Boston College Law Review

Volume 62 | Issue 5 Article 5

5-25-2021

The Economic Loss Doctrine & Data Breach Litigation: Applying the "Venerable Chestnut of Tort Law" in the Age of the Internet

Nicolas N. LaBranche
Boston College Law School, nicolas.labranche@bc.edu

THE ECONOMIC LOSS DOCTRINE & DATA BREACH LITIGATION: APPLYING THE "VENERABLE CHESTNUT OF TORT LAW"[1] IN THE AGE OF THE INTERNET

Abstract: Data controllers and processors are increasingly finding themselves the targets of hackers who steal the personal identifiable information (PII) stored in their systems and sell it on the dark web. Data subjects, whose PII is exposed in a data breach, routinely have been turning to data breach litigation as a means of compensation for the damages that they suffer. Routinely, plaintiffs have pleaded negligence causes of action against data controllers or processors. A plaintiff's ability to overcome procedural hurdles, not the merits of their case, often dictates the success or failure of these tort claims. One prominent hurdle is the economic loss doctrine (ELD), a rule that restricts tort recovery for purely economic damages. The ELD is a ubiquitous doctrine with a variety of applications and paradigms in tort law. Data breach litigation, however, does not implicate the doctrine's policy goals of promoting private ordering and preventing unlimited and unforeseeable liability. Instead, this Note argues that the ELD in data breach litigation should be more pliable and include a special relationship test that the plaintiffs are presumed to satisfy.

INTRODUCTION

Over ninety percent of all data ever created has been produced in the past two years—the result of 2.5 quintillion bytes of data generated daily.[2] This data boom is a result of many factors such as the growth of internet-connected devices, the rise of social media, and the growing demand by data controllers and processors[3] to accumulate personal identifiable information[4] (PII).[5] Both

[1] Nathan A. Sales, *Regulating Cyber-security*, 107 NW. U. L. REV. 1503, 1535 (2013).

[2] *See* Bernard Marr, *How Much Data Do We Create Every Day? The Mind-blowing Stats Everyone Should Read*, FORBES (May 21, 2018), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#75b56c8460ba [https://perma.cc/RV9F-J8XN] (describing the growth of the use of data, and then listing some of the reasons for the massive growth of data).

[3] *See* Commission Regulation 2016/679, 2016 O.J. (L 119) 33 (EU) (defining data controller and processor for the General Data Protection Regulation); Chris Brooks, *Data Controller vs. Data Processor*, DIGIT. GUARDIAN (Aug. 11, 2020), https://digitalguardian.com/blog/data-controller-vs-data-processor-whats-difference [https://perma.cc/GU4T-AGKB] (defining the terms data controller and data processor in relation to its use in the European General Data Protection Regulation (GDPR)). Both data controllers and processors are terms that came into prominence due to the GDPR. *See* Brooks, *supra* (referencing that companies that seek to become GDPR compliant must understand these two terms). The GDPR provides guidance for the use of these terms. *Id.* A data controller is a legal person, public or private entity that "determines the purposes and means of the processing of

public and private entities have committed vast resources to effectively collect and process PII to increase efficiency, make better decisions, and provide better services.[6] Whole sectors of the modern economy—particularly social media websites—depend on the aggregation, processing, and selling of PII to maintain a viable business model.[7]

The PII collected and processed by internet platforms, the government, and private businesses ranges from relatively benign information, such as a name or email address, to highly sensitive data, such as an individual's social

---

personal data." Commission Regulation 2016/679, *supra*, at 33. A data controller controls the extent of the use of personal data. *See* Brooks, *supra*. Data controllers may give data to third parties to process for a variety of reasons. *Id.* A data processor is person, public or private entity that "processes personal data on behalf of the controller." Commission Regulation 2016/679, *supra*, at 33. The data processor does not own the data, and its use of the data is limited to the scope allowed by the data controller. *See* Brooks, *supra*.

[4] Memorandum from Clay Johnson III, Deputy Dir. for Mgmt., Off. of Mgmt. & Budget on Safeguarding Against and Responding to the Breach of Personally Identifiable Information to the Heads of Executive Departments and Agencies 1 n.1 (May 22, 2007), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-16.pdf [https://perma.cc/3LXC-JAZJ]. PII is a broad term and extends to any information that when combined with other information can be linked to a specific individual. *See id.* (stating that PII includes information such as an individual's mother's maiden name which when combined with other facts could be traced to that specific individual). Typical forms of PII include names, biometric data, or social security numbers. *Id.*

