# Doctoring Up Cybersecurity Standards: A Solution to Adequate Internet Security Measures Post *Wyndham*

*Vince Vela*



## I. Introduction

In today's technological world, it is common for corporations and individuals alike to enjoy and exploit the benefits of cloud computing. These advancements, however, come with a price as the modern technological age continues to grow. By its very nature, the normal course of business has changed drastically. From private entrepreneurial websites to conglomerates like Amazon, Inc., making purchases online has never been easier. Rather than traveling to your products, consumers today simply create an account with a certain business, enter personal credentials, provide a credit or debit card number for the transaction, and give an address for the shipment of their newly owned product.

As a way to facilitate this course of business, it is normal for online venders to utilize their consumer's information and store it for future use in the event that the consumer would like to purchase again. Due to the storing of valuable information onto the cloud, an increasing number of online security breaches via hacking from unauthorized individuals has occurred. This has led to multiple areas of contention between state laws and regulations, the businesses found therein, along with their valuable stored information and the use of the cloud itself.

This Note aims to fill the gaps between the legal and the constantly changing technological world. Since valuable personal property is at

stake when consumer information is stored in online databases, it is imperative that laws offering protection provide adequate safeguards to those most at risk. In filling these gaps, this Note first explains the use of cloud computing, including cloud variations and the essential components to these online databases. Second, this Note delves into an in-depth analysis of *Federal Trade Commission v. Wyndham Worldwide Corporation*, a recent FTC (Federal Trade Commission) case that has provided uncertainty in the cybersecurity world. Third, this Note identifies the gray areas from *Wyndham* that remain in question as well as provides a foundation of existing case law to shed light on the topic. Fourth, this Note proposes a change in the FTC's current proceedings to provide a rule that identifies specific cybersecurity measures to obtain adequate protections in the event of cyber attacks.

## II. Cloud Computing

### A. *Generally*

Cloud computing is an internet-based service that allows online users to store and access information over the Internet rather than a personal computer's hard drive. Through the development of this technology, businesses benefit from the use of cloud computing in several ways including: cost savings, reliability, manageability, and a strategic edge over competitors.[1] As a result, it does not come as a shock that the number of small businesses using cloud computing is expected to increase from 37% to 80% by 2020.[2]

In a virtual sense, clouds come in many shapes and sizes. Data clouds can be public, private, or a hybrid of the two. Furthermore, depending on what the cloud actually provides for a user, a cloud can be deemed as an Infrastructure-as-a-Service ("IaaS"), a Platform-as-a-Service ("PaaS"), or a Software-as-a-Service ("SaaS").[3] Each type of cloud has its own specific attributes that make it more desirable for users depending on the services needed. That being said, this Note will primarily focus on where a cloud is located, being public or private, and the major implications of how either type can be seriously subjected to data breaches that can create problems for businesses everywhere.

1. *Advantages and Disadvantages of Cloud Computing*, LevelCloud, http://www.levelcloud.net/why-levelcloud/cloud-education-center/advantages-and-disadvantages-of-cloud-computing/ (last visited May 23, 2016).

2. Graham Winfrey, *How the Cloud Will Transform Business by 2020*, Inc. (Aug. 7, 2014), http://www.inc.com/graham-winfrey/why-the-cloud-will-transform-small-business-by-2020.html.

3. Goran Čandrlić, *Cloud Computing – Types of Clouds*, GlobalDots (Feb. 26, 2013), http://www.globaldots.com/cloud-computing-types-of-cloud/.

### B. *Public and Private Clouds*

As previously stated, cloud computing can take several forms for their users. Depending on the information stored, a user may decide on either a public or private cloud, or a hybrid of the two. The main difference between a public and private cloud is where the cloud itself is located. A private-cloud computing system is established if the user is utilizing a cloud that is located as a part of an extension of an operation that the business owns and maintains itself.[4] On the other hand, a business would use a public-cloud system if it were to utilize and pay for the same services from a third party.[5]

From a cost-benefit analysis, one can see the major advantages for businesses, specifically for small businesses, for the utilization of public clouds. By using a third-party server, rather than creating and maintaining a costly personal data infrastructure, a business can outsource their methods of retrieval and storage of information, which will result in major cost-saving benefits.[6] Additionally, public clouds are known to have a flexible and tailored approach with payment methods depending on the size and volume of data a business plans to utilize.[7] Lastly, public-clouds are also preferred over private clouds due to their virtually unlimited access and ease of availability.[8]

Private-clouds, as opposed to public clouds, are generally used by corporations and individuals who prefer their information stored on a "non-shared resource" platform that operates as an extension of the business itself.[9] One major consideration for using a private-cloud system that may deter users from their utilization would be the overhead management and costs associated with maintaining this type of platform.[10] That being said, larger corporations that have the available capital to promote a private-cloud database system are often able to exploit the many security advantages available to battle increasing threats of cyber attacks.[11]

