70 Rutgers U. L. Rev. 717

Rutgers University Law Review
Spring, 2018

Note
Michael A. Stoolman[a1]

THE CAUSE OF ACTION FOR BREACH OF DATA?: THE PROBLEM WITH RELYING ON COURTS WHEN MANAGING THE RISKS OF CLOUD SERVICES

TABLE OF CONTENTS

*718 I. INTRODUCTION

"If you spend more on coffee than on IT security, then you will be hacked. What's more, you deserve to be hacked."[1] If, as author and former Special Advisor to the President for Cyberspace Richard A. Clarke[2] suggested in his keynote address at the 2002 RSA Conference, a cup of coffee's worth of cybersecurity measures is inadequate, how much should a company spend to protect its information? How can that amount even be calculated? One certainty, as the above quote warns, is that attacks will not soon subside. Today's reality of the pervasive threat to cybersecurity is made obvious by the range of headlines inundating the news cycles. From the Yahoo! breach of more than one billion user accounts,[3] to the distributed denial of service cyberattack on Dyn, rendering websites like Twitter, Netflix, and PayPal inaccessible,[4] the year 2016 alone showed no relent. And the threat is not limited to the commercial context--education,[5] national security,[6] and even politics[7] have all been venues for cyberattacks.

While appreciating the entire scope of the problem, this Note will more narrowly attempt to identify how a company should make the decision of contracting with a cloud services vendor. This involves assessing the harm and risk of a data breach, traversing the relevant legal framework, and, if necessary, spreading that risk through insurance.

This Note will begin with a background discussion in Part II that provides the history of data breaches and the magnitude of the consequential harm that follows.[8] Part III will identify the specific ***719** problem that companies face when contracting with information technology ("IT") service vendors for cloud-based services, including data storage. It will then examine the law relevant to disputed rights and obligations following a data breach and why companies will likely be without significant legal redress against their vendors, under theories in either contract or tort.[9]

Acknowledging this reality, Part IV will analyze a company's choice of cloud-computing as a cost-benefit analysis, the calculation of which requires due diligence on both the vendor and the jurisdictional notice requirements for a breach.[10] Even after this front-end risk is assessed, gaps may remain. Part V will introduce the emerging cyber insurance market designed to more adequately spread this risk, acknowledging that the law may not be fully up to speed in this rapidly-evolving area.[11]

Finally, Part VI will conclude this Note and propose a company's wisest choice is to assess risk proactively at the onset of an IT service agreement, filling any gaps with a cyber insurance policy, rather than relying on the uncertain and, at times, esoteric judicial system to reactively remedy any harm.[12]

II. BACKGROUND

A. The History of Data Breaches

It is difficult to pinpoint the birth of the data breach. While it is true the use of internet-based services to store data is a recent advancement, societies have been securing information since ancient times.[13] Julius Caesar used a letter-substitution code to share information with military officials without divulging the substance of the messages to his enemies.[14] The impact of the "Caesar cipher" remained through the golden age of radio nearly two millennia later, when companies would ***720** encode

messages to their customer-listeners as a sales gimmick.[15] Whether for guarding state secrets or simply for fun, cryptography, or "the practice of hiding information so that unauthorized persons can't read it," has long been present in human societies.[16]

With the advent of internet computing in the 1980s came the ability for companies and governments to store much larger amounts of individuals' data than ever before, due to larger and more complex information systems.[17] But so too were the vulnerabilities of such systems displayed during this decade.[18] In 1984, global credit information corporation TRW (now known as Experian) suffered a data breach resulting in the loss of ninety million records.[19] In 1986, Revenue Canada suffered a sixteen million record loss as result of a data breach.[20]

In the healthcare sector, Congress responded by enacting the Health Insurance Portability and Accountability Act ("HIPAA") in 1996, specifically Title II.[21] HIPAA Title II established national standards for protecting individuals' medical records and other personal information in the midst of the newly electronic nature of health care transactions.[22] Title II also established a Fraud and Abuse Control Program, and currently mandates that the program's guidelines "shall include procedures to assure that [information by health plans, providers, and others] is provided and utilized in a manner that appropriately protects the confidentiality of the information and the privacy of individuals receiving health care services and items."[23]

Spreading beyond healthcare, the threat of data breaches and personal information loss led to increased public awareness in the early 2000s.[24] In September 2002, California became the first state to enact ***721** legislation that required both public and private organizations to promptly notify Californians of any data breach that could possibly compromise the data subjects' personal information.[25] This legislation followed the breach of a state-operated data storage facility holding social security numbers, first and middle initials, last names, and payroll deduction amounts of California state employees.[26] The breach was not discovered until a month after it occurred, and the affected employees were not notified until two weeks after that.[27] Under the belief that "the earlier you know, the easier it is for you to stop the damage," the notification requirement was the "heart" of the California act.[28] Under the law, the disclosure had to be "expedient" and made "without unreasonable delay."[29] This concept of mitigation by notification will be discussed in greater detail, with a comparison of different jurisdictions' notification requirements later in this Note.[30]

Today, the types of attacks and variations of victims continue to expand. The Target Corporation breach, which has become a well-known staple in the literature on modern breaches,[31] remains a classic example of hackers obtaining customer information from a large retailer.[32] Credit card-present transactions are a reliable source for stealing card data; the breach is dubbed a "point-of-sale intrusion."[33] But it is clear the landscape is changing when "hacktivists" breach the website of Ashley ***722** Madison, a site designed specifically to facilitate extramarital affairs.[34] Interestingly, this breach was no moral crusade against adultery, but rather done to "expose alleged lies Ashley Madison told customers about a service" regarding payment of fees.[35] To call the future of these attacks unpredictable is an understatement.

B. Measuring the Harm of a Data Breach

Before attempting to measure the harms associated with data breaches, it is helpful to define the term precisely. The Ponemon Institute's *2016 Cost of Data Breach Study* defines "data breach" and its causes as:

> [A]n event in which an individual's name plus Social Security number, medical record and/or a financial record or debit card is potentially put at risk-- either in electronic or paper format. In our study, we have identified three main causes of a data breach. These are a malicious or criminal attack, system glitch or human error. The costs of a data breach can vary according to the cause and the safeguards in place at the time of the data breach.[36]

While a "system glitch" or "human error" are causes under the definition, most data breaches are caused by "criminal and malicious attacks."[37] Per the study's sample of sixty-four U.S. organizations that suffered a breach, 50% of attacks were by criminal and malicious attacks, while only 23% were by human error and 27% by system glitches.[38]

The significance of this lies in the fact that criminal attacks require the most time to detect and contain, and therefore ultimately cost more.[39] In fact, the cost of data breaches in the United States has continually risen since 2013 and reached a record high in 2016, the last year studied.[40] The calculated per capita cost[41] of data breaches in the United ***723** States was

$221 million in 2016.[42] This figure is made up of both direct and indirect costs; direct being those "incurred to resolve the data breach such as investments in technologies or legal fees," totaling $76 million, and indirect being "abnormal turnover or churn of customers," totaling $145 million.[43] Indirect costs have consistently been around two to three times larger than direct costs since 2006.[44]

As for the average cost per organization affected, the data is more ambiguous. Following 2011, where average cost per organization was highest at $7.24 million, costs decreased significantly in 2012 and 2013 to around $5.5 million.[45] However, there has since been a steady increase--from $5.4 million per organization in 2013 to $7.01 million per organization in 2016--suggesting a trend of increasing costs in the future.[46] An explanation for the inverted trend may be due to the size of breaches increasing by five percent from 2015 to 2016 alone, as well as customer loss, or "abnormal churn," increasing by three percent during that time, both contributing to higher indirect costs.[47]

Globally, the average cost of a data breach for an organization is only four million dollars, about three million less than in the United States.[48] The United States, not shockingly from the numbers above, faces the costliest data breaches of all twelve countries studied in the Ponemon Institute's global report.[49] Global figures also suggest the same causation statistics as those from the U.S. report--about half are caused by criminal or malicious attacks, while human error and system glitches each account for about a fourth of all breaches.[50] One difference between the U.S. study and the global study is the industries affected. In the United States, the industries most affected are health, life sciences, and ***724** finance, respectively.[51] Globally, the order of most affected industries are: healthcare, education, and then finance.[52]

Because most data breaches occur from criminal and malicious attacks, it may be helpful to identify the actors and their motives. First, despite the fear of an attack from within, the reality is that over eighty percent of all attackers come from outside the firm.[53] External actors can be financially motivated criminals, "hacktivists," or even nation-state actors.[54] While not as common, internal actors like rogue or disgruntled employees, or even recruits of competitors, can also be to blame.[55] Considering data over the past six years, the primary motive of the actors resoundingly continues to be that of financial gain with a far-away second being espionage.[56] Other motives such as simple fun, ideology, and grudges make up a miniscule percent of actors' purposes.[57] Still, the idea of "secondary motive" exists, meaning while financial gain might have been the primary reason for the attack, another one of the above secondary motives might have also been present, and yet not represented in the data.[58]

Maybe most alarming is the time needed to execute a breach or, frankly, the lack thereof. The actual compromise of data requires only days, if not minutes or seconds.[59] And attackers are becoming even quicker, as phishing techniques can now be accomplished within seconds.[60] Exfiltration of data can also occur within days, and sometimes within minutes or seconds.[61] But this "days or less" timeframe is, unfortunately, not reciprocated by the time it takes to discover the breach.[62] Data from 2015 shows that while nearly one hundred percent of compromises occurred within "days or less," only about twenty-five ***725** percent of discoveries occurred within "days or less."[63] This disparity, according to the data, is only getting worse.[64]

As discussed, the longer the delay in discovery, the higher the ultimate cost of the breach. Being such a significant monetary harm, the question naturally turns to the relevant legal rights and obligations of the parties affected by a breach.