[5] *See* Irfan Ahmad, *How Much Data Is Generated Every Minute?*, SOC. MEDIA TODAY (June 15, 2018), https://www.socialmediatoday.com/news/how-much-data-is-generated-every-minute-infographic-1/525692/ [https://perma.cc/BGC9-SX96] (displaying where new data is coming from, and describing how much data is produced by prominent social media, internet, and data-based companies); Erik Brynjolfsson & Andrew McAfee, *The Data Boom Is the Innovation Story of Our Lifetime,* THE ATLANTIC (Nov. 21, 2011), https://www.theatlantic.com/business/archive/2011/11/the-big-data-boom-is-the-innovation-story-of-our-time/248215/ [https://perma.cc/5GEH-T5CN] (exploring how people use data in today's economy and how private entities are increasingly finding novel ways to use information, resulting in a data boom); Tim Keary, *A Look at Data Trends for 2019*, INFO. AGE (Mar. 26, 2019), https://www.information-age.com/data-analytics-trends-2019-123481163/ [https://perma.cc/BR87-7298] (providing indicators that show that industries are increasingly turning to data analytics to fuel decision-making and investing significant resources in data analytics); *Rise of the Data Analyst—What's Behind the Boom*, PURDUE UNIV. GLOB., https://www.purdueglobal.edu/blog/information-technology/rise-of-data-analyst/ [https://perma.cc/9X8H-EF5E] (Jan. 15, 2021) (linking the growth in data analytic jobs to the growth of data being generated).

[6] *See* Kimberly A. Houser & Debra Sanders, *The Use of Big Data Analytics by the IRS: Efficient Solution or the End of Privacy as We Know It?*, 19 VAND. J. ENT. & TECH. L. 817, 818–20 (2017) (describing how the Internal Revenue Service (IRS) is increasingly using data to enforce the tax code and possible worries that arise from government data collection); Brynjolfsson & McAfee, *supra* note 5 (exploring the ways in which private entities are using data to make more informed decisions); Keary, *supra* note 5 (tracking the investment of private companies in data analytics).

[7] *See* Kurt Wagner, *This Is How Facebook Uses Your Data for Ad Targeting*, VOX (Apr. 11, 2018), https://www.vox.com/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg [https://perma.cc/A5ZN-PXG9] (explaining that Facebook—and social media companies generally—heavily rely on the aggregation of users' PII, and noting that these social media platforms collect individual PII and sell that data to advertisers who through algorithms target individual users who they believe would be likely to buy or use a product).

security or credit card number.[8] Data controllers and processors can use PII in a variety of ways, such as designing targeted advertising or creating individualized credit reports.[9] These factors combine to make PII extremely valuable to the source individual, the data controller or processor who stores the data, and to any malicious actors who gain access to it.[10] Despite this, many Americans are unaware of the true extent PII collection by internet platforms, the government, and private businesses.[11]

---

[8] *See* Memorandum from Clay Johnson III, Deputy Dir. for Mgmt., Off. of Mgmt. & Budget on Safeguarding Against and Responding to the Breach of Personally Identifiable Information to the Heads of Executive Departments and Agencies, *supra* note 4, at 1 n.1 (defining PII, and providing common examples); *What Is a Credit Report and What Does It Include?*, EQUIFAX, https://www.equifax.com/personal/education/credit/report/what-is-a-credit-report-and-what-does-it-include/ [https://perma.cc/Y9NC-Y5VS] (stating what is included in the average American's credit report). One common purpose of the aggregation of PII is to create an individual credit report. *What Is a Credit Report?*, CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/ask-cfpb/what-is-a-credit-report-en-309/ [https://perma.cc/J92H-EGNR] (June 8, 2017). A credit report "is a statement that has information about your credit activity and current credit situation such as loan paying history and the status of your credit accounts." *Id.* A credit report can contain an individual's address, name, birthdate, social security number, phone number, and the intimate details of their financial life. *Id.* The breadth of data collected can result in significant harm to individuals if someone or something exposes their data. *See* Ron Lieber, *Why the Equifax Breach Stings So Bad*, N.Y. TIMES (Sept. 22, 2017), https://www.nytimes.com/2017/09/22/your-money/equifax-breach.html [https://perma.cc/42FP-7LLT] (detailing the consequences of the Equifax data breach for Americans, including the effects of decades of PII being exposed and that many individuals no longer trust the institutions that make up the credit reporting system).

[9] *See* Brynjolfsson & McAfee, *supra* note 5 (showing ways in which private entities have used the power of data, and providing examples of a variety of industries using data analytics to fuel growth and efficiency); Lieber, *supra* note 8 (describing the process in which PII is aggregated by credit card reporting processes then plugged through algorithms or black boxes that then create a unique individual credit score, which banks and landlords use as metric to judge the credit worthiness of that individual).