### C. *Security Problems with the Clouds*

Regardless of where or how a cloud user stores their online information, be it publically or privately, the threat of data breaches is becoming a prevalent problem for businesses in the cloud. Due to this increasing problem, the FTC created a guide to aid businesses in data security when sensitive personal information or, in other words, con-

4. *Public Cloud or Private Cloud?*, AKAMAI, https://www.akamai.com/us/en/resources/public-private-cloud.jsp (last visited May 24, 2016).
5. *Id.*
6. *Id.*
7. *See id.*
8. *See id.*
9. *Id.*
10. *Id.*
11. *See id.*

sumer's online personal property, is at risk of cyber attacks.[12] This information often includes consumers' names, Social Security numbers, credit and debit card numbers, and other personal account data that identifies customers or employees.[13] In this publication, the FTC advises businesses to (1) be aware of all computers and servers where sensitive personal information is stored, including identifying the connections of computers with such information, using data encryptions for sensitive customer data; and (2) consider data access restrictions from certain information.[14] Furthermore, a business should be well advised on password management and laptop security.[15] In addition, a business should understand firewall protections, the use of wireless and remote access from multiple devices, provide a system in place for detecting potential breaches, and focus on employee training for a data security plan.[16]

Despite the FTC's efforts, businesses using cloud storage information data systems continue to see upsetting revelations of cyber attacks. From 2012 to 2013, the number of reported data breaches increased by 62% and was further calculated to retain a loss of $18 billion from credit card fraud.[17] Furthermore, the U.S. Bureau of Labor Statistics has projected a promising outlook for professionals seeking data security analyst positions with an employment percentage increase of 37% between 2012 and 2022.[18] These statistics allow the assumption for increased risk of cyber attacks in the future.

### D. *Case Law on Security Data Breaches*

Just as the technological era emerged exponentially, so to must the law that governs it. A multitude of case and statutory law has been promulgated to shape and form the realm of cloud computing database security. Through the powers provided by Congress, the FTC is "empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[19]

12. *See generally* FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2011), https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

13. *Id.* at 2.

14. *Id.* at 9–11.

15. *See id.* at 12–13.

16. *Id.* at 14–18.

17. Tony Bradley, *3 Staggering Retail Data Breach Statistics*, CSO (Nov. 26, 2014), http://www.csoonline.com/article/2852383/data-breach/3-staggering-retail-data-breach-statistics.html.

18. *Data Security Analyst: Job Description, Duties and Requirements*, STUDY, http://study.com/articles/Data_Security_Analyst_Job_Description_Duties_and_Requirements.html (last visited May 23, 2016).

19. Federal Trade Commission Act, 15 U.S.C. § 45(a)(2) (2012).

Undoubtedly, the FTC is provided wide discretion in their congressional grant of authority. These powers, however, are often subject to attack by those who feel the FTC should not be able to act and decide matters in certain instances. We see this in the FTC's authority in determining unfair labor practices in connection to the realm of cyber security, particularly customer data breaches. Unfortunately for those who question the FTC's role in cyber law, the courts have decided, with the pounding gavel of the landmark *Wyndham* case, that the FTC's statutes can and should be interpreted to extend to cyber security related issues.[20]

## III. *Wyndham* Analysis

The *Wyndham* case remains paramount in determining the broad scope of the FTC's powers. The case emerged after a series of three separate cyber security attacks between 2008 and 2009 that allowed hackers to access the Wyndham Worldwide Corporation's computer systems.[21] The data breaches resulted in fraudulent charges accruing over $10.6 million stolen from consumers' personal and financial information that happened to be stored in the Wyndham network.[22] As a result, the cyber attacks triggered the FTC to bring an action against Wyndham, stating that the corporation's acts amounted to an unfair practice.[23]

In terms of Wyndham's unfair cybersecurity practices, the FTC proclaims that Wyndham's acts "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."[24] The FTC specifically stated in their claim that Wyndham:

> (1) allowed company branded hotels to store payment card information in clear readable text;
>
> (2) allowed the use of easily guessed passwords to access property management systems;
>
> (3) failed to use available security measures, such as firewalls, to limit access between the hotel management system, company network, and the Internet;
>
> (4) allowed hotel property management systems to connect to its network without taking appropriate cybersecurity precautions, including not ensuring the hotels had implemented adequate security policies and procedures, knowingly continued to use an outdated operating system, and, due to improper management, could not identify the source of at least one of the cybersecurity attacks;

20. *See generally* F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3rd Cir.) (2015).
21. *Id.*
22. *Id.*
23. *Id.*
24. *Id.* (citing FTC's complaint at ¶ 24).