III. THE LAW AND ITS SHORTCOMINGS

Facts arising out of a data breach can support theories of legal liability. A company that enters into a contract with an IT service vendor for data storage potentially has a claim for breach of contract when that data is breached. Alternatively, a company could claim the vendor was negligent in allowing a breach to occur. While both contract and tort theories seem plausible, the legal doctrine, in addition to the law in practice, likely either diminishes or entirely precludes both claims. Another theory is in bailment. While creative, it has shown similar ineffectiveness in court. This section will explore these causes of action and ultimately determine that the significant harm of a data breach may not be actionable under traditional legal avenues.

A. The Specific Problem for a Company Using the Cloud: A Rock and a Hard Place

In light of a data breach's potential multi-million dollar harm, a company should carefully review its IT service contract's

fine print, as this can be central in determining liability shifts between it and its cloud-hosting vendor.[65] Contracting away a vendor's liability altogether, or even just certain types of liabilities, can be devastating to the company in the event of a data breach.[66] Even if there is an express warranty to keep data confidential (and thus such warranty would be breached by the vendor in the event of a compromise) the breach of warranty remedy may ***726** be severely diminished by damages limitations.[67] Indemnity provisions implicating the vendor may be just as futile if the vendor is only required to indemnify third-party claims by individual victims against the company, and not class-action claims; the much more common and practical route in data breach cases.[68]

The effect of these contractual protections for vendors can be the subject of litigation.[69] In *Silverpop Systems, Inc. v. Leading Market Technologies, Inc.*, marketing company Leading Market Technologies ("LMT") contracted with IT services vendor Silverpop Systems ("Silverpop") to store its advertising content and recipient email addresses on Silverpop's web-based email-marketing system.[70] Silverpop's network was hacked, and LMT's list of roughly 500,000 user email addresses was possibly exported by third parties.[71] Silverpop sought a declaratory judgment requesting that, because any loss of value incurred by LMT was merely consequential to any breach of contract, it should therefore not be recoverable under the damages limitation in the service contract, which extinguished Silverpop's liability for any consequential damages.[72] Conversely, the direct harm, measured as the "benefit of the bargain," would be simply the monthly cost of the service.[73] The Eleventh Circuit agreed that this harm was consequential rather than direct, and so barred such recovery under the damages limitation provision in the contract.[74]

Silverpop signifies the importance of how courts characterize the harm of a data breach, and that limitations of liability or damages in IT service contracts will generally be given great deference. LMT's dilemma placed it between the "rock" of angry and litigious consumers, and the "hard place" of a vendor who is not liable for anything other than the monthly cost of the service. This problem presents choices for companies ***727** like LMT: either go to court after a breach and face the precedent of *Silverpop*, or manage this risk in other ways before turning to the cloud. For the reasons that follow, theories in contract, tort, or even bailment will likely fail for companies like LMT, making going to court largely unviable.

B. Contract Law

1. Goods or Services: Which Law Applies?

When a vendor provides cloud-hosting services to a company for a fee, a "standard service contract[]" creates a legal relationship between the vendor and the company.[75] A service, as opposed to a good, is an "intangible commodit[y]."[76] The distinction prescribes the applicable law: a contract for the sale of goods will be governed by the *Uniform Commercial Code* ("UCC") as enacted in the relevant state,[77] while a contract for services will be governed by the common law, or "general contract law," of the state.[78] When the contract involves a transaction of both goods and services, it is deemed a "mixed" contract.[79] To determine which law applies, most courts ask whether the predominant factor of the transaction involves the services rendered or the goods sold.[80] Contracts involving the transfer of intangible goods such as data fall under the traditional "services" definition and are therefore governed by common law, and not the UCC.[81] This categorization is not without controversy. Critics have argued that in today's "information age," service contracts ***728** are much more prevalent, and it is backwards to exclude them from our uniform body of commercial law.[82]

Still, and for the purposes of this Note, IT service contracts are likely to be held outside the scope of the UCC, so the analysis will be grounded in common law contract doctrine. The distinction may not ultimately matter, as the UCC mirrors the common law in its treatment of consequential damages limitations-- the substance of the following analysis.[83]

2. Measuring the Harm, Limiting Liability, and Policing the Agreement

The remedy for breach of contract is often calculated to put the injured party in the position in which she would have been had the contract been performed.[84] This is commonly referred to as protecting the expectancy interest or "the benefit of the bargain."[85] Placing the injured party in the rightful position, however, may require more than compensating the *direct harm* of the breach. Additional harm that occurs as a *consequence* of the breach of contract may also be recoverable. Consequential damages, sometimes referred to as special damages, however, require a certain degree of knowledge by the breaching party

when the contract is formed.[86] The classic case, a staple in the first-year contracts course, is *Hadley v. Baxendale*, where it was held damages are recoverable only where the loss "may reasonably be supposed to have been in the contemplation of both parties, at the time they made the contract, as the probable result of the breach of it."[87] In *Hadley*, failing to deliver a crank shaft to a mill in breach of contract did not warrant liability for the mill's resulting lost profits, as that was not to have been ***729** reasonably "in the contemplation of both parties" when they made their agreement for the crank shaft.[88]

What exactly it means to be "in the contemplation" of a party remains murky and subject to a separate academic debate.[89] Not surprisingly, parties contract around this unpredictability through damages limitations provisions, limiting contract remedies solely to direct harm, if any harm at all.[90] A typical provisions may appear as follows: "IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, PUNITIVE, SPECIAL OR OTHER DAMAGES WHATSOEVER ...."[91] Additionally, the limitation on liability provision will cap all liability to a U.S. dollar amount reflecting the direct damage.[92] Placing these clauses in the contract effectively removes any *Hadley* foreseeability question, and under both common law and the UCC, agreed-upon limits on remedies are generally enforceable.[93] The exception, both at common law and under the UCC, is triggered when the remedy limitation is unconscionable.[94]

Unconscionability, another foggy contracts doctrine, polices agreements or terms that "include an absence of meaningful choice on the part of one of the parties together with contract terms which are unreasonably favorable to the other party."[95] The absence of meaningful choice is the "procedural" component, evidenced by fine print, convoluted language, lack of understanding, and unequal bargaining power between ***730** the parties.[96] Unreasonably favorable terms to one party that are "plainly oppressive" to the other constitute the "substantive" component.[97] For the agreement or term to be voidable on these grounds, courts usually must find both procedural and substantive unconscionability as a matter of law.[98] While both the UCC[99] and common law[100] clearly enshrine unconscionability, the reality is that "judges have been cautious in applying the doctrine ... recognizing that the parties often must make their contract quickly, that their bargaining power will rarely be equal, and that courts are ill-equipped to deal with problems of unequal distribution of wealth in society."[101] The doctrine is especially dormant in large-scale transactions; as the Ninth Circuit has noted, "it makes little sense in the context of two large, legally sophisticated companies to invoke the ... unconscionability doctrine."[102]

3. Contract Law Applied to the Cloud

In the context of IT service contracts, remedy limitations routinely appear, protecting vendors by drastically decreasing their exposure to liability in the event of a data breach.[103] One document management company's "Terms & Conditions" includes the following clause:

> IN NO EVENT WILL [VENDOR] BE LIABLE FOR DAMAGES OF ANY KIND, UNDER ANY LEGAL THEORY, ARISING OUT OF OR IN CONNECTION WITH YOUR USE, OR INABILITY ***731** TO USE, THE SERVICES OR ANY WEBSITES ASSOCIATED WITH IT, INCLUDING ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, INCLUDING BUT NOT LIMITED TO, PERSONAL INJURY, PAIN AND SUFFERING, EMOTIONAL DISTRESS, LOSS OF REVENUE, LOSS OF PROFITS, LOSS OF BUSINESS OR ANTICIPATED SAVINGS, LOSS OF USE, LOSS OF GOODWILL, LOSS OF DATA, AND WHETHER CAUSED BY TORT (INCLUDING NEGLIGENCE), BREACH OF CONTRACT OR OTHERWISE, EVEN IF FORESEEABLE.[104]

This waiver, while perhaps overly-expansive,[105] includes the preclusion of consequential damages, "even if foreseeable."[106] In the data breach context, it then becomes necessary to define the type of harm as either direct or consequential.[107]

