BREACH NOTIFICATION LAWS IN COLORADO: A POTENTIAL MODEL FOR OTHER STATES

Data breaches are slowly becoming a fact of life. In August 2013, Yahoo's databases were breached, leaking the information of three billion accounts.[1] At least 868 data breaches occurred in 2017 alone, revealing the records of well over 200 million people.[2] Just recently, on December 11th, 2017, news outlets began to pick up on a list of 1.4 billion passwords in plain text that was circulating the internet.[3] The regularity and cost[4] of these breaches has reignited the drive to reform the laws governing privacy, both on the national and state level.[5]

Privacy law in the United States takes a vastly different form compared to much of the rest of the world. In Europe, the right to privacy is regulated under the General Data Protection Regulation (GDPR).[6] The GDPR is a complex, demanding piece of legislation that goes a long way towards protecting the personally identifiable information of European citizens.[7] Instead of a single, uniform piece of legislation, the United States takes a checkerboard approach to the right to privacy.[8] Privacy protections are afforded by various agencies and authorizing statutes; including but not limited to the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), and the Department of Health and Human Services (HHS).[9] These federal agencies aim to protect the privacy rights of United States citizens through enforcement actions; however, the

1. Jim Finkle & Jonathan Stempel, *Yahoo says all three billion accounts hacked in 2013 data theft*, REUTERS (Oct. 3, 2017, 2:57 PM), https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1.

2. John DiGiacomo, *2017 Security Breaches: Frequency and Severity on the Rise*, REVISION LEGAL (Oct. 18, 2017), https://revisionlegal.com/data-breach/2017-security-breaches/.

3. Mohit Kumar, *Collection of 1.4 Billion Plain-Text Leaked Passwords Found Circulating Online*, THE HACKER NEWS (Dec. 11, 2017), https://thehackernews.com/2017/12/data-breach-password-list.html.

4. A 2017 study conducted by the Ponemon Institute calculated that cybercrime costs United States companies an average of $21.22 million each year, resulting from the 130 known security breaches taking place last year. This cost is the highest average cost in the world by a wide margin. Germany is in second place with an average cost to companies of $11.15 million. The United States is up from the 2016 average of $17.36 million per company. *2017 Cost of Cyber Crime Study,* PONEMON INSTITUTE LLC, Oct. 1, 2017, at 13, *available at* https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf.

5. *See* Colo. H.B. 1128, 71st Gen. Assemb., 2d. Reg. Sess. (Co. 2018); Tom Schatz, *Congress is walking the online privacy tightrope on oversight*, THE HILL (Apr. 24, 2018, 11:00 AM), http://thehill.com/opinion/technology/384589-congress-is-walking-the-online-privacy-tightrope-with-oversight.

6. Natasha Lomas, *WTF is GDPR?*, TECHCRUNCH (Jan. 20, 2018), https://techcrunch.com/2018/01/20/wtf-is-gdpr/.

7. *Id.*

8. Ieuan Jolly, DATA PROTECTION IN THE UNITED STATES: OVERVIEW, PRACTICAL LAW COUNTRY Q&A 6-502-0467, Westlaw (last updated July 1, 2017).

9. *Id.*

United States utilizes a dual-tiered system of federalism for privacy law.[10] As such, the responsibilities placed upon companies by federal agencies often coincide or even contradict the responsibilities derived from state governments.[11]

In this paper, I will explore the interplay between the FTC and the responsibilities placed upon companies by Colorado when it comes to cybersecurity practices and data breaches. I will begin by discussing the enabling statute for the FTC's adjudication of bad actors in the wake of a data breach. I will then turn to the data breach notification statute in Colorado and examine its strengths and weaknesses. I will conclude by analyzing the bill recently passed by the legislature which modified Colorado's breach notification law, including the weaknesses that the bill addresses and the changes that the bill makes to the notification timeline. This statute builds upon the data breach framework currently in place under the FTC, making Colorado's breach notification timeline one of the strictest in the nation. While the statute is a platform for other states to build upon, there are several changes that could be made which would strengthen consumer protections going into the future.