> (5) failed to implement restricted access procedures from third parties;
>
> (6) failed to employ reasonable measures to detect and prevent unauthorized access to its computer network or to conduct security investigations; and
>
> (7) failed to follow proper incident response procedures.[25]

Not agreeing with the allegations against them, Wyndham filed a motion to dismiss.[26] Wyndham's primary argument focused on the unfairness of its conduct and whether the FTC had authority to bring this action in spite of recent legislation from Congress.[27] Throughout a lengthy discussion over such contentions, the district court denied Wyndham's 12(b)(6) failure to state a claim motion and thus established that the FTC did in fact have jurisdiction over cybersecurity by allowing the case to continue.[28]

Wyndham's next argument, being a central component to this Note, delved into Wyndham's due process rights in that the FTC failed to give fair notice of the specific cybersecurity standards that Wyndham was required to follow.[29] To shed light on the fair notice doctrine, the district court highlighted three separate legal standards when agencies are involved in statutory or regulatory interpretation.[30] The first standard is where an agency administers a statute without special authority to create new rights or obligations.[31] Under this approach, courts will give respect to the agency's view in its persuasiveness; however, courts will ultimately be responsible for determining the interpretation of the statute.[32]

The second standard the court highlighted was where an agency exercises its authority in order to fill gaps in its statute.[33] Here, the courts will give deference to the agency as the primary interpreter of the statute so long as the interpretation is reasonable.[34] That being said, courts often exercise caution when dealing with civil regulations by stating that parties should be entitled to an "ascertainable certainty" of what is legally required by the agency's regulation.[35]

The third and last standard the district court explained was where an agency interprets the meaning of its own regulation.[36] Here again, courts will generally defer to a reasonable agency interpretation so

25. *Id.* at 240–41.
26. *Id.* at 242.
27. *Id.* at 244, 247.
28. *Id*. at 242.
29. *Id*. at 249.
30. *Id.* at 250.
31. *Id.* at 250–51.
32. *Id.* at 250.
33. *Id.* at 251.
34. *Id.*
35. *Id.*
36. *Id.*

long as the private parties are entitled to know with ascertainable certainty what is required.[37] The district court goes on to say the second and third contexts have a higher standard of fair notice due to the nature on how agencies interpret differently from courts.[38] Knowing this, Wyndham argued they should have been entitled to an ascertainable certainty of the FTC's interpretation of the security requirements needed to be in accordance with Congress's Title 15 U.S.C.A. § 45(a).[39] Unfortunately for Wyndham, the district court found this argument equally unpersuasive, stating:

> Wyndham's position is unmistakable: the FTC has not yet declared that cybersecurity practices can be unfair; there is no relevant FTC rule, adjudication or document that merits deference; and the FTC is asking the federal courts to interpret § 45(a) in the first instance to decide whether it prohibits the alleged conduct here. The implication of this position is similarly clear: if the federal courts are to decide whether Wyndham's conduct was unfair in the first instance under the statute without deferring to any FTC interpretation, then this case involves ordinary judicial interpretation of a civil statute, and the ascertainable certainty standard does not apply. The relevant question is not whether Wyndham had fair notice of the FTC's interpretation of the statute, but whether Wyndham had fair notice of what the statute itself requires.[40]

Therefore, as it may seem, although Wyndham lost their ascertainable certainty argument, the district court found that Wyndham would still have a chance for a dismissal by reasons of fair notice principles when Wyndham claimed they "lacked notice of what *specific* cybersecurity practices . . . necessary to avoid liability."[41] The court did not hesitate to reject this argument with ease—stating that Wyndham's focus was on the FTC's interpretation and not the fair notice principles themselves.[42] Therefore, the court ultimately decided not to take up a matter it was not explicitly asked to take on.

In light of the district court's decision, they further added reasons why Wyndham's fair notice claim fails. Using the FTC's guidebook on protecting personal information, as previously mentioned, the court identified several recommendations that corporations and individuals can utilize to secure sensitive consumer information. Wyndham argues, however, that the FTC's policy is "too vague to be relevant to the fair notice analysis" in that the FTC fails to provide and identify specific examples of what is necessary for compliance with § 45(a).[43]

37. *Id.*
38. *Id.* at 251–52; *see also* Frank H. Easterbrook, *Judicial Discretion in Statutory Interpretation*, 57 OKLA. L. REV. 1, 3 (2004).
39. *Wyndham*, 799 F.3d at 252.
40. *Id.* at 253–54.
41. *Id.* at 255 (emphasis added).
42. *Wyndham*, 799 F.3d at 255.
43. *Id.* at 258.

Moreover, Wyndham claimed that if the allegations against them are determined not to be vague, the FTC still failed to explicitly state what specific cybersecurity measures actually triggered their violation.[44] In support of this argument, Wyndham claimed the FTC alleged that the security measures "*taken together*" caused the FTC's suit.[45]

The district court, siding again with the FTC, tackled both of Wydham's arguments on two fronts. The first being that even if the FTC failed to specify which allegations formed the necessary and sufficient conditions of the violations, businesses like Wyndham could still ascertain the possibility of liability under the statute.[46]