This was precisely the question discussed earlier in *Silverpop*, where LMT was seeking damages for the loss of value of its compromised email list.[108] Because of Silverpop's damages limitations provision, the characterization of the harm was dispositive--the vendor was only liable for direct harm.[109] Applying common law, the Eleventh Circuit held that direct damages "compensate for the value of the very performance promised" or, as it may be stated, the "loss of the benefit of the bargain," while consequential damages remedied those "additional losses ... that are incurred as a result of the defendant's breach."[110] Lost market value of the email list was held to be consequential.[111] While a confidentiality provision for the data existed in the parties' contract, it was only ***732** incidental to the purpose of the agreement: email marketing--not the safe

storage of LMT's information.[112]

The holding of *Silverpop* suggests that if confidentiality is not the primary purpose of the vendor's service, any harm resulting from a breach will necessarily be consequential and unrecoverable due to the pervasive practice of including damages limitations in these contracts.[113] Any challenge to a provision's enforceability because of unconscionability is likely futile, as the doctrine's procedural prong is rarely at issue when two sophisticated companies are dealing.[114] This may be disheartening to companies that entrust their data to cloud-service providers because, as discussed in Part II, the indirect costs of data breaches--including loss of customer goodwill through "abnormal turnover or churn," or as in *Silverpop*, the loss of value to its customer information--were two to three times larger than direct costs this past decade.[115]

Even if, after realizing this, companies bargain for access to consequential damages and vendors remove remedy limitations, a question remains whether this kind of harm would fall outside the common law's default position of compensating only direct harm. The rule of *Hadley v. Baxendale* may be just as problematic for companies as remedy limitations since the compensation of indirect harm is much more the domain of tort law.[116] Companies might find hope in a recent class action against Anthem, Inc. where plaintiffs survived a motion to dismiss in a case seeking consequential damages after the Anthem data breach.[117] The district court's finding that no California contract law precluded awarding consequential damages in a data breach case may be analogous to companies claiming similar remedies against vendors. Still, *In re Anthem* regarded claims of the actual victims of the breach, and the case was only at the motion to dismiss stage.[118] Ultimately, it is unlikely vendors will remove consequential damage limitations anyway, ***733** especially after the credence given to them in *Silverpop*. Contract law may simply be of no help to companies in such situations.

C. Tort Law

It may seem that where data has been breached through the vendor's negligence, the applicable cause of action is obvious--negligence. At least with regard to physical and emotional harm, "[a] person acts negligently if the person does not exercise reasonable care under all the circumstances."[119] The negligence cause of action has five elements: duty, breach, cause in fact, scope of liability (proximate cause), and harm.[120] Ostensibly, a negligence cause of action fits in the data breach setting: the vendor breached its duty of reasonable care in storing the data, which caused harm to the company--harm that is within the scope of foreseeable consequences of the behavior that made the act tortious. The problem arises, however, because of the *type* of harm.

The harm this Note has discussed has been neither physical nor emotional. Instead it falls within the category of "economic loss," defined as: "pecuniary damage not arising from injury to the plaintiff's person or from physical harm to the plaintiff's property."[121] Viewing this harm distinctly, tort law rejects any general duty to avoid unintentional infliction of economic loss onto another,[122] especially where the harm is caused by negligent performance of a contract.[123] Neither can a party recover for economic loss caused by the unintentional injury to a third person or property in which the party has no proprietary interest.[124]

Essentially, the economic loss rule precludes a tort cause of action for an otherwise breach of reasonable care that results in purely pecuniary loss.[125] This categorical exclusion is grounded in the belief of a "meaningful distinction between contract law and tort law, and that in ***734** cases of potential overlap, contract law is a superior system for regulating behavior and achieving socially optimal results."[126] Where harm is purely monetary, and especially where the duty arises out of a contract, the breach of duty is not actionable as a tort.[127] And while there is sometimes a distinction between applying the economic loss rule in the context of goods but not services, if a contract exists for the services, the economic loss rule incontrovertibly applies.[128]

In the cybersecurity setting, the economic loss rule has been in full force.[129] These cases involve precisely the type of harm the economic loss rule refuses to remedy: pecuniary harm.[130] The rule impacts both individual victims as well as the companies who use pay-for-cloud services. Individuals affected by data breaches face the economic loss rule when bringing negligence actions against the compromised companies.[131] In *Dittman v. UPMC*, a Pennsylvania court cited the economic loss rule in rejecting a common law negligence cause of action for a data breach.[132] Independently of the economic loss rule, the court found strong public policy in requiring the legislature, and not the courts, to create such a duty of care in the electronic storage setting.[133] The court was not prepared to undermine the economic loss rule.[134]

Tort bars are not limited to individual victims. Again, using *Silverpop* as an example, companies suing vendors for resulting

harm of the breach face the same obstacle of the economic loss rule and are likely stuck with their contract claims.[135] Ironically, it is believed contract causes of action more appropriately determine how to remedy the consequential harm of ***735** a data breach.[136] But as noted in the previous section, contract law effectively disregards consequential damages, pointing instead to tort law for remedy. It becomes clear, through this circular rationale where contract is pointing fingers at tort, and tort pointing right back, companies face serious challenges in seeking legal redress for the harm of a data breach from their vendors.[137]

D. Bailments

A final legal theory relevant to this discussion may be a bailment cause of action. Bailment is a property doctrine that "occurs when there is delivery of personal property by a prior possessor to a subsequent possessor for a particular purpose with an express or implied understanding that when the purpose is completed the property will be returned to the prior possessor."[138] The bailor transfers property to the bailee, who must have physical control over the property and an intention to exercise that control.[139] Attaching to the delivery is bailee's duty of care, the standard of which depends on the type of bailment: gross negligence in bailments for the sole benefit of the bailor, slight negligence in bailments for the sole benefit of the bailee, and ordinary negligence in bailments for the mutual benefit of both bailor and bailee.[140] Ordinary negligence is the prevailing standard for bailments resulting in accidental loss or damage to the property, though strict liability may be ***736** the standard in cases of improper delivery to someone other than the bailor-owner.[141]

Damages incurred by bailor because of bailee's negligence are bases for tort causes of action independent of any breach of bailment contract.[142] Not only are tort damages available, but the measure of contract damages is notably unique in the case of a bailment.[143]

The dichotomy remains one of direct and consequential harm, but in some cases direct harm is characterized quite differently.[144] While breach of contract before the bailment begins only measures the loss of the bargain, where the breach of contract occurs during the bailment, bailor's direct harm is "generally the loss of property from an injury to the chattel."[145] So too are consequential damages recoverable when contemplated.[146] However, just as in contract, limitation on liability for bailed goods can be agreed upon by the parties at the outset.[147]

The benefits of a bailment cause of action to bailee also exist in tort, as it is not clear the economic loss rule applies to negligence claims arising out of bailments.[148] Regardless, the opportunity to present two causes of action--both seemingly more flexible than their traditional forms--makes bailment a serious consideration for lawyers.

In the cyber context, the transferring of data has been argued to constitute a bailment.[149] While "novel" and "creative," courts have resoundingly rejected the bailment claim for a data breach.[150] In *In re Target*, a class of plaintiffs alleged a claim for bailment, arguing Target, ***737** as bailee, wrongfully lost their bailed personal financial information.[151] The court agreed intangible personal information could constitute bailed property, but that there was never an agreement that Target would return the property to plaintiffs, an element of bailment formation.[152] Also, the court noted it was not Target who wrongfully retained their information, but rather third party criminals.[153]

This analysis has been criticized by Professor Todd Ommen,[154] who questions courts' overall dismissiveness of independent bailment claims in these cases.[155] An existence of a distinct injury is critical because, as Ommen and this Note point out, other "duplicative" claims (breach of contract and negligence) get dismissed.[156] Surviving motions to dismiss may allow bailment claims to get the attention they deserve from courts.[157]

However, bailment claims are subject to the same consequential damages limitations hindering contract claims. Interestingly, though, because certain bailments allow more generous characterizations of direct harm, a question is presented of whether consequential damages limitations would even be pertinent in such a case.[158] On the tort side, because the economic loss rule may not apply to bailments, pure economic recovery might very well be possible in a data breach suit. Still, as shown, ***738** courts have rejected the bailment theory at the motion to dismiss stage, making many of these points rhetorical.

Ultimately, whether in contract, tort, or bailment, litigation may not provide companies the redress they seek against vendors after suffering harm from a data breach. Acknowledging this, it then becomes a question of how companies should manage this risk.

IV. A COST CALCULATION: DO IT YOURSELF OR RISK THE CLOUD

Understanding that litigation against vendors might not be a viable avenue after a data breach occurs, there are considerations companies should take when contracting for cloud services. To clarify, the term "cloud" can most simply be defined as the Internet.[159] "Cloud computing" services involve the delivery of software, platform, or infrastructure resources over the Internet, scaled to the customer's demand and billed to the customer either by use or for a fixed time.[160]

The cloud can be distinguished as either public or private. Public cloud data centers are located at the vendor's site and available to multiple subscribers, while private cloud data centers are on-site and not shared by other organizations, with the company itself managing the infrastructure.[161] Some private cloud computing is do-it-yourself, while others are also through vendors charging monthly payments (payments much higher than public cloud services due to the leasing of the physical infrastructure).[162]

In determining whether to subscribe to cloud services, a company should consider two things. First, the company should research its prospective vendor. Due diligence will provide the company a better idea of the cybersecurity risks it faces. Second, the company should consider applicable states' data breach notification laws. This jurisdictional consideration informs the company if, and/or how long, the vendors have ***739** to notify it of the breach.[163] This is key as time can be of the essence in mitigating damage. Ultimately, it is a balance of costs--while the cloud service will be cheaper and more flexible, the risks that accompany such a service should be weighed against that convenience.