I. UNFAIR AND DECEPTIVE TRADE PRACTICES ADJUDICATED BY THE FTC

Several administrative agencies have the power to adjudicate violations of privacy law but the FTC is commonly understood as the privacy and data security police.[12] The FTC has the ability to adjudicate unfair and deceptive trade practices under Section 5 of the FTC Act.[13] This power has been construed to include adjudicating violations of privacy policies and instances of poor cybersecurity.[14] The power of the FTC to adjudicate actors with poor cybersecurity was vindicated by the Third Circuit in *FTC v. Wyndham Worldwide Corporation*.[15] In that case, Wyndham, a large hotel chain, had their computer systems breached three times over a short period.[16] Hackers infiltrated a property management system that had consumer information including names, home addresses, email addresses, phone numbers, payment account numbers, expiration dates, and security codes.[17] The treasure trove of information was unlocked by hackers using a brute force attack, a method that is easy to recognize and halt for any

10. *Id.*

11. *See* Miriam B. Russom et al., *Legal Concepts Meet Technology: A 50-State Survey of Privacy Laws*, U. ILL. CHI. (Dec. 6, 2011), https://www.cs.uic.edu/~sloan/papers/RussomEtAl50State-Survey.pdf.

12. William McGeveran, *Privacy and Data Protection Law*, 200–12 (2016).

13. 15 U.S.C. §45(5)(a) (2018); McGeveran, *supra* note 12.

14. Daniel JT McKenna, Odia Kagan, Andrew E. Kampf, *Third Circuit Rules That Ftc Can Regulate Cybersecurity Practices*, 68 CONSUMER FIN. L.Q. REP. 477, 477 (2014).

15. *Id.* at 477–479.

16. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 241–42 (3d Cir. 2015).

17. *Id.*

competent security professional.[18] Nevertheless, the security professionals at Wyndham did not spot the attack.[19] Despite Wyndham being put on notice by past breaches using the same method, hackers were able to acquire the information of 619,000 customers which resulted in at least $10.6 million in fraudulent charges.[20]

The Third Circuit held that Wyndham's cybersecurity practices fell within the plain meaning of "unfair," allowing the FTC to adjudicate Wyndham for an unfair and deceptive trade practice because of the company's poor cybersecurity.[21] An unfair trade practice is defined as a practice that results in a "substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[22] The unfair trade practice rule does not expressly require that an unfair trade practice be immoral, unethical, unscrupulous, or oppressive.[23] Here, the FTC posted on their website a guidebook of cybersecurity best practices and transcripts of adjudications of companies with security practices that fell well below the requisite standard.[24] The Third Circuit viewed these postings as notice to companies describing practices that will not survive review as adequate security measures.[25] Thus, the court ruled that Wyndham had fair notice of proper cybersecurity practices as long as the company could reasonably foresee that a court may construe its conduct as falling within the meaning of the statute.[26] That is, having poor cybersecurity practices presents a cost to consumers that outweighs the benefit to the company and competition.[27]

Wyndham is an example of a company being held accountable for atrocious cybersecurity practices or a material misrepresentation in the security measures available to customers, which is the essence of the FTC's enforcement actions when it comes to privacy and cybersecurity. The case is also an example of the limitations placed on the FTC acting under its authority to prosecute unfair and deceptive trade practices. Specifically, the FTC must bring the enforcement action while consumers can only report the wrongdoing, without the ability to file an action on their own.[28] Most importantly, the FTC may bring an action following a data breach for poor cybersecurity practices; however, the FTC does not necessarily mandate that the adjudicated company inform affected individuals that

18. *Id.* at 240–43.
19. *Id.*
20. *Id.* at 242.
21. *Id.* at 244–49.
22. 15 U.S.C. § 45(n) (2018).
23. *Wyndham*, 799 F.3d at 244.
24. *Id.* at 257–58.
25. *Id.*
26. *Id.* at 258–59.
27. *See id.* at 255–59.
28. *See* McGeveran, *supra* note 12.