As for the second front, the court pointed to Wyndham's actions and juxtaposes them to relevant close corollaries.[47] Here, the court used a preceding action against CardSystems Solutions, Inc. ("CSS") that provided a framework for cybersecurity measures that previously failed FTC requirements.[48] In viewing both actions respectively, the FTC's complaints show that both CSS and Wyndham: (1) created unnecessary risks to sensitive and vulnerable information; (2) failed to monitor and adequately access the vulnerability of their web applications; (3) failed to employ strong ID and user passwords; (4) failed to use readily available security measures, such as firewalls to limit access; and (5) failed to invoke detection measures and investigate for security threats.[49] Using the CCS's action as a template, the district court found little trouble concluding Wyndham's similar cybersecurity measures were as equally inadequate under §45(a) of the FTC.[50]

In conclusion, the *Wyndham* case is primarily known for the expansion of the FTC's authority into the cybersecurity world with the use of § 45(a) for unfair trade practices against consumers. Although the FTC began bringing administrative actions against companies for inadequate cybersecurity measures in 2005, the vast majority of those cases ended in settlements.[51] The *Wyndham* case, therefore, has provided the FTC with a clear victory in that they may now enter the cyber world without fear of jurisdictional stripping from Congress.

## IV. Arising Questions from *Wyndham*

With Wyndham's unveiling of the FTC's authority in the cyber world, a new question arises for corporations using the public and pri-

44. *Id.*
45. *Id.*
46. *Id.*
47. *Id.* at 258–59.
48. *Id.* at 258; *see generally In re* CardSystems Solutions, Inc., No. C-4168, 2006 WL 2709787 (F.T.C. Sept. 5, 2006).
49. *Wyndham*, 799 F.3d at 258.
50. *Id.*
51. *Id.* at 240.

vate cloud domains for their online data information systems. The district and appellate courts from *Wyndham* found that the hotel management's information system clearly lacked the necessary cybersecurity measures with an overwhelming sweep using the help of CSS's prior complaint. This now begs the question, what is to be said about the companies and corporations whose cybersecurity measures are maintained in a manner closer to the FTC's required standards?

### A. *Preceding Case Law*

As previously mentioned, although the FTC has been bringing administrative actions against companies for inadequate cybersecurity measures since 2005, many of the disputes have been resolved through settlements.[52] However, certain cases have been brought into light that offers additional guidance towards a court's determination of reasonable cybersecurity standards.

In 2005, the FTC issued a complaint against BJ's Wholesale Club, Inc., a Delaware corporation, for failing to employ reasonable and appropriate security measures that constituted an unfair practice according to FTC standards.[53] The FTC's complaint states that BJ's Wholesale Club operated approximately 150 stores in sixteen states.[54] The corporation operated under a membership-only agreement in order for consumers to make purchases.[55] As a result, during the time of the complaint, the corporation was stated to have close to eight-million valid membership agreements.[56]

The framework of BJ's membership requires the corporation to obtain authorization from a bank that issues a credit card to consumers for purchases made at the store.[57] Using a computer network for authorization, BJ's also must acquire the "customer's name, card number and expiration date, and certain other information (collectively, 'personal information')."[58] Furthermore, BJ's also uses its computer networks to manage inventory using wireless scanners that operate using wireless access points for transmission of information.[59]

Due to fraudulent charges discovered beginning from November 2003 to February 2004, the FTC investigated BJ's data security measures.[60] Upon their inspection, the FTC concluded that the corporation "did not employ reasonable and appropriate measures to secure

52. *Id.*
53. *See generally*, *In re* BJ's Wholesale Club, Inc., No. C-4148, 2005 WL 6241019 (F.T.C. Sept. 20, 2015).
54. *Id.* at **7.
55. *Id.*
56. *Id.*
57. *Id.* at **1.
58. *Id.*
59. *Id.*
60. *Id.* at **2.

personal information collected at [BJ's] stores."[61] Specifically, the FTC found that the corporation: (1) used no encryptions for information that was in transit to and from the bank and for their personal in-store computer networks; (2) allowed for anonymously accessible stored information due to commonly known default user IDs and passwords; (3) failed to provide readily available security measures that could limit the access to their computer networks; (4) did not use sufficient detection measures to search for unauthorized access and further failed to conduct security investigations; and lastly (5) created an unnecessary risk for the personal information by storing it up to an additional 30 days when it was no longer needed.[62]

BJ's failed security measures led the FTC to conclude that the corporation's practices employed unfair acts in violation of § 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).[63] As a result, subsequent action from the FTC ordered and required BJ's to establish a "comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information it collects from or about consumers."[64] As part of the requirement, the security program must also "contain administrative, technical, and physical safeguards appropriate to BJ's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected."[65] Specifically, the FTC ordered that BJ's should:

> (1) Designate an employee or employees to coordinate and be accountable for the information security program; (2) Identify material internal and external risks to the security, confidentiality, and integrity of consumer information that could result in unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks; (3) Design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures; and (4) Evaluate and adjust its information security program in light of the results of testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that BJ's knows or has to reason to know may have a material impact on the effectiveness of its information security program.[66]

Furthermore, the FTC also required BJ's to obtain an assessment from a "qualified, objective, independent third-party professional."[67]

61. *Id.*
62. *Id.*
63. *Id.*
64. *Id.* at **4.
65. *Id.*
66. *Id.*
67. *Id.*

According to the FTC, the auditor was to certify that the corporation had met or exceeded the security measures provided for by the order, as well as to assure that BJ's security program was sufficiently effective in providing "reasonable assurance that the security, confidentiality, and integrity of consumers' personal information has been protected."[68]

### B. *Where Should the Threshold Be?*

Returning to *Wyndham's* analysis, one can see the strikingly similar complaints the FTC issued against both the hotel management chain and BJ's Wholesale Club. Yet, there still is yet to be a case that identifies specific facts that come closer to the threshold of the FTC's standards.