A. Due Diligence: Researching the Vendor

Due diligence on a potential vendor's security protocols helps companies determine that vendor's risk of breach.[164] Additionally, due diligence on vendors' finances gives companies an idea of their vendors' capability of satisfying obligations that arise out of a data breach.[165] Due diligence can be accomplished through a questionnaire inquiring into the "provider's financial condition, insurance, existing service levels, capacity, physical and logical security, disaster recovery, business continuity, redundancy, and ability to comply with applicable regulations."[166]

The company should also understand the physical condition of the security infrastructure and data center. "Best-in-class" data centers are audited by the Auditing Standards Board, which reports on compliance with regulations.[167] Evidence of such compliance can be accessed by prospective customers.[168] It is also desirable that the vendor own the server equipment, as ownership removes any limitation to the vendor's ability to control and support the cyber infrastructure.[169] Other physical concerns should be the use of backup power generators, fire and flood prevention systems, and video surveillance on the premises of the data center.[170] The geographic location (or locations if more than one)[171] of the data center is important in determining the geographic boundaries of ***740** service.[172] Finally, companies can ask the vendor for a tour of the data center facilities.[173]

Other inquiries should be tailored to the information that the company is seeking to store as well as its overall risk profile.[174] Two variables are primarily involved in the risk assessment: "(1) the criticality of the business process being supported by the cloud computing solution, and (2) the sensitivity of the data that will be stored in the cloud."[175] A Foley & Lardner LLP report identifies three levels of risk, each depending on the magnitude of those two variables: low, medium, and high risk.[176]

Based on that risk profile, due diligence will achieve a better idea of whether such risk is being adequately addressed. Questions could regard the vendor's security guidelines, policies, and procedures, and whether the vendor's protections actually mirror those the vendor itself uses for its own data management.[177] The company's risk profile will also inform the customer of the contractual language that should be included in the service agreement-- language, as discussed, that is given great deference.[178] Certainly a warranty for confidentiality, an indemnification of claims by third parties, and at least an attempt to reinstate consequential damages are all recommended.[179] Less obviously, companies should seek to obligate the vendor's regulatory compliance; establish customer support hours, asset maintenance, and disaster recovery plans; bargain for breach of warranty remedies; and identify cure provisions in the event of material breach of the contract.[180] ***741** Tailoring the contract to the specific needs of the company addresses the risks identified from due diligence.

B. State-by-State Notification Requirements

The other major component of a company's risk profile consists of the applicable state notification laws. Statutes vary from jurisdiction to jurisdiction on exactly what duties companies have in notifying affected individuals of a breach.[181] In fact, forty-seven states,[182] the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have all implemented such laws.[183] As discussed earlier, California was the trailblazer in instituting the first data breach notification law.[184] All states that have notification laws also place duties on vendors and service providers to notify their customers after a breach, who must then notify the affected individuals.[185]

These laws are important because "the longer it takes to detect and contain a data breach the more costly it becomes to resolve."[186] Therefore, the shorter a vendor has to notify its customer of a data breach, the quicker the company can then notify affected individuals and begin to contain the harm. Because timing is key, when notice must be given should always be identified and considered in risk analyses.

Most of these notification laws include similar language: "[F]ollowing discovery or notification of the breach in the security of the system ... [t]he disclosure shall be made in the most expedient time possible and without unreasonable delay ...."[187] This could mean sixty days, if not ***742** sooner.[188] Notification methods can be governed to include written notice, electronic notice, or even telephone notice.[189] The content of the notice may be required to include a description of the incident; what kind of personal information was accessed or acquired; a description of the company's plans to avoid further access; and telephone numbers of the company, consumer reporting agencies, as well as state and federal law departments.[190]

It then becomes an issue as to which state law applies. It is clear that a company's duty of notification to affected individuals is determined by the state law of where the *individual* resides.[191] Therefore, a single data breach can involve multiple notification requirements if victims reside in various states.[192] But because these laws also obligate service providers to notify their customers of the breach, the question then becomes: under which state law does the service provider's duty arise?

The answer may also be jurisdiction-specific, as some state laws seem to provide guidance. In New Jersey, the service provider's duty to customers is still triggered by the customer's duty to New Jersey residents affected by the breach.[193] Therefore, regardless of where the cloud vendor is located, or where the company does its business, both vendor and customer have obligations under New Jersey law if the data breach involves personal information of a single New Jersey resident. It necessarily follows that companies should be analyzing their duties and protections under any state in which their data subjects may reside.

Some states give vendors a specific time frame to notify their customers after identifying a breach; that time being merely ten days in Florida.[194] Other variations include a definitional exclusion for loss of encrypted data[195] and for allowing delay in notification when law enforcement is involved.[196] It would serve a company well to analyze the ***743** potentially applicable state notification laws to get a better idea of both the time it is owed by vendors, and the time it owes affected victims.

After a company seeking cloud services does its due diligence and performs jurisdictional-specific research, the ultimate decision of whether to use the cloud or not will come down to a cost/benefit analysis.[197] Cloud hosting will have the benefit of low up-front costs, while a do-it-yourself model will give the company more control.[198] But the fixed costs of self-hosting--such as assembling security strategy, training staff, monitoring new threats and countermeasures, and developing relationships with law enforcement--are expensive, and such costs can be absorbed much more easily by larger, cloud-hosted infrastructures.[199]

V. CYBER INSURANCE

While due diligence and research into applicable notification laws can greatly minimize potential risks of cyberattacks, the reality remains that data breaches are nonetheless pervasive and costly.[200] As discussed, litigating liability under traditional legal doctrines can ultimately be futile for a company that has suffered a data breach.[201] The remaining gaps, even after choosing the right cloud-service vendor and preparing for the worst, should not be expected to be filled through a court judgment. These gaps may be better addressed proactively, before any breach, through cyber insurance.

A. Cyber Insurance Background

Not only have those seeking to redress the harm of data breaches had difficulty in court, but they have also found difficulty with insurance companies, especially when making claims under traditional liability ***744** policies.[202] Cyber-based claims made under property insurance providers have run into policy exclusions.[203] Interestingly though, in *Retail Ventures, Inc. v. National Union Fire Insurance Co.*, a crime insurance policy was interpreted broadly enough to cover a loss of stolen customer information, expanding coverage by way of a proximate cause standard.[204] Still, insurance companies are aggressively denying these types of claims under traditional liability policies.[205]

This gap of coverage allowed the cyber insurance market to emerge in the late 1990s.[206] Because these policies are new, market standardization is lacking and coverage can vary significantly.[207] Most policies cover security breach liability while varying in coverage for either first-party losses or third-party losses.[208] Another distinction is the insurer's obligation of legal defense or merely the lower obligation of indemnity.[209] Today, the most effective risk spreading includes self-insuring against IT risks with a cyber policy, and requiring the cloud service vendor to be insured as well when negotiating the terms of the IT service agreement.[210]

B. Policy Coverage

A sample cyber policy from The Travelers Companies showcases coverage of both first and third party liability.[211] First party coverage will pay to the insured any direct costs incurred, including "security breach remediation and notification expenses," during the policy term.[212] First party coverage additionally covers various types of electronic fraud, ***745** extortion, and business interruption.[213] "Crisis management event expenses" will also be paid out to the insured, which covers indirect costs much like those described earlier in the Note.[214] As discussed, the costs of churn, or customer loss, can make up a significant portion of costs incurred due to a data breach.[215] Covering such indirect economic harm, this is an attempt to fill the exact gap that contract and tort law often refuse to redress.