[10] *See* James Short & Steve Todd, *What's Your Data Worth?*, 58 MITSLOAN MGMT. REV. 17, 17–19 (2017) (exploring the valuation of personal data by businesses, and providing examples of how businesses have valued data); Ellen Neveux, *Healthcare Data: The New Prize for Hackers*, SECURE LINK, https://www.securelink.com/blog/healthcare-data-new-prize-hackers [https://perma.cc/P53Z-FEJB] (Nov. 19, 2020) (quantifying the price that hackers can get for certain types of data on the black market); *The World's Most Valuable Resource Is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [https://perma.cc/QF4H-UB34] (describing the importance and value of data to businesses in the economy).

[11] *See* Houser & Sanders, *supra* note 6, at 819–20 (explaining the ways in which the IRS mines social media, phones records, and other public sources to process that data to increase the efficiency of tax enforcement); Ian Bogost, *Welcome to the Age of Privacy Nihilism*, THE ATLANTIC (Aug. 23, 2018), https://www.theatlantic.com/technology/archive/2018/08/the-age-of-privacy-nihilism-is-here/568198/ [https://perma.cc/5CTM-M84H] (declaring that indifference to and ignorance of the extent of data collection has ended personal privacy); Natasha Singer, *What You Don't Know About How Facebook Uses Your Data*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html [https://perma.cc/7JX4-LYDJ] (describing the process in which social media companies can track the off-site internet patterns of individuals).

Malicious actors or hackers routinely breach public and private entities that store data to harvest and sell PII on the black market.[12] When PII is exposed through a breach, victims have struggled to obtain adequate compensation through government regulatory actions—even though the data controller or processor took inadequate precautions to secure their data.[13] In response, victims of data breaches are frequently turning to the courts to pursue litigation against the data controller or processor that has mishandled their PII.[14]

Currently, there is no one court-tested theory for litigants, leaving plaintiffs to creatively plead numerous causes of action, drawing from statutes, torts, and contract law.[15] In ninety percent of class actions, however, plaintiffs

---

[12] *See* IDENTITY THEFT RES. CTR., 2019 END-OF-YEAR DATA BREACH REPORT 2 (2020), https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf [https://perma.cc/TW39-V9WA] (providing a general overview of data breaches in 2019); Kira Caban, *2020 Breach Barometer: 41M Patient Records Breached as Hacking Incidents Escalate*, PROTENUS (Feb. 18, 2020), https://blog.protenus.com/2020-breach-barometer-41m-patient-records-breached-as-hacking-incidents-escalate [https://perma.cc/E7E2-RQXP] (detailing that hacking in the healthcare industry increased in 2019). In 2019, data breaches across all industries, including within the government, increased by 17% from 2018. IDENTITY THEFT RES. CTR., *supra*, at 2. Although the total number of records breached decreased, this is likely due to the Marriott data breach skewing the numbers for 2018. *Id.* at 14. The business sector recorded the highest number of breaches in both 2018 and 2019. *Id.* In 2018, industries reported 578 data breaches, which increased to 644 data breaches in 2019, exposing 18,328,975 records. *Id.* at 13–15. The healthcare sector was the second most breached industry. *Id.* In the healthcare industry, the number of breached records tripled between 2018 and 2019, to 41,404,022 records. Caban, *supra*. In 2019, the healthcare industry suffered 525 breaches, an increase from the 369 breaches in 2018. IDENTITY THEFT RES. CTR., *supra*, at 2. It is estimated that on the black market, medical records can be sold for around $50 per record. Caban, *supra*.

[13] *See* Recent Case, *Cyberlaw—Data Breach Litigation—D.C. Circuit Holds That Heightened Risk of Future Injury Can Constitute an Injury in Fact for Article III Standing.—In re* U.S. Office of Personnel Management Data Security Breach Litigation*, 928 F.3d 42 (D.C. Cir. 2019)*, 133 HARV. L. REV. 1095, 1095–96 (2020) (describing the struggles of government employees to get compensation for a data breach); Emily Birnbaum & Maggie Miller, *Equifax Breach Settlement Sparks Criticism*, THE HILL (July 22, 2019), https://thehill.com/policy/cybersecurity/454207-equifax-breach-settlement-sparks-criticism [https://perma.cc/9Q7V-MTBJ] (explaining that critics viewed the Equifax settlement as inadequate); Lily Hay Newman, *$700 Million Equifax Fine Is Still Too Little, Too Late*, WIRED (July 22, 2019), https://www.wired.com/story/equifax-fine-not-enough/ [https://perma.cc/M9FK-Q83D] (arguing that the Equifax data breach settlement was too minor and ineffective to remedy the harm suffered).

