of the data they have held for a set period of time. Having accepted the premise that breaches today could yield compromises of personal information in the future as technology develops, data trustees must know what information could have been taken if they are to be expected to provide people with meaningful notification down the road. Of course, preventing data trustees from destroying unneeded data would perpetuate the possibility of the data itself being stolen.[178] Thus, the statute should emphasize preserving records of the type of data held as opposed to the actual information itself. For example, keeping note of the fact that a company once held Jane Doe's social security number is easier and less dangerous than preserving the nine-digit number itself. In this way, a federal data breach notification statute could ensure that data trustees retain sufficient records to alert people if future developments render their personal data compromised, while limiting relative risk and costs.

In fact, Congress could determine that some data records might not need to be preserved indefinitely. Most banks require credit-card replacements every few years.[179] Consequently, there would be no reason to require data holders to keep record of a credit-card number indefinitely. Forced information obsolescence, as exemplified by credit-card numbers, might lessen the eventual impact of quantum factoring by making old, encrypted data mines useless, although readable. An ideal federal data breach notification statute could encourage a higher velocity of data obsolescence by loosening reporting and

177. *See supra* notes 134–138, 145–148 and accompanying text.

178. *See* George Platsis, *Data Destruction: Importance and Best Practices*, SEC. INTEL. (Nov. 19, 2020), https://perma.cc/RHL8-3BRG (observing that a data holder might desire to get rid of data for various reasons and outlining multiple ways to destroy the data so that it is never in danger of becoming recovered and compromised).

179. *See What to Expect When Your Capital One Credit Card Expires*, CAP. ONE (Mar. 13, 2020), https://perma.cc/K4XF-9XZ5 ("Credit cards generally need to be replaced every three to five years, depending on the issuer.").

record-keeping requirements when updates have made older information useless.

Picture this in the context of passwords: most organizations encourage password changes every few months to reduce the useful life of a hacked password.[180] Acquiring an old password might not grant immediate access to a system, but given many people's bad habit of making slight changes to existing passwords in updates, it could provide valuable information in guessing current passwords.[181] However, if the velocity of password changes increases, perhaps requiring updates on a weekly or even daily basis, then any given individual old password becomes less useful, both because of its shorter lifespan and because, as iterations of a password expand, it becomes more difficult to keep varying the password in predictable ways. Many pieces of information are static, like social security numbers.[182] But to the extent possible, constantly refreshing information might lessen the potential fallout from quantum decryption. Indeed, the greatest defense against problematic future decryption of current data is a simple reduction in the sheer volume of data presently collected.[183] Data that does not exist cannot be abused. Even if a federal data breach notification law could not completely force an increase in the velocity of information obsolescence, encouraging one by limiting records retained by data holders to possession of useful information could provide a helpful incentive.

---

180. *See* Dave Johnson, *How Often You Should Change Your Passwords, According to Cybersecurity Experts*, BUS. INSIDER (June 26, 2020, 10:07 AM), https://perma.cc/H6GV-J6TD (stating that "conventional wisdom holds that you should change your passwords every few months" to minimize the window in which a cybercriminal could use a compromised password).

181. *See* Lorrie Cranor, *Time to Rethink Mandatory Password Changes*, FTC (Mar. 2, 2016, 10:55 AM), https://perma.cc/GB8F-TLTT ("[U]sers who are required to change their passwords frequently select weaker passwords to begin with, and then change them in predictable ways that attackers can guess easily.").

182. *See Can I Change My Social Security Number*, SOC. SEC. ADMIN., https://perma.cc/UF3P-JFS6 (last updated Nov. 30, 2019) (detailing very limited circumstances under which a social security number can be changed).

183. *See* FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD iv (2015), https://perma.cc/BL3U-MEPU (urging data minimization because it decreases potential harm in the event of a data breach and decreases risk of data use in defiance of reasonable consumer expectations).