Third party coverage includes payment on behalf of the insured, of "[l]oss" for any "[c]laim" against the insured made during the policy period for a "[n]etwork and [i]nformation [s]ecurity [w]rongful [a]ct."[216] "Loss" means defense expenses and money the insured is legally obligated to pay as a result of a claim.[217] "Claim[s]" include: demands of both damages and non-monetary relief, a civil proceeding, a criminal proceeding, administrative or regulatory proceedings, an alternative dispute resolution proceeding, or requests to toll or waive a related statute of limitations.[218] Finally, a "[n]etwork and [i]nformation [s]ecurity [w]rongful act" encompasses, among other things, unauthorized access or use of electronic or non-electronic data containing identity information and failure to provide notification of such access or use required under any applicable breach notification law.[219]

C. Studies on Cyber Claims and the Future of the Industry

With such broad coverage tailored specifically to the harms of cybersecurity, cyber insurance may be critical for any company using cloud services for personal information storage. Of course, policy premiums are not cheap, because coverage limits can be in the tens of millions of dollars.[220] A $1 million policy can mean premiums between ***746** $10,000 and $35,000.[221] And that is a small policy; varying by company size, a single insured can attain $10 to $20 million in coverage.[222] Stacked policyholders can insure up to $350 million.[223] Because the market is new, risk is often difficult to measure and premiums can vary greatly between insurers for the same coverage.[224]

A deeper question becomes whether these policies are effectively spreading risks. The NetDiligence *2015 Cyber Claims Study* analyzed actual reported cyber claims to identify real costs of such incidents.[225] Studying 160 reported incidents between 2012 and 2015, most of which were for total insured losses, multiple key findings were made.[226] The average claim for a large company was $4.8 million.[227] The average claim, generally, was $673,767.[228] Average legal defense costs were $434,354, average legal settlement costs were $880,839, and average crises services costs were $499,710.[229] Notably, average claim payouts began to decrease drastically after 2012, and have been steadily decreasing since.[230] Ultimately, the study concluded that fully assessing cyber insurance costs remains difficult and the future of risk management and underwriting in this field will depend on many more cyber claims being processed.[231]

While much is changing in the field, and much remains unknown, there is a general trend of growth and momentum in cyber insurance.[232] Niche small business insurer Hiscox released a report on cyber readiness, and among other key findings it found over a quarter of firms in the United States, Germany, and the United Kingdom planned to take out a cyber policy in 2017.[233] This is in addition to forty percent of firms in these countries reporting to have cyber insurance already.[234] The reasons ***747** behind this momentum are unsurprisingly grounded in cost reduction, peace of mind, and security.[235]

However, smaller organizations are not moving to cyber insurance at the same rate as the larger organizations.[236] Unfortunately, while bigger firms have higher costs, the very smallest firms'[237] costs are actually disproportionately higher per incident.[238] In any event, most firms are increasing spending on cyber security.[239] One benefit of cyber insurance may be that many insurers provide add-on services like employee training and preventative hardware and software, which could perhaps lower these cyber security costs for both large and small companies.[240]

Ultimately, while the market is dynamically growing, problems remain. The Hiscox study concluded that education is a challenge and that the inherit complexities of cyber insurance need to be made easier to understand.[241] The future of cyber insurance will likely mirror the future of data breaches, which continue to persist and evolve dramatically.

*748 VI. CONCLUSION

A company seeking to use cloud services for any of a multitude of reasons-- especially personal data storage--must understand the risks and costs of doing so. The harm of a data breach can be catastrophic, and studies show consequential, indirect harm vastly outweighs direct harm. It would be a mistake to rely solely on courts to resolve liability determinations in actions either by a company against its cloud vendor, or against a company by affected individuals. The law of contracts, torts, and even bailments will likely fail to remedy the significant harms of a data breach.

Instead of reactively addressing the harm post-incident, a company can proactively analyze the risk before moving to the cloud. Not only should due diligence be done on the cloud service vendor, but a careful look at the vast differences of state breach notification laws will be necessary. Even when the cost analysis justifies using a cloud service, and proper contract drafting is achieved, some significant risks remain, and a cyber insurance policy may adequately fill the remaining gaps. The future of the cyber insurance market will likely symbiotically develop with the now pervasive and growing threat of data breaches.

The problem of data breaches, while rapidly evolving, is consistent in one regard--it is not soon subsiding. While the law is a trusted mechanism of enforcing rights and obligations, it can often be ill-equipped to address new and evolving problems. The law may eventually catch up with a tailored cause of action for this problem, but for now this risk should be addressed in other ways.

Richard A. Clarke's highly-caffeinated warning at the 2002 RSA Conference is no less salient today. Microsoft president and 2017 RSA Conference keynote speaker, Brad Smith, echoed the same caution: "This is not the world that the internet's inventors envisioned a quarter of a century ago, but it is the world that we inhabit today."[242]

Footnotes

a1 J.D. Candidate, May 2018, Rutgers Law School, Camden, New Jersey. I am greatly appreciative to Distinguished Professor Jay M. Feinman, **Jordan** M. **Rand**, and the editors of the Rutgers University Law Review, all of whom made publishing this Note possible.

1 Richard A. Clarke, Special Advisor to the President for Cyberspace, Keynote Address at the 2002 RSA Conference (Feb. 19, 2002).

2 Clarke served in the White House for presidents George H.W. Bush, Bill Clinton, and George W. Bush. Dan Schawbel, *Richard Clarke: What He Learned About Leadership from the White House*, FORBES (May 23, 2017), https://www.forbes.com/sites/danschawbel/2017/05/23/richard-clarke-what-he-learned-about-leadership-from-the-white-house/#48

efdc8160f9.

[3] Vindu Goel & Nicole Perlroth, *Yahoo Reveals Largest Breach Ever Reported*, N.Y. TIMES, Dec. 15, 2016, at A1.

[4] Drew FitzGerald & Robert McMillan, *Cyberattacks Knock Out Top Websites*, WALL ST. J., Oct. 22, 2016, at A1.

[5] *See, e.g.*, Keith Wagstaff & Chiara A Sottile, *Cyberattack 101: Why Hackers Are Going After Universities*, NBC NEWS (Sept. 20, 2015), http://www.nbcnews.com/tech/security/universities-become-targets-hackers-n429821.

[6] *See, e.g.*, Nicole Perlroth, *Infrastructure Armageddon*, N.Y. TIMES, Oct. 15, 2015, at F10.

[7] *See, e.g.*, David E. Sanger & Scott Shane, *Russian Hackers Acted to Aid Trump, U.S. Says*, N.Y. TIMES, Dec. 10, 2016, at A1.

[8] *Infra* Part II.

[9] *Infra* Part III.

[10] *Infra* Part IV.

[11] *Infra* Part V.

[12] *Infra* Part VI. I owe much to **Jordan** M. **Rand** for his suggestion of organizing the Note in this way, and for his help in providing both materials and understanding in this topic. Telephone Interview with **Jordan** M. **Rand**, Partner, Klehr Harrison Harvey Branzburg LLP (Dec. 22, 2016).

[13] *See* JOANNA LYN GRAMA, LEGAL ISSUES IN INFORMATION SECURITY 5 (2d ed. 2015).

[14] *Id.*

[15] *Id.* One might recall the use of a “Caesar cipher” to decode a secret radio program message from Ovaltine in the radio-age-set film, A CHRISTMAS STORY (Metro-Goldwyn-Mayer 1983).

[16] GRAMA, *supra* note 13, at 5.

[17] *Id.* at 35.

[18] Ernie Hayden, *Islands in the Data Stream*, INFO. SECURITY, May 2013, at 23, 24.

[19] *Id.*

[20] *Id.* The Revenue Canada and TRW hacks remain to be some of the largest data incidents, even when compared to those in today’s world. *See* JOHN R. VACCA, COMPUTER AND INFORMATION SECURITY HANDBOOK 741-42 (2d ed. 2013).

[21] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, tit. II, §§ 200-271, 110 Stat. 1936, 1991-2037 (codified as amended in scattered sections of 42 U.S.C.).

[22] *Summary of the HIPAA Security Rule*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations (last visited Mar. 29, 2018).

[23] § 201(a), 110 Stat. at 1992 (codified as amended at 42 U.S.C. § 1320a-7c(a)(3)(B)(ii) (2012)).

[24] Hayden, *supra* note 18, at 24.

[25] Act of Sept. 29, 2002, ch. 1054, 2002 Cal. Stat. 6790 (codified as amended at CAL. CIV. CODE §§ 1798.82, 1798.29 (West 2017)); Timothy H. Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet a Suitable Template for National Identity Theft Legislation*, 10 RICH. J.L.& TECH. 1 (2003). The California law is commonly known by its bill name, SB 1386. *See* S. 1386, 2001-2002 Leg., Reg. Sess. (Cal. 2002).

[26] Skinner, *supra* note 25, at 4.

[27] *Id.*

[28] *Id.* at 6.

[29] *Id.* at 5.

[30] *See infra* Section IV.B.

[31] *See, e.g.*, Thad A. Davis et al., *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2015 COLUM. BUS. L. REV. 613, 643-45 (2015); David C. Grossman, Comment, *Blaming the Victim: How FTC Data Security Enforcement Actions Make Companies and Consumers More Vulnerable to Hackers*, 23 GEO. MASON L. REV. 1283, 1288-89 (2016); Justin C. Pierce, Note, *Shifting Data Breach Liability: A Congressional Approach*, 57 WM. & MARY L. REV. 975, 980 (2016).

[32] Pierce, *supra* note 31, at 980.

[33] VERIZON, 2016 DATA BREACH INVESTIGATIONS REPORT 31 (2016).

[34] Elizabeth Falconer, *Ashley Madison Breach: Hacktivists or Criminals?*, N.C. J.L. & TECH. (Sept. 17, 2015), http://ncjolt.org/ashley-madison-breach-hacktivists-or-criminals.

[35] *Id.*

[36] PONEMON INST., 2016 COST OF DATA BREACH STUDY: UNITED STATES 4 (2016) [hereinafter PONEMON, UNITED STATES].