their information was stolen.[29] This is because there is no national breach notification law; instead, there is a state-by-state approach to breach notification.[30]

II. COLORADO'S OLD BREACH NOTIFICATION LAW

Colorado's breach notification law is codified in Colo. Rev. Stat. § 6-1-716.[31] This statute sets out several definitions, including the definition of a data breach, which is described as:

> [The] unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or commercial entity for the purposes of the individual or commercial entity is not a breach of the security of the system if the personal information is not used for or is not subject to further unauthorized disclosure.[32]

This definition has several noteworthy points. First, a breach is defined as the "acquisition" of unencrypted data.[33] Colorado's definition differs from several other states, such as California's definition, which uses the lower standard of "access of unencrypted data."[34] Acquisition, which requires both access and data exfiltration, can be more difficult to prove, whereas proof of mere access to the information is a much lower standard.[35] Looking at the purpose of these statutes, to inform the public when their information is at risk, a lower standard for notification is the optimal way to ensure that this purpose is met. This purpose runs against the countervailing interest of the company to avoid customer panic and to maintain the public's trust. Nevertheless, forewarned is forearmed, and here the legislature decided to put business interests above the interest of the general public.

Second, this statute only pertains to the acquisition of unencrypted computerized data.[36] While many consider encryption to be a great bulwark standing against hackers, this notion is generally not the case.[37] The central premise of encryption is taking text that is intelligible and turning

---

29. Although breach notification is often the next step for a company being investigated by the FTC, there is no statutory requirement to do so under federal law. *See id.*

30. Russom et al., *supra* note 11.

31. COLO. REV. STAT. § 6-1-716 (2018).

32. *Id.* at 716(a).

33. *Id.*

34. CAL. CIV. CODE §§ 1798.29, 1798.82, 1798.84 (2018).

35. *See generally* Alex Reynolds, *GDPR matchup: US state data breach laws*, IAPP PRIVACY TRACKER (May 10, 2017), https://iapp.org/news/a/gdpr-match-up-u-s-state-data-breach-laws/.

36. § 6-1-716(a).

37. Computerphile, *Password Cracking - Computerphile*, YOUTUBE (July 13, 2016), https://www.youtube.com/watch?v=7U-RbOKanYs.

it into unintelligible text using some sort of cipher.[38] Presently, these ciphers are implemented using polynomial graphs, the points on which must be calculated before a result is received.[39] Depending on the points graphed, the result can be either intelligible or unintelligible.[40] Graphing points and checking whether the result is intelligible makes it extremely difficult for a computer to guess the secret passcode using any method other than brute force, requiring billions upon billions of attempts before the intelligible result is achieved.[41] Thus, we assume that the encrypted information is "secure," which is assumedly why the leak of encrypted information is outside of the scope of Colorado's breach notification law.

Colorado's general rule of providing notice to consumers when unencrypted computerized data is acquired has exceptions. One such exception includes when there is no reasonable likelihood of misuse.[42] It is a curious line for the legislature to draw: with the anonymity of IP addresses[43] how can one assess the likelihood of misuse? One potential low likelihood of misuse scenario is when a security researcher discloses the breach.[44] If the disclosure is made by security researcher, there is a tacit assumption that the security researcher is the first person to notice that the vulnerability exists.[45] Yet even in this scenario, there is no guarantee that the security researcher was the first to find the vulnerability; it could be the case that the vulnerability has been "in the wild" for a substantial

38. John P. Pullen, *Everything to Know About Encryption*, TIME (Feb. 16, 2016), http://time.com/4212068/encryption-what-is/.

39. A full explanation of precisely how modern encryption works unfortunately falls outside the scope of this paper, though the inquiring mind may look at Martinez et al. for an excellent explanation. Martinez et al., *A Survey of the Elliptic Curve Integrated Encryption Scheme*, 2:2 J. OF COMPUTER SCI. & ENGINEERING, 7, 8–12 (2010).