Although there is no concrete discussion for a required minimum standard on cybersecurity measures concerning sensitive consumer information stored on public and private clouds, the court from *Wyndham* attempted to find a common denominator in this respect. In determining Wyndham's attempted vagueness argument for their fair notice claim, the court first identified the regulatory language from § 45 that defines a violation as acts or practices that "cause or is likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[69] The court continued by stating:

> While far from precise, this standard informs parties that the relevant inquiry here is a cost-benefit analysis that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity. We acknowledge there will be borderline cases where it is unclear if a particular company's conduct falls below the requisite legal threshold. But under a due process analysis a company is not entitled to such precision as would eliminate all close calls. Cf. Nash v. United States, 229 U.S. 373, 377, 33 S. Ct. 780, 57 L. Ed. 1232 (1913) ("[T]he law is full of instances where a man's fate depends on his estimating rightly, that is, as the jury subsequently estimates it, some matter of degree."). Fair notice is satisfied here as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute.[70]

Although the court gives reference to the cybersecurity measures of *borderline* cases, they refuse to set out a bright line rule to follow.

68. *Id.*

69. F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 244 (3rd Cir. 2015); Federal Trade Commission Act, 15 U.S.C. § 45(n) (2012).

70. *Wyndham*, 799 F.3d at 255–56.

Instead, the court acknowledges that companies who store sensitive consumer information should estimate, just as a jury would, on what would be reasonably required of them.

The standard of reasonableness is one that is well grounded in a legal sense. In negligence tort claims for example, there is a duty to act reasonably or to reasonably foresee a potential harm to another.[71] Often the term "reasonable" is relevant to specific situations. Professionals have the duty to act as a reasonable professional would with similar skill and circumstance.[72] In torts concerning children, a child is to be viewed under the standard of how a reasonable person of like age, intelligence, and experience under like circumstances would act.[73] As it may seem, the idea of reasonableness changes under the circumstances where it is invoked. This begs the question, what is or what can be the reasonable standards for cybersecurity measures? Further, as for the relativeness of a reasonable standard, can there be any consistency in cybersecurity standards when there is constant technological advancements?

The court from *Wyndham* also maintains a determination for cybersecurity standards to be viewed from a cost-benefit analysis.[74] Here, an analysis should consider "the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity" that competes with "the costs to consumers that would arise from investment in stronger cybersecurity."[75] Again, the court designates that this should be done on a fact intensive examination through a case-by-case approach and further remains silent on any indication for consistency.

In sum, the remaining questions from *Wyndham* are that of relativeness. With limited case law pertaining to failed cybersecurity measures, companies and cloud users alike bear the burden of providing what they believe to be reasonable standards of cybersecurity in the dynamics of the technological world. As a result, consumer personal and property in businesses' online databases remain at risk.

## V. Legal Dynamics of the Technological World

The idea of precedent, *stare decisis*, revolves around a sense of consistency. Throughout history, courts have held true to a form of consistency in order to provide for an ordered and structured legal system. However, time has proven that some circumstances give way for changes in the law depending on societal factors throughout a given era. When certain aspects change, the law answers by adapting to those changes and strives for some form of consistency yet again.

71. *See generally* Restatement (Second) of Torts § 4 (1965).
72. *See* Matarese v. Buka, 897 N.E.2d 893, 898 (Ill. App. Ct. 2008).
73. *See generally* Goodfellow v. Coggburn, 560 P.2d 873 (Idaho 1977).
74. *Wyndham*, 799 F.3d at 255.
75. *Id.*

In attempts to battle the dynamics of the legal world, and yet still provide a sense of consistency, legislatures and common law circumstantially give courts bright line rules, *prima facia* elements, and even determinative and dispositive factors. Using these, lawyers and courts alike can take advantage of the legal system's desire for consistency and be sure, for the most part, that courts will not sway off course as an outlier.

However, time has proven that under certain circumstances, whether a societal view or a political motivation, the legal world remains to be dynamic and constantly changing. Therefore, throughout the internet boom and society's internet-connected world, one can see the dynamics of the legal world at work. For example, a new form of law has emerged known as "Internet Law" that encompasses many legal issues relating to the use of the internet. These legal issues include: property rights, intellectual property, patents, and contracts. As a result, just as the internet has led to many legal changes, this Note proposes yet another change in the cyberworld dealing with adequate cybersecurity measures.