[37] *Id.* at 1, 4.

[38] *Id.* at 8 fig.5.

[39] *Id.* at 1. Malicious or criminal data breaches, in total, cost tens of millions of dollars more than those caused by system glitches or human error, respectively. *See id.* at 8 fig.6.

[40] *Id.* at 5 fig.1.

[41] *Id.* at 5 n.2 (defining per capita cost as "total cost of data breach divided by the size of the data breach in terms of the number of lost or stolen records").

[42] *Id.* at 5 fig.1.

[43] *Id.* at 5.

[44] *Id.* at 14 fig.15.

[45] *Id.* at 6 fig.2.

[46] *Id.*

[47] *Id.*

[48] *Compare* PONEMON INST., 2016 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 1 (2016) [hereinafter PONEMON, GLOBAL ANALYSIS], *with* PONEMON, UNITED STATES, *supra* note 36, at 1.

[49] PONEMON, GLOBAL ANALYSIS, *supra* note 48, at 5 fig.1. The Ponemon global report's twelve participants were the United States, the United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, the Arabian Region (United Arab Emirates and Saudi Arabia), Canada, and South Africa. *Id.* at 1.

[50] *Id.* at 11 ch.2.

[51] PONEMON, UNITED STATES, *supra* note 36, at 7 fig.4.

[52] PONEMON, GLOBAL ANALYSIS, *supra* note 48, at 10 fig.4.

[53] VERIZON, *supra* note 33, at 7 fig.2.

[54] Tom Brown & Emily Lowe, *Know Your Enemy: Inside the Hacker's Mind*, WILLIS TOWERS WATSON CYBER CLAIMS BRIEF, Winter 2016, at 3, 4, https://www.willis.com/documents/publications/Industries/Financial_Institutions/16527%20BROCHURE_Cyber%20Claims%C20Winter%202016.pdf.

[55] *Id.*

[56] VERIZON, *supra* note 33, at 7 fig.3.

[57] *Id.*

[58] *Id.* at 8.

[59] *Id.* at 10 fig.7.

[60] *Id.* at 11.

[61] *Id.* at 10 fig.7.

[62] *Id.* at 10 fig.8.

[63] *Id.*

[64] *Id.*

[65] Cynthia P. Arends, *Shifting Liability for a Data Breach Through Contractual Terms*, FOR THE DEF., Mar. 2015, at 61, 61-62, http://www.iadclaw.org/assets/1/7/_5-_Cohen.pdf.

[66] *See id.* at 61.

[67] Adeola Adele et al., *More Vendors, More Problems*, WILLIS TOWERS WATSON CYBER CLAIMS BRIEF, Winter 2016, at 6, 6, https://www.willis.com/documents/publications/Industries/Financial_Institutions/16527%20BROCHURE_Cyber%20Claims%C20Winter%202016.pdf. So too could any breach of contract remedy be limited. *Id.* These damages limitations are discussed further *infra* Section III.B.

[68] Adele et al., *supra* note 67, at 7 ("[T]hird-party claims ... are a relatively rare consequence of a data breach .... Data breaches with less than 100,000 affected individuals are less likely to interest a plaintiff's lawyer, who typically is only paid a percentage of the final recovery.").

[69] Silverpop Sys., Inc. v. Leading Mkt. Techs., Inc., 641 F. App'x 849 (11th Cir. 2016) (per curiam); *see also* Arends, *supra* note 65, at 63.

[70] *Silverpop*, 641 F. App'x at 850.

[71] *Id.*

[72] *Id.*

[73] *Id.* at 856.

74 *Id.* at 856-57.

75 *See* Arends, *supra* note 65, at 61.

76 Jesse M. Brush, *Mixed Contracts and the U.C.C.: A Proposal for a Uniform Penalty Default to Protect Consumers* 3 (Yale Law Sch. Legal Scholarship Repository, Student Scholarship Paper No. 47, 2007), http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1047&context=student_papers.

77 U.C.C. § 2-102 (AM. LAW INST. & UNIF. LAW COMM'N 2016) ("Unless the context otherwise requires, this Article applies to transactions in goods ....").

78 Abby J. Hardwick, *Amending the Uniform Commercial Code: How Will a Change in Scope Alter the Concept of Goods?*, 82 WASH. U. L.Q. 275, 278 (2004).

79 *Id.* at 281.

80 *Id.* at 279-81 (citing Bonebrake v. Cox, 499 F.2d 951, 960 (8th Cir. 1974)).

81 Raymond T. Nimmer, *Services Contracts: The Forgotten Sector of Commercial Law*, 26 LOY. L.A. L. REV. 725, 726, 728 (1993). *But see* Rottner v. AVG Techs. USA, Inc., 943 F. Supp. 2d 222, 230-32 (D. Mass. 2013) (holding software--under the specific facts of the case--a "good" for purposes of the UCC and applying the Delaware version of the Code in a breach of warranty action).

82 *See* Nimmer, *supra* note 81, at 727; *see also* Larry W. Smith, *A Survey of Current Legal Issues Arising from Contracts for Computer Goods and Services*, 1 COMPUTER L.J. 475, 476 (1979) ("[J]ust as the computer has brought about revolutionary changes in certain segments of society, courts find themselves facing equally new and complex legal issues ... such as ... the right to keep computer records private ....'). A proposed Uniform Computer Information Transactions Act ("UCITA") sought to create a clear and uniform set of rules to govern these computer-based transactions but adoption efforts failed in most states. *See* Brian D. McDonald, *The Uniform Computer Information Transactions Act*, 16 BERKELEY TECH. L.J. 461, 462-63 (2001).

83 U.C.C. §§ 2-715, -719 (AM. LAW INST. & UNIF. LAW COMM'N 2016).

84 RESTATEMENT (SECOND) OF CONTRACTS § 344(a) (AM. LAW INST. 1981).

85 *Id.* § 344(a), § 344 cmt. a.

86 *See id.* § 351, § 351 cmt. a.

87 Hadley v. Baxendale (1854) 156 Eng. Rep. 145, 151; 9 Ex. 341, 354.

88 *Id.* at 151-52; 9 Ex. at 354-56.

89 *Compare* Globe Refining Co. v. Landa Cotton Oil Co., 190 U.S. 540, 545 (1903) (Holmes, J.) ("It may be said with safety that mere notice to a seller of some interest or probable action of the buyer is not enough necessarily and as matter of law to charge the seller with special damage on that account if he fails to deliver the goods."), *with* Kerr S.S. Co. v. Radio Corp. of America, 157 N.E. 140, 141 (N.Y. 1927) (Cardozo, C.J.) ("Notice of the business, if it is to lay the basis for special damages, must be sufficiently informing to be notice of the risk.").

90 *See* Arends, *supra* note 65, at 63 (discussing these limitations in IT service contract settings).

91 *Supply Agreement*, LAW INSIDER, § 11.1 (Dec. 18, 2007), https://www.lawinsider.com/contracts/13tERji00dwEZo0xHw3Jei/axt-inc/supply-agreement/2007-12-18#limitation-of-liability/disclaimer-of-consequential-damages.

92 *Id.* § 11.2.

93 E. ALLAN FARNSWORTH, CONTRACTS § 4.28, at 308 (4th ed. 2004).

94 *See id.* (first citing Martin Rispens & Son v. Hall Farms, 621 N.E.2d 1078 (Ind. 1993); then citing U.C.C. §§ 2-718 to 2-719 (AM. LAW INST. & UNIF. LAW COMM'N 1952)).

95 Williams v. Walker-Thomas Furniture Co., 350 F.2d 445, 449 (D.C. Cir. 1965).

96 FARNSWORTH, *supra* note 93, at 301. Another example of procedural unconscionability is a "take-it-or-leave-it" contract, known as a contract of adhesion. *Id.* § 4.26, at 286.

97 *Id.* at 303.

98 *Id.* at 299, 302.

99 U.C.C. § 2-302 (AM. LAW INST. & UNIF. LAW COMM'N 2016). Karl Llewellyn, author of much of the UCC, including section 2-302, called this section "perhaps the most valuable section in the entire Code." FARNSWORTH, *supra* note 93, at 298. But Llewellyn made clear that this was about much more than unequal bargaining power, and instead concerned the "general commercial background and the commercial needs of the particular trade or case" when determining whether the terms were "so one-sided as to be unconscionable under the circumstances existing at the time of the making of the contract." U.C.C. § 2-302 cmt. 1 (AM. LAW INST. & UNIF. LAW COMM'N 2016). For background on Karl Llewelyn and the drafting of the UCC, see PERSPECTIVES ON THE UNIFORM COMMERCIAL CODE, at ix-48 (Douglas E. Litowitz, ed., 2d ed. 2007).

100 RESTATEMENT (SECOND) OF CONTRACTS § 208 (AM. LAW INST. 1981).

101 FARNSWORTH, *supra* note 93, at 302.

102 Cont'l Airlines v. Goodyear Tire & Rubber Co., 819 F.2d 1519, 1527 (9th Cir. 1987).

103 Matthew Spohn & David Navetta, *Recent Case Highlights the Dangers of Consequential Damage Waivers in IT Contracts*, NORTON ROSE FULBRIGHT DATA PROTECTION REP. (Sept. 26, 2016), http://www.dataprotectionreport.com/2016/09/recent-case-highlights-the-dangers-of-consequential-damage-waivers-in-it-contracts.