40. *See id.*

41. *See* Mohit Arora, *How secure is AES against brute force attacks?*, EE TIMES (May 7, 2012, 5:29 PM), https://www.eetimes.com/document.asp?doc_id=1279619. The truth of this statement depends on the sophistication of the encryption and how much is known about the list of encrypted passwords. A brute force attack begins with "a" before moving on to "aa", "aaa", "aaaa", until the character limit is reached. Then "b, ab, bb, aab, abb, bbb" repeating until all possible combinations of permissible characters are tested. This method can take an extremely long time to crack all passwords in a list because of the number of possibilities that the computer must work through. Sometimes a dictionary attack, using a list of known passwords like the one mentioned *supra* note 3, plus a defined set of rules to get permutations of the password can be a more effective method of breaking the encryption. For example, tested permutations of "password1" in a dictionary attack could include: PASSWORD1, P455W0RD1, password!, PASSWORD!, P455W0RD!, PaSsWoRd!, pAsSwOrD1, PASSword1, passWORD1, and so on, with the list of permutations set to include general substitutions such as numbers for letters, different traditional capitalization schemes, and other common changes that users implement to create a more "secure" password. By using a list of known passwords and making these slight changes, there is an increased chance of cracking the password in a short period of time compared to testing all possible combinations. *See* Computerphile, *supra* note 37.

42. COLO. REV. STAT. § 6-1-716(a) (2018).

43. An IP address is similar to an ordinary postal address. Unlike a regular postal address, however, IP addresses are dynamic in nature and can be changed very easily. This makes using an IP address as a proxy for identity a dubious proposition at best.

44. *See id;* Brian Krebs, *Panerabread.com Leaks Millions of Customer Records*, KREBSONSECURITY (Apr. 18, 2018), https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/.

45. *See* Krebs, *supra* note 43.

period of time.[46] When the barrier for notification is so low, as easy as sending out a simple email, and the risk to consumers is so high, with the cost of identity theft,[47] it is dangerous to draw a line at "no reasonable likelihood of misuse" for the sake of ease and efficiency.

The codified aspects of personal information in Colorado include: an individual's Social Security number; driver's license or identification card number; and financial account, credit card, or debit card number in combination with the security code, access code, or password that would permit access to the resident's financial account.[48] Notably, the statute does not include encrypted information, nor does it include splices or aspects of the financial account, such as a credit card number and a person's name absent other information to better identify the individual.[49] Colorado's definition compares quite poorly to notification laws in other states, such as in California, where personal information includes: an individual's Social Security number, driver license number, financial information, medical information, health information, passwords, access codes, or pin numbers.[50] For instance, suppose an individual has an email account and a password which is leaked. If the email and password combination is used on banking websites, online retailers such as Amazon, to communicate with a loan or mortgage distributor, or any other location in which individuals place their personal information that would be protected under the statute, it would be trivial for the attacker to gain access to the information protected under the statute using information which is not protected under the statute. This hypothetical is far from existing only in the theoretical realm and poses a very real threat to consumers.[51]

Colorado places several responsibilities on a company suffering a data breach. When a company owns or licenses computerized data that includes personal information about a resident of Colorado, the company must notify residents:

> When it becomes aware of a breach of the security system, [the individual or commercial entity shall] conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. The individual or commercial entity shall give notice as soon as possible to the affected Colorado resident unless the end of investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to

46. *See generally id.*

47. Kelli B. Grant, *Identity theft, fraud cost consumers more than $16 billion*, CNBC (Feb. 1, 2017, 9:11 AM), https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html.

48. COLO. REV. STAT. § 6-1-716(1)(d)(I) (2018).

49. *See id.*

50. *See* Russom et al., *supra* note 11.

51. Cristina Chipurici, *Hacked Email: Why Cyber Criminals Want to Get Into Your Inbox*, HEIMDAL SECURITY (Aug. 25, 2016), https://heimdalsecurity.com/blog/hacked-email-why-cyber-criminals-want-inbox/.