As previously stated, *Wyndham's* decision leaves a question unanswered as to what it specifically means to provide reasonable cybersecurity measures. Businesses and individuals who store personal and consumer information have limited factors to base their own security measures on and remain unsure of what will meet FTC standards. Although the factors that *Wyndham* sheds some light, cloud users are still in the shadows in what they must do themselves to escape the FTC's pounding of their gavel. Therefore, this Note will look at the pros and cons of various legal alternatives that may provide consumers a sense of adequate protection without the harsh results that businesses fear in terms of liability.

### A. *The Relevant Factors and Balancing Approach*

In order to provide an adequate analysis of the various legal alternatives, one must first identify the status quo that was utilized in *Wyndham*. In *Wyndham*, the court found that a reasonableness approach with the inclusion of a cost-benefit analysis would promote the best results in terms of the competing parameters between justifying businesses' liability and adequate consumer protections.[76] Under the scope of this analysis, the FTC is able to show flexibility in their determinations by promoting their findings under a case-by-case analysis. In essence, the FTC is provided with much discretion when using this approach because there has yet to be any specifics as to what is actually required for companies finding themselves in a position like that of Wyndham Worldwide.

76. *See id*. at 236.

As previously stated, the discussion over the cybersecurity measures used in *Wyndham* were far from reasonable in nearly all aspects and therefore made the FTC's decision to bring the action at all relatively easy. During the FTC's investigations, the agency found that rather than using weak firewalls, Wyndham failed to use *any* firewalls at critical access points.[77] In addition, Wyndham also failed to use *any* encryptions for their customer files and also failed to require some users to change their login credentials at *all*.[78] Among the other failures from Wyndham's cybersecurity measures, it was seemingly simple to understand why the FTC is seeking recourse for Wyndham's consumers.

In retrospect, the court from *Wyndham* recognizes there will be instances where it would be "unclear if a particular company's conduct falls below the requisite legal threshold."[79] That being the case, when a company is at the discretion of the FTC, should there not be a legal threshold readily apparent? To this, the court from *Wyndham* shies away from giving specific requirements and instead points to the FTC's guidebook, *Protecting Personal Information: A Guide for Business*, created in 2007.[80] Arguably, it can be stated that this guidebook, having not been mandated by law, offers no real threshold for businesses other than what *could* be done in order to implement adequate cybersecurity measures. However, the court believed following the offered guidelines would have placed Wyndham in a better position to avoid liability.[81]

In addition to the standard of reasonable cybersecurity measures, the court from *Wyndham* also invoked a cost-benefit analysis. In an even less specific manner, the court stated business liability rests on the balancing of the "probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to [businesses] that would arise from investment in stronger cybersecurity."[82] Therefore, businesses are told they should implement security standards based on the harms that could potentially occur to their consumer base. Thus, the more at stake for consumer theft, the more security standards a business should implement. Again, this leaves a business at the FTC's mercy in that it must ascertain what standards of security are needed with no clear way to know if it is in accordance with FTC standards. The court from *Wyndham* acknowledged this uncertainty and still chose not to delineate but rather leave it to a "man's fate . . . on . . . estimating rightly."[83]

77. *Id*. at 256.
78. *Id.*
79. *Id*. at 255–56.
80. *Id.* at 256.
81. *Id*. at 257.
82. *Id*. at 255–56.
83. *Id*. at 256 (citing *Nash v. United States*, 299 U.S. 373, 377 (1913)).

The standards used in *Wyndham* offer extreme flexibility throughout society's technological advancements and growing reliance on the use of the internet. By using the reasonable, relevant factors and cost-benefit analysis, the FTC can continue to impose liability on businesses that fall below the desired threshold, even with the growing concern of the changing technological world. As new and improved methods of both cyber threats and security standards become in use, the FTC can stand firmly on the standards used in *Wyndham* to combat any of the new cyber methods by invoking their idea of reasonableness. Although this parallels smoothly with the dynamics of the cyber world, much is left uncertain to those businesses affected most by the FTC's vague cybersecurity measures.

### B. *The Bright Line Test and the Required Minimum*

Leaving a more flexible approach for a hard-and-fast, consistent approach may provide the additional benefits for businesses, but at what cost? If consistency in the law and legal effects were of the most importance, then implementing cybersecurity measures under a bright line test would most likely have the best results. Under an approach like this, businesses and individuals who are storing personal consumer information would adhere to the black letter law that designates exactly what is required of them in order to avoid liability in the occurrence of a data breach.

Although this test may provide a sure shot approach to avoiding liability for businesses using the cloud, it is likely to produce additional problems along the way. For example, if the legal system were to implement the exact cybersecurity measures that businesses need to adhere to, then there is a strong likelihood that those measures would soon become obsolete due to technological advancements. As a result, consumers will ultimately be at greater risks due to the legal delay that would apply when it came to updating the law to the additionally discovered cyber threats. In addition, businesses would have no incentive to continue to strive for the best possible security measures for their consumers knowing that they would be shielded from liability simply because they abided by what was required of them.