104 Arends, *supra* note 65, at 63 (alteration in original).

105 This disclaimer extinguishes liability even for *direct* harm. As for the personal injury waiver, interestingly, the UCC finds limitations on consequential personal injury due to consumer goods "prima facie unconscionable." FARNSWORTH, *supra* note 93, at 308. Whether that prima facie rule would apply to service contracts is questionable, because the rationale of preventing defective and physically dangerous products is perhaps not as persuasive in the services setting.

106 Arends, *supra* note 65, at 63.

107 *See* Spohn & Navetta, *supra* note 103.

108 Silverpop Sys., Inc. v. Leading Mkt. Techs., Inc., 641 F. App'x. 849, 854-55 (11th Cir. 2016) (per curiam).

109 *Id.* at 855.

110 *Id.* at 855-56 (quoting Schonfeld v. Hillard, 218 F.3d 164, 175-76 (2d. Cir. 2000)).

111 *Id.* at 856.

112 *Id.*

113 *See* Spohn & Navetta, *supra* note 103.

114 *See supra* note 102 and accompanying text.

115 PONEMON, UNITED STATES, *supra* note 36, at 5, 14.

116 While *Hadley* is famous for the rule of consequential damages, it should be remembered the plaintiff was *not* awarded consequential damages in the case. Hadley v. Baxendale (1854) 156 Eng. Rep. 145, 151-52; 9 Ex. 341, 356.

117 *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 3029783, *15-16. (N.D. Cal. May 27, 2016).

118 *Id.* Following that decision, it appears the case has settled. *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2017 WL 3730912 (N.D. Cal. Aug. 25, 2017).

119 RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL AND EMOTIONAL HARM § 3 (AM. LAW INST. 2010).

120 *See* David G. Owen, *The Five Elements of Negligence*, 35 HOFSTRA L. REV. 1671, 1674, 1682 (2007).

121 RESTATEMENT (THIRD) OF TORTS: LIAB. FOR ECON. HARM § 2 (AM. LAW INST., Tentative Draft No. 1, 2012).

122 *Id.* § 1.

123 *Id.* § 3.

124 RESTATEMENT (THIRD) OF TORTS: LIAB. FOR ECON. HARM § 7 (AM. LAW INST., Tentative Draft No. 2, 2014).

125 Jay M. Feinman, *The Economic Loss Rule and Private Ordering*, 48 ARIZ. L. REV. 813, 813 (2006).

126 *Id.* at 817. Absent from contract law is the type of reasonableness inquiry delegated to courts and juries that is found in tort law, signifying an ideological decision to allow individuals to bargain voluntarily. *See id.* at 818.

127 Vincent R. Johnson, *The Boundary-Line Function of the Economic Loss Rule*, 66 WASH. & LEE L. REV. 523, 526 (2009).

128 *See id.* at 527 n.13.

129 *See* David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 942-50 (2016) (first citing *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014); then citing Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421 (5th Cir. 2013); and then citing Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162 (3d Cir. 2008)).

130 *See supra* Section II.B.

131 *See, e.g.*, Dittman v. UPMC, 154 A.3d 318 (Pa. Super. Ct. 2017).

132 *Id.* at 325.

133 *Id.* at 324 (holding that the only duty the legislature has prescribed is notification of the data breach, and therefore a judicially-created duty of care "disrupts that deliberative process").

134 *Data Breach Negligence Claims Not Recognized in Pennsylvania*, BLANK ROME LLP (June 2015), https://www.blankrome.com/index.cfm?contentID=37&itemID=3607.

135 *See* Silverpop Sys., Inc. v. Leading Mkt. Techs., Inc., 641 F. App'x. 849, 852-53 (11th Cir. 2016).

136 "[T]ort principles, such as negligence, are better suited for resolving claims involving unanticipated physical injury, particularly those arising out of an accident. Contract principles, on the other hand, are generally more appropriate for determining claims for consequential damage that the parties have, or could have, addressed in their agreement." Opderbeck, *supra* note 129, at 948 n.89 (quoting Spring Motors Distribs., Inc. v. Ford Motor Co., 489 A.2d 660, 672 (N.J. 1985)).

137 *See, e.g.*, *Silverpop*, 641 F. App'x at 852-59 (dismissing both negligence and breach of contract claims against a vendor for harm arising out of a data breach).

138 RALPH E. BOYER ET AL., THE LAW OF PROPERTY: AN INTRODUCTORY SURVEY 14 (4th ed. 1991).

139 *Id.*

140 *Id.* at 16. Yet, there is movement away from a categorical framework toward a uniform standard of care. *Id.* ("The trend is for [an ordinary negligence] standard in all cases.").

141 *Id.*; Richard H. Helmholz, *Bailment Theories and the Liability of Bailees: The Elusive Uniform Standard of Reasonable Care*, 41 U. KAN. L. REV. 97, 99 (1992).

142 HUGH EVANDER WILLIS, PRINCIPLES OF THE LAW OF DAMAGES 132 (1910).

143 *See id.* at 132-33.

144 *See id.* at 132; *see also* Andrew Tettenborn, *Consequential Damages in Contract--The Poor Relation?*, 42 LOY. L.A. L. REV. 177, 183 (2008) ("Direct loss claims ... are treated rather differently .... The defaulting carrier or bailee is liable for the value of goods destroyed or the depreciation of goods damaged." (citing 25 SAMUEL WILLISTON & RICHARD A. LORD, WILLISTON ON CONTRACTS § 66:104 (4th ed. 2002))).

145 WILLIS, *supra* note 142, at 133.

146 *See id.* For the legal standard, see the discussion of *Hadley v. Baxendale*, beginning *supra* note 87.

147 BOYER ET AL., *supra* note 138, at 16.

148 Ward Farnsworth, *The Economic Loss Rule*, 50 VAL. U. L. REV. 545, 560 n.34 (2016).

149 Douglas H. Meal with David T. Cohen, Ropes & Gray LLP, *Private Data Security Breach Litigation in the United States*, *in* INSIDE THE MINDS: PRIVACY AND SURVEILLANCE LEGAL ISSUES: LEADING LAWYERS ON NAVIGATING CHANGES IN SECURITY PROGRAM REQUIREMENTS AND HELPING CLIENTS PREVENT BREACHES 101 (2014), https://www.ropesgray.com/~/media/Files/articles/2014/February/Meal%20Chapter.ashx/PDF.

150 *See id.* (first citing *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 974-75 (S.D. Cal. 2012), *aff'd*, 380 F. App'x 689 (9th Cir. 2010); then citing Richardson v. DSW, Inc., No. 05 C 4599, 2005 WL 2978755, at *4 (N.D. Ill. Nov. 3, 2005)).

151 *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014).

152 *Id.*; *see also DSW*, 2005 WL 2978755, at *4 (dismissing a bailment claim because the parties never agreed information would be returned).

153 *Target*, 66 F. Supp. 3d at 1177.

154 *Todd Ommen*, PACE U., http://law.pace.edu/faculty/todd-ommen (last visited Mar. 29, 2018).

155 Todd Ommen, *Bailment Claims: A Cause of Action in Data Breach Cases*, WEITZ & LUXENBERG: BLOG (Apr. 14, 2015), http://www.weitzlux.com/blog/2015/04/14/bailment-claims-cause-action-data-breach-cases ("No court to date has given sufficient thought or analysis to bailment claims in the context of data breaches. The claim is a natural fit for a situation where an individual provides valuable and private information to a third party for safekeeping, and the remedy, based on the value of the property lost or damaged, would provide a distinct injury and an ascertainable measure of damages.").

156 *Id.* This Note has discussed how both contract and tort claims arising out of a data breach likely fail against vendors. *See supra* Sections III.B-C.

157 *See* Ommen, *supra* note 155.

158 *See supra* text accompanying note 107. If the harm is characterized as "direct," then a limitation of consequential damages would be, fittingly, of no consequence.

159 FOLEY & LARDNER LLP, CLOUD COMPUTING: A PRACTICAL FRAMEWORK FOR MANAGING CLOUD COMPUTING RISK 2 (2013), https://www.foley.com/files/Publication/493fc6cc-aa03-4974-a874-022e36d12184/Presentation/PublicationAttachment/c9bd65f3-a6fd-4acb-96de-d1c0434f1eb7/CloudComputingPracticalFrameworkforManag.

160 *Id.*

161 Swarnpreet Singh & Tarun Jangwal, *Cost Breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues*, 4 INT'L J. COMPUTER SCI. & INFO. TECH. 17, 17, 21 (2012).

162 *See, e.g.*, DIMENSION DATA, PRIVATE CLOUD (2016), https://www.dimensiondata.com/Global/Downloadable%20Documents/Private%20Cloud%C20Technical%20Brief.pdf. For clarity, this Note uses "cloud computing" or "cloud services" when referring to subscripted services through a vendor over a public cloud, in contrast to private self-hosting.