> occur. Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.[52]

When personal information is taken from an individual or commercial entity that does not own or license the data, the company must notify the owner or licensee of the data immediately after discovering the breach under a similar standard of when misuse is "occur[ing] or [is] reasonably likely to occur."[53] The company licensing the data must cooperate with both law enforcement and the owner or licensee of the data, though they do not need to disclose anything that may constitute "confidential business information or trade secrets."[54]

A company may delay notice if a law enforcement agency determines that notice will impede a criminal investigation and the law enforcement agency tells the business entity not to provide notice.[55] Additionally, notice must be given to credit reporting agencies if the breach affects more than 1,000 Colorado residents.[56] All of these rights may only be enforced by the Colorado Attorney General's office, there is no private right of action under Colorado's breach notification law.[57]

III. COLORADO'S UPDATED BREACH NOTIFICATION LAWS: COLO. H.B. 18-1128

Colorado House Bill 18-1128 is entitled "Protections for Consumer Data Privacy, Concerning strengthening protections for consumer data privacy."[58] The primary sponsors of the bill are Representative Bridges, Representative Wist, Senator Court, and Senator Lambert.[59] The bill was presented before the Colorado Legislature on January 19, 2018.[60] It was unanimously approved by the House Committee on State, Veterans, and Military Affairs, and thereafter passed to Appropriations on February 14, 2018.[61] After being passed with amendments on the second reading in the house, it passed without amendments on the third reading and was introduced in the senate.[62] The senate passed the bill with a few amendments

---

52. § 6-1-716(2)(a).
53. *Id.* at § 716(2)(b).
54. *Id.*
55. *Id.* at § 716(2)(c).
56. *Id*. at § 716(2)(d).
57. *See Data Breach Charts November 2017*, BAKERHOSTETLER (Nov. 2017), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.
58. Colo. H.B. 18-1128, 71st Gen. Assemb., 2d. Reg. Sess. 1 (Co. 2018).
59. *Id.*
60. *Protections For Consumer Data Privacy*, COLO. GEN. ASSEMB., https://leg.colorado.gov/bills/hb18-1128 (last updated May 17, 2018).
61. *Id.*
62. *Id.*

broadening the scope of the bill, and the house concurred with the senate amendments.[63] The bill was passed along for Governor Hickenlooper's signature on May 4th, 2018.[64] Interestingly, the bill passed unanimously both in the house and in the senate, indicating the bi-partisan effort involved in protecting consumer data.[65]

The legislation creates a new statute, C.R.S. 6-1-713.5, which requires covered entities to implement and maintain "reasonable security procedures and practices" to protect personal information that are appropriate to "the nature and size of the business and its operations."[66] The new statute is a data security law imposing a similar standard to the one implemented by the FTC.[67] Under the ruling in *Wyndham*, a company must maintain "'reasonable measures to detect and prevent unauthorized access' to its computer network."[68] The reasonableness standard extends to the cost-benefit analysis in 15 U.S.C § 45(n): whether the cost to consumers for the lower quality of cybersecurity is outweighed by the benefits to the company or to competition in the marketplace.[69] Even if advocates like myself would prefer a privacy-first assessment of the cybersecurity needs of a company, it is simply not feasible to implement the requisite technology to ensure that all consumer data is always kept in the safest manner possible. This infeasibility results in some shortcuts that companies may allowably take.[70] Thus, like the FTC's unfair trade practices enforcement statute, the Colorado Legislature accounts for the difficulty and cost of effective data protection in the new statute, introducing a reasonableness assessment of security procedures and practices when deciding culpability for a breach.[71]

The legislation also involves an overhaul of section 716 of the Colorado code which defines the context in which consumers must be notified of a security breach.[72] Specifically, if the cost of providing notice exceeds $250,000 or if more than 250,000 Colorado residents must be notified that their information has been breached, substitute notice may apply.[73] Substitute notice requires either an email to affected residents, conspicuous posting on the breached company's website, or a news briefing to statewide media.[74] The new allowance of substitute notice demarcates an

