Washington and Lee Law Review

Volume 79 | Issue 1 Article 12

Winter 2022

Comment: The Necessary Evolution of State Data Breach Notification Laws: Keeping Pace with New Cyber Threats, Quantum Decryption, and the Rapid Expansion of Technology

Beth Burgin Waller
Woods Rogers PLC, bwaller@woodsrogers.com

Elaine McCafferty
Woods Rogers PLC, emccafferty@woodsrogers.com

Comment: The Necessary Evolution of State Data Breach Notification Laws: Keeping Pace with New Cyber Threats, Quantum Decryption, and the Rapid Expansion of Technology

Beth Burgin Waller* and Elaine McCafferty**

Table of Contents

INTRODUCTION 522

I. EMERGING THREATS HAVE UPENDED DATA BREACH NOTIFICATION LAWS 522

II. STATE DATA BREACH STATUTES FAIL TO ADDRESS AUTOMATED WIDESPREAD ACCESS AND UNCLEAR ACQUISITION 525

III. EVOLUTION OF TECHNOLOGY, INCLUDING QUANTUM COMPUTING, REQUIRES CHANGES TO THE CURRENT STATE DATA BREACH NOTIFICATION REGIME 527

IV. THE PUSH FOR FEDERAL LEGISLATION TO UNIFY A NOTICE STANDARD AND ADDRESS THESE CONCERNS 529

* Principal, Chair of Cybersecurity & Data Privacy Practice, Woods Rogers PLC; J.D., William & Mary Marshall-Wythe School of Law; B.A., Hollins University.

** Associate, Woods Rogers PLC; J.D., Washington and Lee University School of Law; B.A., University of Connecticut.

INTRODUCTION

The legal framework that was built almost two decades ago now struggles to keep pace with the rapid expansion of technology, including quantum computing and artificial intelligence, and an ever-evolving cyber threat landscape. In 2002, California passed the first data breach notification law, with all fifty states following suit to require notice of unauthorized access to and acquisition of an individual's personal information.[1] These data breach notification laws, originally designed to capture one-off unauthorized views of data in a computerized database, were not built to address PowerShell scripts by cyber terrorists run across thousands of servers, leaving automated accessed data in their wake. Similarly, the safe harbors for encryption built into these statutes were not designed with quantum computing and its possibility of quantum decryption in mind. These evolving technologies and threats require that state data breach notification laws be reformulated for a modern era. This Comment examines the interplay between these challenges and discusses a path forward.

I. EMERGING THREATS HAVE UPENDED DATA BREACH NOTIFICATION LAWS

A myriad of exploited threat vectors have emerged in the two decades since California passed the first data breach notification law. Most recently, the proliferation of ransomware, and, in particular, double extortion ransomware, has emerged as a scourge to society. Ransomware "is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and systems that rely on them unusable," unless a ransom is paid in exchange for a decryption key.[2] In the case of double extortion ransomware, threat actors go beyond encrypting data in place by also exporting victim data for sale or threatening

1. Phillip Harmon, *Data Breach Notification Laws and the Quantum Decryption Problem*, 79 WASH. & LEE L. REV. 471, 479 (2022).

2. *Ransomware 101*, STOP RANSOMWARE, https://perma.cc/V5TA-9HMS.

publication as blackmail.[3] In 2019, a group of cyber-criminal pioneers, known as the "Maze" group, instigated the first published double extortion case involving Allied Universal, a security staffing company based in the United States.[4] News articles in 2019 called this a "game-changing blackmail model."[5] In the case of Allied Universal, Maze reportedly stole 7 GB worth of data prior to executing their encryption tactics to encrypt the Allied Universal network.[6] Maze then approached their victim demanding 300 bitcoins, valued at approximately $2.6 million at the time.[7] When the victim refused to pay, Maze published 700 MB of data on a Russian hacking forum on the dark web.[8] This reflected approximately "10% of the [data] stolen" and, after posting, Maze contacted the information security magazine, *Bleeping Computer*, to share information about the heist.[9] Maze, in writing to *Bleeping Computer*, claimed it was "writing to you because we have breached Allied Universal security firm (aus.com), downloaded data and executed Maze ransomware in their network."[10]

Cyber-criminal gangs soon began to follow Maze's method of double extortion. Groups began offering "ransomware-as-a-service" or RaaS, with threat groups offering malware and infrastructure in exchange for a fee or profit

3. *See* Janus Agcaoili et al., *Ransomware Double Extortion and Beyond: REvil, Clop, and Conti*, TREND MICRO (June 15, 2021), https://perma.cc/Q5VG-77D9; *Ransomware 101*, *supra* note 2; *see also* Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://perma.cc/9SFW-Q4AN (describing the ten most common pieces of information sold on the dark web with prices that range from $1 to $2,000).