163 The notification laws also inform the company itself how long it has to notify its customers (the affected individuals or "data subjects").

164 Adele et al., *supra* note 67, at 8.

165 *Id.*

166 FOLEY & LARDNER LLP, *supra* note 159, at 16.

167 UPTIME LEGAL SYS. LLC, CLOUD COMPUTING DUE DILIGENCE: A CHECKLIST FOR LAW FIRMS 4 (2015), http://www.tsrconsult.com/wp-content/uploads/2015/10/Cloudchecklist.pdf.

168 *See id.*

169 *Id.* at 5.

170 *Id.*

171 *Cloud Computing Due Diligence Checklist*, CLIO, https://landing.clio.com/rs/themissolutionsinc/images/Cloud%20Computing%C20Due%C20Diligence%20Checklist.pdf (last visited Mar. 29, 2018).

172 HOGAN LOVELLS, COMPLIANCE CHECKLIST FOR PROSPECTIVE CLOUD CUSTOMERS (2011), http://www.cisco.com/c/dam/en_us/about/doing_business/legal/privacy_compliance/docs/CloudComplianceChecklist.pdf.

173 UPTIME LEGAL SYS. LLC, *supra* note 167, at 5.

174 HOGAN LOVELLS, *supra* note 172.

175 FOLEY & LARDNER LLP, *supra* note 159, at 2.

176 *Id.* Low risk involves a low-critical mission with generally available data, citing Twitter and Facebook as examples. Medium risk involves critically higher missions, but still with generally available data, like web-conferencing or use of non-confidential sales data. Finally, high risk will involve "mission critical processes utilizing highly sensitive data." *Id.*

177 HOGAN LOVELLS, *supra* note 172.

178 *See* Spohn & Navetta, *supra* note 103.

179 *Id.*

180 HOGAN LOVELLS, *supra* note 172.

181 *See generally* STEPTOE & JOHNSON LLP, COMPARISON OF US STATE AND FEDERAL SECURITY BREACH NOTIFICATION LAWS (2016), http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf.

182 All states except Alabama, New Mexico, and South Dakota have data breach notification laws. *See id.*

183 STEPTOE & JOHNSON LLP, *supra* note 181.

184 *See supra* text accompanying notes 24-29. California's law has evolved significantly since 2002. For California's new, statutorily created "model security breach notification form," see CAL. CIV. CODE § 1798.29(d)(1)(D) (West 2017).

185 *See* STEPTOE & JOHNSON LLP, *supra* note 181. For example, Pennsylvania requires that "[a] vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data." 73 PA. STAT. AND CONS. STAT. ANN. § 2303(c) (West 2008).

186 PONEMON INSTITUTE, UNITED STATES, *supra* note 36, at 2.

187 N.Y. GEN. BUS. LAW § 899-aa(2) (McKinney 2012 & Supp. 2017).

188 EXPERIAN, DATA BREACH RESPONSE GUIDE 9 (2013), https://www.experian.com/assets/data-breach/brochures/response-guide.pdf.

189 *See, e.g.*, N.C. GEN. STAT. § 75-65(e)(1)-(3) (2016).

190 *Id.* § 75-65(d) ("The notice shall be clear and conspicuous.").

191 EXPERIAN, *supra* note 188, at 9.

192 *Id.*

193 N.J. STAT. ANN. § 56:8-163(b) (West 2012).

194 FLA. STAT. § 501.171(6)(a) (2016) ("In the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall notify the covered entity of the breach of security as expeditiously as practicable, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred.").

195 N.Y. GEN. BUS. LAW § 899-aa(1)(b) (McKinney 2012 & Supp. 2017).

196 N.J. STAT. ANN. § 56:8-163(c)(2) (West 2012).

197 DAVID MOLNAR & STUART SCHECHTER, MICROSOFT RESEARCH, SELF HOSTING VS. CLOUD HOSTING: ACCOUNTING FOR THE SECURITY IMPACT OF HOSTING IN THE CLOUD 2 (2010), https://pdfs.semanticscholar.org/db9f/b8fbc92b74d3d84e02240bf98064170ef23a.pdf.

198 *Id.* at 15.

199 *Id.* at 11.

200 *See supra* Part II.

201 *See supra* Part III.

202 Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges*, 33 QUINNIPIAC L. REV. 369, 397 (2015).

203 *Id.* at 396. One case involved a property insurance company denying a cyber-based claim grounded in insuring "forgery," through strict construction of the definition. In litigation, the court agreed with the insurance company, finding the policy's "forgery" coverage limited to traditional negotiable instruments such as checks and promissory notes, and not electronic transfers. Metro Brokers, Inc. v. Transp. Ins. Co., No. 1:12-CV-3010-0DE, 2013 WL 7117840, at *4-5 (N.D. Ga. Nov. 21, 2013).

204 691 F.3d 821, 824-825, 832 (6th Cir. 2012).

205 Podolak, *supra* note 202, at 398.

206 *Id.* at 399.

207 *Id.*

208 *Id.*

209 *Id.*

210 FOLEY & LARDNER LLP, *supra* note 159, at 11.

211 The Travelers Indemnity Company, CyberRisk Policy CYB-3001 Ed. 07-10, at 1 (2010) [hereinafter Travelers Policy]. For the sample policy, see **Jordan** M. **Rand**, *Resources*, CYBERINSURANCE L. BLOG, http://www.databreachninja.com/wp-content/uploads/sites/63/2016/03/Travelers-Form-Cyber-Policy.pdf (last visited Mar. 29,

2018).

212 Travelers Policy, *supra* note 211, at 1.

213 *Id.* at 2.

214 *Id.* at 1. "Crisis management event expenses" are defined as "reasonable fees, costs, and expenses incurred and paid by the [i]nsured ... for public relations services ... to mitigate any actual or potential negative publicity resulting from any [w]rongful [a]ct." *Id.* at 5.

215 *See supra* note 43 and accompanying text.

216 Travelers Policy, *supra* note 211, at 1.

217 *Id.* at 8.

218 *Id.* at 3-4.

219 *Id.* at 9.

220 L. D. Simmons II, *A Buyer's Guide to Cyber Insurance*, MCGUIRE WOODS (Oct. 2, 2013), https://www.mcguirewoods.com/Client-Resources/Alerts/2013/10/Buyers-Guide-to-Cyber-Insurance.aspx.

221 *Id.*

222 *Id.*

223 *Id.*

224 *Id.*

225 NETDILIGENCE, 2015 CYBER CLAIMS STUDY 1 (2015), https://netdiligence.com/wp-content/uploads/2016/05/NetDiligence_2015_Cyber_Claims_Study_093015.pdf.

226 *Id.* at 1-3.

227 *Id.* at 3.

228 *Id.*

229 *Id.*

230 *Id.* at 6.

231 *Id.* at 30.

232 *How Firms Rate on Cyber Readiness and Why Some Don't Buy Cyber Insurance: Hiscox Report*, INS. JOURNAL (Feb. 7, 2017), http://www.insurancejournal.com/news/national/2017/02/07/441155.htm.

233 HISCOX, THE HISCOX CYBER READINESS REPORT 2017, at 20 (2017), https://www.hiscox.co.uk/cyber-readiness-report/docs/cyber-readiness-report-2017.pdf.

234 *Id.* This is especially true in the United States, where, based on a November- December 2016 survey, fifty-five percent of firms already have cyber insurance. Lagging behind, and bringing the average down, are the United Kingdom with thirty-six percent and Germany with only thirty percent of firms reporting they currently have cyber insurance. *Id.* at 20-21. The discrepancy is supposedly based on a broader range of concern for United States firms. *Id.* at 20.

235 *Id.* at 21. Another reason is directly related to the notification laws discussed *supra* in Part IV. This additionally supports why the United States has significantly more firms with cyber insurance; the development of the insurance market coincided with the enactment of states' mandatory notification laws. *See id.* at 20 ("[H]igh-profile data breaches and increasing *regulatory pressures* have combined to increase risk awareness in corporate boardrooms." (emphasis added)).

236 *Id.* at 20. Companies of 250 employees or more uptake cyber insurance at a rate of forty-eight percent compared to all others at a rate of thirty-seven percent. *Id.*

237 An organization is considered to be of the "very smallest" if it is made up of less than one hundred employees. *Id.* at 5.

238 *Id.*

239 *Id.* at 8. Expenses include new technology, staffing, staff training, and security consultants. *Id.* at 9.

240 *See id.* at 23. Still, the price of the policy premium would be an important consideration.

241 *Id.* In fact, there may be false positives for the amount of firms responding affirmatively to the study's cyber insurance inquiry. *Id.* Some companies may think they are covered under a traditional policy, which, as this Note has shown, is likely not the case. *See supra* Section V.A.

242 Brad Smith, President, Microsoft Corp., Keynote Address at the RSA Conference 2017: The Need for a Digital Geneva Convention (Feb. 14, 2017) (transcript available at https://mscorpmedia.azureedge.net/mscorpmedia/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf).

70 RUULR 717

End of Document