63. *Id.*
64. *Id.*
65. *See supra* note 5.
66. Colo. H.B. 18-1128 at 3.
67. *Compare* 15 U.S.C. § 45(n) (2018), *with* Colo. H.B. 18-1128 at 3.
68. FTC v. Wyndham Worldwide Corp, 799 F.3d 236, 241, 246 (3d Cir. 2015).
69. *Id.* at 256.
70. The assessment is one of reasonability, meaning that there is not a one-size-fits-all approach to cybersecurity. The burden placed on a large company of ten thousand employees handling sensitive consumer information with substantial revenue and an ability to pay an entire cybersecurity is much greater than a small company with only a handful of employees. *See id.* at 241, 246.
71. Colo. H.B. 18-1128 at 3.
72. *Id.* at 4–11.
73. *Id.* at 5.
74. *Id.*

important change that recognizes the potential breadth of modern security breaches. The cost of individual physical mailing notice can potentially run sky-high when the breach affects a large class of individuals. The purpose of the statute is to inform and protect consumers, not to bankrupt the company. Allowing substitute notice is a welcome change to ensure that consumers are informed in the case of a breach.

Additionally, the legislation expands the definition of personal information.[75] There would be several new categories for personal information: medical information, health insurance identification number, biometric data, and username or email addresses in combination with a password or security question and answer that would permit access to an online account.[76] Furthermore, student, military, and passport identification numbers are encapsulated in the definition of personal information within the new legislation.[77]

Under Colorado's old breach notification law, notice must be provided to affected individuals "in the most expedient time possible and without unreasonable delay."[78] The amended bill tightens the timeline language, requiring that notice be provided "not later than 30 days after the date of determination that a security breach occurred."[79] A security breach occurring is defined as "the point in time in which there is sufficient evidence to conclude that a security breach has taken place."[80] Florida also has a thirty day requirement for notification; however, Florida also has a fifteen day "good cause" exception, making the maximum delay for notification forty-five days.[81] Colorado has not incorporated a good cause exception, making Colorado's notification timeline the strictest in the nation.[82] Additionally, companies must now provide notice to the Colorado Attorney General when 500 or more Colorado residents are affected by the security breach.[83] Like the other notice requirements in the bill, notice must take place within thirty days following the breach.[84]

IV. STATE AND FEDERAL OVERLAP

There is a curious overlap between state privacy laws and federal privacy laws. Within the federal scheme, the primary enforcer of privacy law is the FTC with unfair and deceptive trade practices adjudications.[85] Under the Colorado scheme, the Attorney General is looking less to regulate a

75. *Id.* at 5–6.
76. *Id.*
77. *Id.* at 5.
78. COLO. REV. STAT. § 6-1-716(2)(a) (2018).
79. Colo. H.B. 18-1128 at 8.
80. *Id.* at 5.
81. FLA. STAT. § 501.171(3)(a) (2018).
82. *See* Colo. H.B. 18-1128 at 8; Russom et al., *supra* note 11.
83. *Id*. at 10.
84. *Id.*
85. *See* McGeveran, *supra* note 12.

company's cybersecurity practices, but instead to inform the public when a company has a cybersecurity failure.[86] Both frameworks work to punish an actor retroactively; however, the state-level breach notification law only needs to look at the timeline for notification of a breach, or even if any notification was made at all.[87] The FTC, on the other hand, must compare the cybersecurity practices of the company to the cybersecurity best practices posted on the FTC website, as well as other prior adjudications of companies with poor cybersecurity practices.[88] The result of this analysis is a lower burden of production for state adjudication because it is easier to prove a timeline violation than it is to do a comparative analysis of cybersecurity best practices to the implementation of cybersecurity practices at a company.[89]

Most of the time, the FTC takes only easy cases where there is an egregious offense, that is to say, a clear violation of cybersecurity best practices.[90] For instance, in *Wyndham*, the company was breached on three separate occasions using an extremely disruptive form of penetration.[91] Once in, there was no level of separation between the different permissioned accounts, allowing the attacker to gain access to all information using an account belonging to the individual at the front desk.[92] If that is not a clear example of an absolute failure of cybersecurity practices, it is difficult to see what would be. In practical terms, this approach means that the FTC is adjudicating the worst of the worst but letting those more borderline cases slide by.[93] Under Colorado's breach notification law, however, this level of leniency is prohibited.[94] Even the most borderline offender can be prosecuted under strict timeframe framework.[95] For instance, if a company knows with certainty that the company was breached on day one and does not notify the public until day 40, absent some