Apart from a bright line test, another way that may be able to bring cybersecurity measures up to adequate measures would be the establishment of a required minimum approach. This approach, much like a bright line test, would undoubtedly benefit businesses in ascertaining what must be done to avoid liability. However, in understanding that this approach essentially parallels the bright line test, perhaps the answer to ascertaining both adequate cybersecurity measures for consumers, as well as providing businesses with a way for avoiding liability, lies with its application.

If, for example, a required minimum approach was working in tandem with an incentive program for businesses, then society may be

able to achieve a deterrence of cyber attacks as well as a fair approach for businesses ascertaining adequate cybersecurity standards. In addition, businesses that compete for the same class of consumers will also have a competitive advantage if they were to continue to strive for up-to-date cybersecurity measures as the technological world advances.

This approach could also allow for little legal involvement due to the possibility of its self-regulating aspects. Here, like all other business markets, the consumers and businesses will be able to decide what cybersecurity measures to provide and what measures to accept. So long as the security measures are known, consumers can make an informed decision of where they are willing to place their personal information. As a result, this approach may promote healthy competition for businesses by letting them decide what to offer. Therefore, a business would only be required to implement the legally required minimum, but without more, remains at the peril of other businesses that may decide to provide additional security and presumably gain consumers due to their added protections.

Unfortunately, by their very essence, a bright line rule or required minimum standard for cybersecurity measures is, and always will be, at risk of becoming obsolete by the nature of the cyber world. Unlike that of the flexible reasonable approach used in *Wyndham*, the bright line and required minimum approaches are subject to less flexibility on the dynamics and therefore may provide inadequate results in terms of consumer protection in the long run.

### C. *Providing the Specifics*

The FTC brought their action against Wyndham Worldwide based on § 45(n) of Title 15 of the U.S.C.A. Subsection 45(n) claims that the FTC shall have no authority to declare an act as unfair unless "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition."[84] Using the statute's text, the court from *Wyndham* construed its meaning to represent a cost-benefit analysis among the relevant factors as discussed previously. However, under no circumstances does the statute, nor the court's interpretation of the statute, relate to any specific cybersecurity measures that should be taken into account. A question thus comes to mind, could the FTC promulgate a new rule that works in accordance with § 45(n) that would provide for specific cybersecurity measures?

In order to answer this, perhaps guidance lies in other federal establishments. As such, the Health Insurance Portability and Accountability Act ("HIPAA") under the Department of Health and Human Services is able to show how another federal entity deals with its sensi-

84. Federal Trade Commission Act, 15 U.S.C. § 45(n) (2012).

tive consumer data. Understanding medical documentation is of clear importance in terms of privacy and confidentiality, HIPAA provides an in-depth approach on multiple safeguards that the department should take into consideration, such as administrative, physical, and technological safeguards.[85]

As to HIPAA's technological safeguards, it lays out a more detailed variation of cybersecurity standards than the FTC's counterpart under § 45(n).[86] Particularly, § 164.312(a)(1) states that covered entities or business associates in the realm of protected health information *must* "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights."[87] Furthermore, subsection (a)(2) also provides implementation specifications including: a *required* unique user identification, a *required* emergency access procedure, an *addressable* automatic logoff function, and an *addressable* encryption and decryption standard.[88] The remainder of § 164.312 also describes with specific particularity that a standard should be in place for verification of persons trying to access certain health information, and further provides details for the transmission of data through electronic communications in order to guard against unauthorized access.[89]

In viewing the aims of HIPAA's technological safeguards and the FTC's interpretation of unfair practices in regards to cybersecurity measures, it is apparent that both statutes embody certain protections to consumers who are at risk of losing online personal property and information. Furthermore, both statutes aim to protect personal data that, if found to be in the wrong hands, could cause severe exposure of confidential information.

Medical records contain data ranging from Social Security numbers, payment history, current medications and diagnoses, as well as contact information. However, in examining the data stored by businesses using the cloud, it is not uncommon to see much of the same information. In *Wyndham*, for example, the hotel's property management system contained customer's "names, home addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes."[90] The similarities between medical and business records provide merit that this type of information should be protected under a similar and consistent approach.

85. *See generally* Health Insurance Portability and Accountability Act, 45 C.F.R. §§ 164.308–312 (2014).

86. *See generally* Health Insurance Portability and Accountability Act, 45 C.F.R. §§ 164.312 (2014).

87. § 164.312(a)(1) (emphasis added).

88. § 164.312(a)(2) (emphasis added).

89. § 164.312(d)–(e).

90. F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3rd Cir. 2015).

As a result, this last alternative calls for the implementation of a rule by the FTC that would resemble the "Technological Safeguards" from the Security Standards for the Protection of Electronic Protected Health Information. Given that the FTC's guidebook on protecting personal information for businesses provides for much of the specifics in a manner like that of HIPAA's Technological Safeguards, it must be stressed that this guidebook is not a sufficient source of authority and thus cannot be relied on as a source of law. Instead, the FTC will have to use other means in accomplishing this task.