The data breach notification statute should next empower an expert entity to universally determine when quantum decryption has conquered public-key encryption. At that point, data-holders will need to issue backward-looking breach notifications based on their records. Rather than having data trustees contact individuals, the statute might function better by having the data owners send their records to a government entity that then compiles and distributes the information.[184] A single notification with every potential compromise of personal information could reinforce the sobering gravity of this development. It would also save consumers from a barrage of separate notifications that could be ignored as spam.

Once the statute has established what reporting responsibilities exist when quantum computing technologies debut, it will need to specify protocols for notification in the subsequent period of uncertainty. Quantum encryption protocols have been discovered, but they require all involved parties to use their own quantum machine.[185] Essentially, online communication will not be fully secure until classical computers have phased out and quantum computers become ubiquitous. If the data breach notification law requires notification in the interim for every breach of insecure personal data, then it will effectively collapse into the abandoned Tennessee statute.[186] If

184. Regulations stemming from Singapore's data breach notification statute have implemented a system in which all breaches must be reported to a centralized authority regardless of whether notifications will be sent to affected individuals. Personal Data Protection (Notification of Data Breaches) Regulations 2021 (GN No. S 64/2021) (Sing.). This model might be used as a framework for consolidating information in preparation of the necessary backward reporting.

185. *See* RIEFFEL & POLAK, *supra* note 32, at 320–21 (explaining that some quantum cryptographic protocols have been developed that are unconditionally secure against attack through their reliance on fundamental properties of quantum mechanics); Charles H. Bennett & Gilles Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, 560 THEORETICAL COMPUT. SCI. 7, 9–10 (2014) (outlining the first quantum key distribution scheme, now known as BB84 after its authors and the year they originally published the paper). While the cloud might allow earlier access to quantum factoring, access to quantum computing through the cloud will not solve the issue of insecure communications. A classical computer would have no reliably secure way of sending confidential information to the cloud.

186. *See supra* Part II.D.

not, then there will be no reporting at all with universally insecure digital communication. Both scenarios are undesirable.

Of course, by that point reporting data breaches will be a relatively small issue compared to the damage caused by the widespread data theft necessitating these reports. Concerns about identity theft that spurred the initial adoption of state data breach notification laws will resurface, now both unchecked and uncheckable.[187] More troubling, no authenticated or secured transactions of any kind will be transmittable online. Compounding the problem, stockpiled data from years of encrypted data raids will suddenly become readable and conceivably fed into neural networks.[188] By limiting any ability for people to safely communicate remotely, quantum factoring could put an incredible strain on our society given its current reliance on the security of online transactions and interactions. This will affect everyone from the online shopper to the five-star general tasked with relaying a high-level military secret. A data breach notification law will not alleviate these issues, especially if it cannot encourage a safer alternative mode of communication once incessant notifications have conveyed the fact that digital interactions are insecure.

Perhaps the only way that a quantum decryption crisis might be avoided is if a protocol similar to traditional public-key encryption is discovered that is secure from both traditional and quantum attacks. If such an innovation is made, it would be imperative that society widely adopt this type of encryption to hold out any hope of weathering the chaos of a quantum-computing storm. For the past few years, NIST has been holding a competition for potential alternatives to current public-key encryption standards and to prepare for a quantum world.[189] Many remaining "post-quantum" contenders rely on a

187. *See supra* note 42 and accompanying text.

188. *See Quantum Computing and Cybersecurity*, *supra* note 124 https://perma.cc/TT7J-PZRX ("[E]ncryption must be secured against Quantum Computers even before these exist, as encrypted data can be saved and decrypted at a later point in time."); Ben Dickson, *The Security Threats of Neural Networks and Deep Learning Algorithms*, TECHTALKS (Dec. 27, 2018), https://perma.cc/C9E9-QUJ8 (explaining the dangers of neural networks and deep learning).