[14] *See* Megan Dowty, Note, *Life Is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 686 (2017) (arguing that data breach victims will constitute the "next wave" of class action law suits (quoting CARLTON FIELDS & JORDAN BURT, THE 2015 CARLTON FIELDS JORDAN BURT CLASS ACTION SURVEY: BEST PRACTICES IN REDUCING COST AND MANAGING RISK IN CLASS ACTION LITIGATION 9 (2015), https://classactionsurvey.com/pdf/2015-class-action-survey.pdf [https://perma.cc/3YGS-5BNR])); Newman, *supra* note 13 (arguing that the government settlement with Equifax was not enough).

[15] *See* JENA VALDETERO ET AL., BRYAN CAVE LEIGHTON PAISNER, DATA BREACH LITIGATION REPORT 15 (2019), https://www.bclplaw.com/images/content/1/6/v6/163774/2019-Litigation-Report.pdf [https://perma.cc/RD7P-LZTB] (describing the creativity of plaintiffs in data breach litigation). Typically, plaintiffs will allege as many causes of action as possible in a complaint due to the uncertainty of which will survive even the early stages of litigation. *Id.*

claim common law negligence.[16] The success of private lawsuits has routinely hinged on the plaintiff's ability to overcome procedural and common law doctrines that courts developed to address a different economic age and are still adopting to the unique facts raised by data breach litigation.[17]

One of the prominent obstacles that plaintiffs must overcome when alleging negligence—or other tort-based claims—is the economic loss doctrine (ELD).[18] The ELD restricts the ability of plaintiffs to bring tort claims when the defendants' alleged tortious conduct inflicts purely economic damages[19] and no harm to person or property.[20] Courts struggle with applying the ELD, and whether to apply the ELD at all, to data breach litigation.[21] Part I of this Note explores the ELD's doctrinal development, the two prevailing paradigms that govern the ELD's application, and provides a general overview of data breach litigation.[22] Part II discusses the intersection of the ELD and data breach litigation through an analysis of how different states have applied their

---

[16] *Id.* at 2 ("Negligence, the most popular legal theory in 2016, remained the primary theory (first legal count) in approximately 50% of all class action complaints and was alleged in over 90% of all class action complaints during both 2017 and 2018." (emphasis omitted)).

[17] *See* Dowty, *supra* note 14, at 686 (describing the Article III standing problem that plaintiffs have faced in data breach litigation); John A. Fisher, Note, *Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach*, 4 WM. & MARY BUS. L. REV. 215, 229–39 (2013) (arguing that negligence per se should apply to data breaches, and detailing a plaintiff's struggle with data breaches); Max Meglio, Note, *Embracing Insecurity: Harm Reduction Through a No-Fault Approach to Consumer Data Breach Litigation*, 61 B.C. L. REV. 1223, 1236–41 (2020) (examining the issues that plaintiffs have faced in consumer data breach litigation).

[18] *See* Catherine M. Sharkey, *Can Data Breach Claims Survive the Economic Loss Rule?*, 66 DEPAUL L. REV. 339, 341 (2017) (noting that the economic loss doctrine (ELD) is a formidable obstacle to litigation); Meglio, *supra* note 17, at 1237–38 (explaining that the ELD is a hurdle for plaintiffs in data breach litigation).

[19] Eileen Silverstein, *On Recovery in Tort for Pure Economic Loss*, 32 U. MICH. J.L. REFORM 403, 403–08 (1999). Economic harms are damages that manifest on a balance sheet. *See id.* at 406. Professor Eileen Silverstein proposes an example of the negligent maintenance of a transformer box that causes a telephone pole to collapse on a factory roof, damaging the roof, hurting some employees, and resulting in the factory closing. *See id.* at 404. The factory owner and injured employees will be able to collect personal and property-based damages. *See id.* The other workers, not hurt by the falling pole, will not be able to collect lost wage damages due to the shutdown of the factory. *See id.* Under a traditional ELD analysis, these purely economic damages of the uninjured workers would be barred. *See id.* (describing how the ELD bars damages for purely economic loss).

[20] Dan B. Dobbs, *An Introduction to Non-statutory Economic Loss Claims*, 48 ARIZ. L. REV. 713, 713 (2006) ("The stand-alone or 'pure' economic loss covered by the economic loss rule refers to pecuniary or commercial loss that does not arise from actionable physical, emotional or reputational injury to persons or physical injury to property."); Jeffery L. Goodman et al., *A Guide to Understanding the Economic Loss Doctrine*, 67 DRAKE L. REV. 1, 1–2 (2019) ("The economic loss doctrine prevents a party who suffers only economic damages from recovering those damages in tort." (emphasis omitted)).