4. *Ransomware Evolved: Double Extortion*, CHECK POINT RSCH. (Apr. 16, 2020), https://perma.cc/4VWZ-G3RM.

5. Muhammad Hamza Shahid, *Ransomware Adopts a Game-Changing Blackmail Model for Information Theft*, INFO SEC. (July 24, 2020), https://perma.cc/5M9V-7R6E.

6. *Id.*

7. *Id.*

8. *Id.*

9. Lawrence Abrams, *Allied Universal Breached by Maze Ransomware, Stolen Data Leaked*, BLEEPING COMPUT. (Nov. 21, 2019, 10:48 PM), https://perma.cc/38VJ-ELBG (explaining that Bleeping Computer received an email signed "Maze Crew" reporting the theft and stating that Maze group "always exfiltrate[s], or steal[s], a victim's files" before it encrypts any computer).

10. *Id.*

sharing.[11] Cyber-criminal cartels—cyber criminals operating Soprano's-style gang families—began to emerge, both locking data and stealing it.[12]

The threat actors employ sophisticated tactics to execute their malicious activity, often utilizing software scripts to execute the removal of data and utilizing anti-forensic techniques to hide their tracks.[13] For example, the PYSA ransomware operation uses a PowerShell script set to execute across a victim's network, gathering up any file that hits on search terms such as "SSN," "bank*statement," or "W-2."[14] A PowerShell "is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework."[15] In other words, it is an automated line of coding designed by non-malicious or malicious software coders to execute a function on a device. In the case of PYSA, or a similar threat actor group, after entering a victim organization's environment undetected, they run a PowerShell script to gather up and remove documents from the victim network for later use on a shame website.[16] The PowerShell script runs automatically, canvassing files using search terms and ultimately exporting a subset of data to the threat actor.[17]

Using a script results in potential "access" to thousands of files across the entirety of an organization's servers. In many instances, it may be impossible to discern whether these files were ever viewed by a real person or just technically modified using a software script. Similarly, there are often limits on an organization's knowledge of whether the data accessed by the

11. Stu Sjouwerman, *Ransomware Gangs: Who Are They and How to Stop Them*, FORBES (Sept. 27, 2021, 9:15 AM), https://perma.cc/BS7U-JTXA (noting the "U.S. government has elevated ransomware threats to a level of priority similar to that of terrorism").

12. *See id*. ("The FBI is monitoring more than 100 active ransomware gangs . . . .").

13. Lawrence Abrams, *Ransomware Gang's Script Shows Exactly the Files They're After*, BLEEPING COMPUT. (Aug. 24, 2021, 2:16 PM) [hereinafter *Abrams*, *Ransomware Gang*] , https://perma.cc/9R85-CPDT.

14. *Id*.

15. *What Is Powershell?*, MICROSOFT (Oct. 5, 2021), https://perma.cc/ES7S-ZT5B.

16. *See Abrams*, *Ransomware Gang*, *supra* note 13.

17. *Id.*

script left the network. If the modified or accessed files contain personal identifying information, the question becomes whether this automated script access is enough to trigger a data breach notification to an individual.

These new threat tactics—removing data by automated means using software scripting—must be reconciled with data breach notification laws that were written in a much simpler time of cybercrime. As discussed in Part III, these laws were not drafted with these largescale automated searches in mind.

II. STATE DATA BREACH STATUTES FAIL TO ADDRESS AUTOMATED WIDESPREAD ACCESS AND UNCLEAR ACQUISITION

"Breach notification laws have been a major driver of data protection efforts in U.S. organizations for more than a decade."[18] These laws serve a laudable purpose: they require custodians of personal information to inform individuals when their personal information has been compromised so that they can take steps to protect themselves from identity theft.[19] But achieving this end can be challenging because the conditions that trigger the duty to notify are not well defined.