189. *See Post Quantum Cryptography Project Overview*, NIST (Jan. 3, 2017), https://perma.cc/AW9T-DLN8 (last updated Dec. 2, 2021) (providing background on the competition).

lattice-based approach to cryptography.[190] While no method for cracking lattice-based encryption with quantum computers has been discovered, it also has not been mathematically proven that this form of encryption is impervious to quantum computers.[191]

Considering these efforts, a federal data breach notification law could contain an explicit exception to notifications, both forward- and backward- looking, for data protected by an approved post-quantum encryption method. On one hand, this could encourage adoption of much-needed new encryption standards blunting the impact of quantum decryption. On the other hand, as this Note has demonstrated, creating a contingency in law based on the assumption that difficult math problems will remain insoluble generates an avenue for that legal framework to crumble as technology advances, nullifying the difficulty evaluation. Data breach notification laws must not allow data holders to hide in the shadows of protective measures that are or will soon be penetrable. Instead of incorporating another concrete exception, a new federal data breach notification statute needs to tie notifications to readability and delegate the decision of what that looks like to experts capable of prescribing a fluctuating standard. That determination should require notifications mindful of past encrypted data that has become insecure and should look to the future in setting current readability standards.

In summary, the impending realization of quantum decryption threatens to radically disrupt efficacy of the current state-level data breach notification patchwork. To soften the impact of this development, data breach notification laws should separate any reference of encryption from the definition of a breach to require alerts corresponding to past breaches made presently harmful by shifts in relative encryption security. Reporting must be tied to a shifting standard of readability as

190. *See* Jeremy Kahn, *Quantum Computers Threaten to End Digital Security. Here's What's Being Done About It*, FORTUNE (Sept. 11, 2020, 8:00 AM), https://perma.cc/6B2J-2U7E (discussing finalists for post-quantum encryption in the NIST competition).

191. *See id.* ("'We say that quantum algorithms cannot break them *yet*,' Delaram Kahrobaei, a professor of cybersecurity at the University of York, in England, says. 'But tomorrow someone comes up with another quantum algorithm that might break them.'").

determined by an independent expert authority. Statutes should require that data holders keep accurate records of data that they have held so that they can issue comprehensive notifications regarding past breaches. The federal government is best situated to implement these changes by issuing its own data breach notification law, both because of its broad jurisdiction and because of its better access to relevant information on the state of technological advancements.

CONCLUSION

Our society relies on encryption to protect our daily digital activities.[192] When data holders fail in their duties to protect people's personal information, data breach notification laws require them to notify affected parties so that they might take damage-mitigating action.[193] Because legislators codified explicit exceptions to notification for encrypted data breaches, data breach notification laws put unwarranted faith in the continued difficulty of public-key encryption's underlying mechanisms.[194] Mathematicians have already developed quantum algorithms capable of rendering current encryption methods useless.[195] Engineers have made considerable strides towards creating a machine able to facilitate these operations.[196] Once a strong enough quantum computer has been realized, modern encryption will fail, effectively bringing current data breach notification laws down with it.[197]

Quantum decryption will have ripple effects in many facets of daily life and the law. Preemptively changing the data breach notification framework could provide one small contribution to dampen this huge impact. Specifically, opening greater avenues for retroactive reporting will help the public better appreciate the magnitude of danger from quantum decryption. People could adjust their behavior by taking greater precautions with their personal data. Reporting requirements that emphasize a moving threshold of readability could help encourage more rapid

192. *See supra* Part I.
193. *See supra* Part II.
194. *See supra* Part III.
195. *See supra* notes 108–110 and accompanying text.
196. *See supra* notes 111–123 and accompanying text.
197. *See supra* notes 122–123 and accompanying text.

adoption of post-quantum encryption as it becomes viable.[198] Data breach notification statutes alone cannot fully protect against a quantum future. But policymakers must prepare now to soften the inevitable blow to society that quantum computers will cause. An updated data breach notification framework provides one tool toward accomplishing that end.

198. *See supra* Part V.