Although the FTC lacks the power to use its guidebook as a source of law, the FTC does have the power to make and create new laws by the powers vested in it by Congress. This can be done in one of two ways. The FTC can first begin by referencing HIPAA's Technological Safeguards in its adjudicative proceedings as a fair and reasonable cybersecurity measure that should be hereafter followed by future potential violators in the business setting. This case-by-case process would allow the FTC to visualize and ascertain if HIPAA's Technological Safeguards could adequately provide the missing link in justifying specific and reasonable cybersecurity measures. Furthermore, businesses that contain personal consumer information via cloud computing will therefore be afforded proper notice upon the FTC's intentions to utilize this new standard as a viable method.

As more cases concerning the adequacy of businesses' cybersecurity measures shape the agency's proceedings, the FTC may decide to take their second option and promulgate a new rule that mimics HIPAA's safeguards under its authority from Congress. Under Title 15 of the U.S.C.A. §57(a), Congress has provided the FTC the power to make "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce" and such rules "may include requirements prescribed for the purpose of preventing such acts or practices."[91]

Creating a rule in this manner requires the FTC to follow several procedural milestones. In order for its creation, the FTC must first publish notice of its proposal and state "with particularity the text of the rule," as well as provide its reasoning.[92] The FTC must also allow any interested persons to submit their arguments and views of the proposed rule as well as make these comments publically available.[93] In addition, the FTC must provide an opportunity for an informal hearing that must be in compliance with Title 15 of the U.S.C.A. § 57(c).[94] Lastly, the FTC must promulgate, if appropriate, a final rule in accordance with the rulemaking record.[95] This includes the rule itself, a

91. Federal Trade Commission Act, 15 U.S.C. § 57a(a)(1)(B) (2012).
92. § 57a(b)(1)(A).
93. § 57a(b)(1)(B).
94. § 57a(b)(1)(C).
95. § 57a(b)(1)(D).

statement of basis and purpose, the transcript, any written submissions, and any other relevant information.[96]

Therefore, assuming the FTC abides by these requirements, the agency can utilize HIPAA's Technological Safeguards to promulgate their own specific standards. By creating a rule that mimics the Technological Safeguards, the FTC can provide the cloud providers and businesses an efficient rule that is proven to work, as well as define with specificity what the FTC desires when viewing a business's cybersecurity measures. Furthermore, a similar rule provided by the FTC would allow for more consistency in the protections of personal property and information that is stored online.

## VI. Conclusion

As the technological world advances, it is imperative that the laws that govern the cyber world adjust to its dynamics. Today, more and more people are finding themselves subject to having their personal information stored with the use of cloud computing. With the online storing of personal information such as names, addresses, Social Security numbers, debit and credit card numbers, and even medical diagnoses, people are continuously at risk over not only privacy concerns, but also major financial concerns in the event of a cybersecurity attack.

To battle the elements of this inevitable harm, the FTC has taken multiple steps in cracking down on businesses that fail to provide adequate cybersecurity measures for their consumers. Often, the FTC thoroughly investigates the business' online data infrastructure only to find severe shortcomings that are deemed unreasonable in terms of Title 15 of the U.S.C.A. § 45(n). In other instances, however, the case may not be so close and the threshold between *reasonable* and *unreasonable* cybersecurity measures can be anywhere from a simple encryption method to a limited data access point from specific personnel only.

Therefore, this uncertainty calls for additional specifics in the FTC's administrative proceedings in order to fill the void. Although the FTC has wide discretion in its rulings, this Note proposes that the agency attempt to follow the path the Department of Health takes in protecting important medical documents located online. Under HIPAA's Technological Safeguards, the desired additional specifics pertaining to cybersecurity measures are readily available for the FTC. Through adjudicative proceedings, the FTC can acquire a general sense of how the rule should be applied. Thereafter, so long as the desired results have been accomplished, the FTC should implement formal rulemaking proceedings that essentially mimic HIPAA's Technological Safeguards.

96. § 57a(e)(1)(B).

Creating a rule with such similarity will only lead to benefits for all parties involved. Businesses that store consumer information online will now have a consistent rule on what cybersecurity measures must be accomplished regarding their consumers in order to avoid an FTC action. Consumers who are most at risk will now have adequate protections afforded to them on a much broader and readily known scale. Lastly, the FTC will benefit by providing a rule that has been proven to work in other administrations, thus relieving the worry for uncertainties.

In conclusion, society's reliance on the internet and the cyber world is continuing to grow exponentially. By way of technology, consumers now have the power to stay connected virtually anywhere. Consumers can now purchase products with the touch of a button and can create various accounts with multiple websites. Unfortunately, these processes often require the consumer to provide personal information that is stored via cloud online databases. As a result, consumers are subjecting themselves to vulnerability by way of identity theft, privacy concerns, and financials harms. It is therefore imperative that the legal implications surrounding the cybersecurity measures also remain dynamic and continue to evolve.