With respect to these conditions, data breach notification laws can be divided into two categories. Most data breach laws require notification when "unauthorized acquisition" of personal information occurs.[20] Other statutes require notification when "unauthorized acquisition and access" occurs.[21] However, because acquisition cannot occur without access, these statutes can be grouped together. In a minority of states, the duty to notify is triggered by events that include "unauthorized access"

18. David Thaw, *Data Breach (Regulatory) Effects*, 2015 CARDOZO L. REV. DE-NOVO 151, 151 (2015).

19. *See* Harmon, *supra* note 1, at 479 ("Data breach notification laws have the dual purpose of protecting private citizens and holding data owners accountable").

20. *See* LIISA M. THOMAS, THOMAS ON DATA BREACH: A PRACTICAL GUIDE TO HANDLING DATA BREACH NOTIFICATIONS WORLDWIDE § 2:25 (2020) (listing state statutes that define a security breach as an unauthorized acquisition of personal information).

21. *Id.*; *see, e.g.*, VA. CODE ANN. § 18.2-186.6 (2021) ("'Breach of the security of the system' means the unauthorized access and acquisition of unencrypted and unredacted computerized data . . . .").

to personal information.[22] Thus, state data breach statutes fall into two categories: the majority approach, which requires both unauthorized access and acquisition to trigger notification, and the minority approach, which requires only unauthorized access.

While the minority approach may seem to offer greater protection than the majority approach, it presents compliance problems because threat actors are adept at disguising their access to security systems. Such access can often go undetected, even by sophisticated security systems, for months or years. As a result, the minority approach is essentially precatory in practice because complete compliance is not feasible.

The majority approach also presents compliance challenges because it is often unclear whether acquisition of personal information has occurred. Most data breach statutes do not define the terms "acquisition" or "acquired."[23] Vermont's data breach statute, one of the few exceptions, provides factors for determining whether personally identifiable information has been acquired, including: "(i) indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing brokered personal information; (ii) indications that the brokered personal information has been downloaded or copied; (iii) indications that the brokered personal information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or (iv) that the brokered personal information has been made public."[24]

With this guidance in mind, consider the following common cybersecurity event. A threat actor gains access to a system, running a PowerShell script across the network and touching files containing personal information, but there is no evidence either confirming or refuting that the information was

22. THOMAS, *supra* note 20, § 2:25; *see, e.g.*, N.J. STAT. ANN. § 56:8-161 (West 2021) ("'Breach of security' means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information . . . ."); CONN. GEN. STAT. § 36a-701b (2021) ("'[B]reach of security' means unauthorized access to *or* unauthorized acquisition of electronic files, media, databases or computerized data, containing personal information . . . ." (emphasis added)).

23. *See, e.g.*, VA. CODE ANN. § 18.2-186.6 (2021); ARIZ. REV. STAT. ANN. § 18-551 (2021); KAN. STAT. ANN. § 50-7a01 (2021).

24. VT. STAT. ANN. tit. 9, § 2430 (2022).

transferred by the threat actor. Under Vermont's statute, does the absence of evidence of downloading or copying mean no information was acquired? Reasonable minds can differ when answering this question, which makes compliance with this statute difficult and uniform application unlikely. This problem is compounded by statutes that offer no guidance on the meaning of "acquired" and demonstrates why data breach statutes are ripe for revision.

III. EVOLUTION OF TECHNOLOGY, INCLUDING QUANTUM COMPUTING, REQUIRES CHANGES TO THE CURRENT STATE DATA BREACH NOTIFICATION REGIME

The evolution of encryption and, specifically, quantum decryption technology, also exposes the need to transform data breach notification laws to fit a modern era. In his Note, *Data Breach Notification Laws and the Quantum Decryption Problem,* Phillip Harmon argues that "the impending realization of quantum decryption threatens to radically disrupt efficacy of the current state-level data breach notification patchwork."[25]

Large-scale quantum computers threaten to turn the safety of encrypting messages on its head.[26] Indeed, the risk is so grave that beginning in 2016, the National Institute of Standards and Technology (NIST) "initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms."[27] The race is on, essentially, with "the goal of post-quantum cryptography (also called quantum-resistant cryptography) [being] to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks."[28]

---

25. *See* Harmon, *supra* note 1, at 513.