86. There are no specific guidelines on what cybersecurity practices should be implemented by a company under either the FTC or the Colorado standard. That would be impracticable because of the wide range of technological and economic capabilities of different companies. Instead, both frameworks opt for a reasonableness standard, allowing for play at the joints for companies with both large and small cybersecurity budgets. This inclusive approach allows for a balance between a company's abilities and the protection of consumer data. *See* FTC v. Wyndham Worldwide Corp, 799 F.3d 236, 255–59 (3d Cir. 2015); Colo. H.B. 18-1128 at 3.

87. *See* Colo. H.B. 18-1128 at 3.

88. *See Wyndham*, 799 F.3d 255–59.

89. *Compare Wyndham*, 799 F.3d 255–59 (describing the analysis under the FTC unfair and deceptive trade practices framework), *with* Colo. H.B. 18-1128 at 3, 6–7, 9–11 (describing the analysis under Colorado's breach notification framework). The required analyses are substantially different. While the FTC must dig into the specifics of the cybersecurity practices, the Colorado Attorney General can stick to a violation of the timeline in most prosecutions of the breach notification law.

90. *See* McGeveran, *supra* note 12.

91. *Wyndham*, 799 F.3d at 241–42.

92. *Id.*

93. *See* McGeveran, *supra* note 12.

94. Colo. H.B. 18-1128 at 7.

95. *Id*. at 11.

directive from law enforcement to withhold notification, there is a clear violation of Colorado's breach notification law.[96]

V. CRITICISM AND POTENTIAL FLAWS

Colorado is taking a positive step forward with its new law, but there are some ambiguities and potential oversights that must be addressed before it becomes the go-to standard adopted by other states. With the growth of the administrative state, it is becoming more difficult for companies to ensure that they are compliant with all regulations governing their actions.[97] For instance, imagine a doctor's office in Denver. The office has a security breach and health records are leaked in unencrypted form. Put more formally, the office has experienced the unauthorized acquisition of unencrypted health records, which now qualify as personal information under Colorado's breach notification law.[98] Under the HIPAA breach notification rule, a regulation with which a doctor's office must comply, the office must notify affected individuals within sixty days.[99] Colorado's notification timeline is a more stringent thirty days.[100] But which timeline governs?

The legislature, in an act of foresight, addressed this issue by amending the bill, adding that "in the case of a conflict between the time period for notice to individuals [under Colorado law and a state or federal regulators law or regulation] the law or regulation with the shortest time frame for notice to the individual controls."[101] This wording indicates that the legislature is attempting to take a hard stance against those actors who have data breaches.[102] The legislature's approach makes sense because the barrier for a corporation to notify affected individuals is quite low compared to the cost of a potential identity theft to the consumer.[103] Nevertheless, this example is one of many difficulties presented through a dual-federalism system of governance, wherein a single regulated entity must discern which rules take priority.

One specter on the horizon that few lawmakers have considered is what is called Shor's Algorithm.[104] This algorithm will, once feasible

96. *Id.* at 7. ("Notice *must* be made in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred.") (emphasis added).

97. *See* Jane W. Moscowitz, *Compliance Programs for Small Businesses*, PRAC. LAW., July 2002, at 25, 34–35. (describing a compliance checklist involving the hiring of several people that is perhaps not feasible for smaller businesses, despite the importance of compliance.)

98. *See* Colo. H.B. 18-1128 at 4–6.

99. HIPAA Breach Notification Rule, 45 C.F.R §§ 164.400–414 (2018).

100. Colo. H.B. 18-1128 at 8.

101. *Id.* at 11.

102. *See id.*

103. *See supra*, notes 46, 72, 73.