26. *See Post-Quantum Cryptography*, NIST (Jan. 3, 2017), https://perma.cc/44RC-SYE4 (last updated Dec. 2, 2021) ("If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere.").

27. *Id.*

28. *Id.* (emphasis omitted).

Many state data breach notification statutes were designed with a safe harbor for encryption of data. For example, Virginia's data breach notification statute provides that "breach of the security of the system" is defined as

> the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth.[29]

The Commonwealth defines "encrypted" as the "transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable."[30]

As Harmon points out in his Note, in the age of quantum computing, with quantum decryption looming, how does one consider a statute like Virginia's that speaks to the "low probability of assigning meaning without the use of"[31] a decryption key?

Harmon addresses a number of issues related to quantum decryption technologies in his Note. Harmon concludes that "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."[32] Similarly, he argues that "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."[33]

---

29. VA. CODE ANN. § 18.2-186.6 (2021).
30. *Id.*
31. *Id.*
32. Harmon, *supra* note 1, at 513.
33. *Id.* at 514.

Though changes to data breach notification laws were proposed in 2021, those proposed changes are modest.[34] The National Conference of State Legislatures notes that in 2021 the trends included legislation that would "[e]stablish or shorten the time frame within which an entity must report a breach"; "[r]equire state or local government entities to report data breaches"; "provide an affirmative defense for entities that had reasonable security practices in place at the time of a breach"; "[e]xpand definitions of 'personal information' (e.g., to include biometric information, health information, etc.)"; and "require private sector entities to report breaches to the state attorney general or other state entity."[35]

What are absent from these 2021 legislative changes are amendments to capture an evolving threat landscape coupled with evolving technologies. These state data breach notification laws effectively create a patchwork quilt of requirements that national businesses and organizations must navigate, law by law, in the midst of a large-scale consumer data breach. The result can be that the same incident may give rise to notification requirements under one state law but not the other, with similarly situated consumers in different states facing wildly different outcomes.

IV. THE PUSH FOR FEDERAL LEGISLATION TO UNIFY A NOTICE STANDARD AND ADDRESS THESE CONCERNS

The best path forward to address these concerns may be the implementation of a federal data breach notification standard. Sectorial federal notification requirements are in place, depending on the industry, with the granddaddy of such legislation being the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[36] Harmon concludes that "[t]he federal government is best situated to implement these

34. *2021 Security Breach Legislation*, NAT'L CONF. OF ST. LEGISLATURES (Jan. 12, 2021), https://perma.cc/V79D-FR8H (describing common trends in state data breach notification legislation).

35. *Id.*

36. Pub. L. No. 104-191, 110 Stat. 1936 (1996); *see* 45 C.F.R. pt. 164 (2022). Even with HIPAA, challenges remain with regard to the definition of access in light of new technologies. *See* 45 C.F.R. § 164.402 (2022) (defining breach as the "acquisition, access, use, or disclosure of protected health information").

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."[37]

While data breach notification bills continue to be proposed at the federal level, none have advanced far in Congress, and they primarily address unifying requirements and notification timelines rather than access and evolving technologies.[38] For example, Senators Warner, Rubio, and Collins proposed the "Cyber Incident Notification Act of 2021"[39] which required certain covered entities to report cyber intrusions or potential cyber intrusions, within twenty-four hours. However, notably missing was a definition of cyber intrusion, which the Bill left up to rulemaking authorities.

Federal legislation aimed at addressing these concerns would be welcome but should equally be built with the flexibility to withstand emerging cyber incidents and technology.

37. Harmon, *supra* note 1, at 514.

38. *See* Maria Korolov, *Pressure Grows for Federal Data Breach Legislation*, DATA CTR. KNOWLEDGE (June 22, 2021), https://perma.cc/YDU4-WBES.

39. S. 2407, 117th Cong. (2021), https://perma.cc/LD39-PUX6 (PDF).