104. For more information on Shor's Algorithm, I suggest reading Stephanie Blanda, *Shor's Algorithm – Breaking RSA Encryption*, AM. MATHEMATICAL SOC'Y (Apr. 30, 2014), https://blogs.ams.org/mathgradblog/2014/04/30/shors-algorithm-breaking-rsa-encryption/. The article goes into far more technical depth than I have space to devote in this paper. Additionally, Deirdre

quantum computing[105] is achieved, render nearly all modern encryption methods trivially broken.[106] Why should this algorithm matter? Because currently it may take decades of brute forcing an encrypted piece of information to finally crack the cipher.[107] Once we reach a point where we can run Shor's Algorithm on a sufficiently powerful device, the encrypted information will be trivially transferred into plain text.[108]

Imagine a hypothetical wherein individuals have their personal information stored in an encrypted database. The database belongs to some private entity and includes items such as the individual's social security number, credit card number, home address, or other things that would otherwise qualify under the current definition of personal information under Colorado's statutory scheme. Suppose that database is exfiltrated and released to the public. Right now, that may not mean much if information is sufficiently encrypted; it is an indecipherable table of letters and numbers which does not fit within the meaning of personal information under Colorado's new breach notification law.[109] But in the future, when we can run Shor's Algorithm, the information in the database will be easily turned into plain text.[110] The people who did not realize that their personal information was stolen in the potentially distant past, because the information was encrypted at the time and there was no mandatory notification, will suddenly be hit with a wave of identity theft, seemingly out of nowhere, because the statutory scheme when the information was stolen did not have a notification requirement for stolen encrypted information.[111]

The legislature does recognize some of the failings of encryption in the new law, requiring breach notification if a strange scenario arises whereby a private key or decrypting program matching the encrypting process for the data was kept in the database. [112] But it does not go far enough with the threat of future decryption mechanisms such as quantum computing and Shor's Algorithm. All things considered, information is power

---

Connelly does an excellent job of explaining the problem of quantum computing as it pertains to encryption, as well as potential solutions, in Cloudflare, *Cloudflare Crypto Meetup (Feb 2017)*, YOUTUBE (Mar. 7, 2017), https://www.youtube.com/watch?v=ctP24WKusX0.

105. Larry Greenemeier, *How Close Are We—Really—to Building a Quantum Computer?*, SCIENTIFIC AMERICAN (May 30, 2018), https://www.scientificamerican.com/article/how-close-are-we-really-to-building-a-quantum-computer/.

106. *Id.*

107. *See* Computerphile, *supra* note 37.

108. *See supra* note 103 and accompanying text.

109. *See* Colo. H.B. 18-1128, 71st Gen. Assemb., 2d. Reg. Sess. 1, 3–11 (Co. 2018).

110. *See supra* note 103 and accompanying text.

111. *See* Colo. H.B. 18-1128 at 8 ("The breach of encrypted or otherwise secured personal information must be disclosed in accordance with this section if the confidential process, encryption key, or other means to decipher the secured information was also acquired in the security breach or was reasonably believed to have been acquired.") This portion of the statute indicates that the hacker must acquire the ability to decrypt the information through the breach which would take an incredible act of negligence on the part of the system administrator. Working off the assumption presented *supra* notes 36–41, encrypted information is currently thought to be "safe."

112. Colo. H.B. 18-1128 at 8.

and giving consumers an opportunity to protect themselves from eventual bad actors is the essential spirit of Colorado's breach notification laws.

VI. CONCLUSION

While the FTC is seen as the data protection police, they simply do not have the resources to ensure that every bad actor is punished for putting private consumer information at risk. Luckily, state privacy breach laws are there to pick up the slack. When a breach does occur, affecting consumers within the state, those consumers must be notified that their information is potentially at risk. Colorado's new breach notification law modification goes a long way towards the goal of informing consumers whenever their information is at risk. It is an excellent platform to build off going into the future. But I would warn the legislature that the job is not finished yet: future technology poses a certain threat to information not yet protected under the statute. If the goal is truly to give consumers a choice in the protection of their data, there is still work to be done with Colorado's breach notification laws.

* *Mitchol Dunham*

* Online Editor for the *Denver Law Review* and 2019 J.D. Candidate at the University of Denver Sturm College of Law.