[21] *See infra* notes 150–251 and accompanying text (describing applications of the ELD in data breach litigation).

[22] *See infra* notes 25–149 and accompanying text.

ELD in data breach litigation.[23] Part III argues that the ELD should not be applied to data breach litigation, as the economic realities of the internet age do not implicate the underlying ELD policy goals of promoting private ordering and avoiding unforeseeable plaintiffs.[24]

I. The Economic Loss Doctrine, Data Breaches & Credit Cards

The ELD, like most of the common law, was developed in the "[t]he [l]aw [o]f [t]he [h]orse," before the digital economy of today.[25] Originally, the ELD served two important policy goals: the promotion of private ordering[26] and the prevention of liability to unforeseeable plaintiffs.[27] Despite originating as a broad bar on purely economic damages, the ELD is now composed of two paradigms, the stranger paradigm and contracting parties paradigm, each with unique exceptions.[28] These exceptions reflect the reality that the common law system embraces flexibility to the unique facts of a case.[29] The doctrine's broad application, numerous and often confusing exceptions, and competing paradigms often serve as an insurmountable roadblock for plaintiffs pursuing tort claims in data breach litigation.[30] This Note argues that the venerable policy goals of private ordering and foreseeability are less practicable in an economy where the telegram has been replaced by the internet.[31]

---

[23] *See infra* notes 150–251 and accompanying text.

[24] *See infra* notes 252–330 and accompanying text.

[25] *See* Lawrence Lessig, Commentary, *The Law of the Horse: What Cyberlaw Might Teach*, 113 Harv. L. Rev. 501, 501, 506 (1999) (arguing that courts should adapt common law doctrines to align with the policy goals of the internet age). Professor Lawrence Lessig argues that there is an inherent difference between the real world and digital world. *Id.* at 511. The common law doctrines developed to fix these real-world problems do not translate to the intangible online world. *Id.*

[26] *See* Jorge L. Contreras, *From Private Ordering to Public Law: The Legal Framework Governing Standards-Essential Patents*, 30 Harv. J.L. & Tech. Rev. 212, 213 (2017) (noting that the phrase "private ordering" generally refers to the ways in which private individuals or entities, free from state influence, allocate resources, delineate rights and duties, and resolve disputes through contract or other legal means).

[27] *See infra* notes 106–108 and accompanying text; *see also* Danielle Sawaya, Note, *Not Just for Products Liability: Applying the Economic Loss Rule Beyond Its Origin*, 83 Fordham L. Rev. 1073, 1076–78 (2014) (describing the origins of the ELD in product liability cases).

[28] *See* Sharkey, *supra* note 18, at 344, 348–77 (explaining the two different paradigms that the ELD operates in and the exceptions that apply to each).

[29] *See* David Corker, *How the Flexibility of English Common Law Can Encourage Good Judgement*, Corker Binning Blog (Nov. 14, 2016), https://www.corkerbinning.com/how-the-flexibility-of-english-common-law-can-encourage-good-judgment/ [https://perma.cc/9Y2G-9PFQ] (noting broadly the flexibility of the common law system, depending on the facts of a given case).

[30] *See* Sharkey, *supra* note 18, at 348–66 (illustrating cases in which courts applied the ELD to the plaintiff's claims); Meglio, *supra* note 17, at 1237–38 (characterizing the ELD as a bar against the negligence claims).

[31] *See* Lessig, *supra* note 25, at 502–03 (arguing that the common law should adapt to the digital space because it is inherently ill-suited to applications beyond the real world).

Part I of this Note provides a history of the ELD, explores the intricacies of the competing paradigms that operate within the ELD, and introduces the ELD as applied to data breaches and data breach litigation.[32] Section A overviews the ELD's doctrinal origins under economic principles that are now ill-suited to the digital age.[33] Section B explores the two paradigms that operate within the ELD and how they can be outcome-determinative in data breach litigation.[34] Section C discusses the policy considerations of private ordering and foreseeability that serve as the impetus for the doctrine's development.[35] Section D illustrates what a data breach is and why data breach litigation raises policy goals that butt heads with the policy goals of the ELD.[36] Section E details the credit card payment system, a commonly litigated data breach situation, and the unique issues raised by the web of contracts surrounding credit cards.[37]

A. The Development of the Economic Loss Doctrine into Two Paradigms

The ELD premiered in American jurisprudence in 1879, in *Savings Bank v. Ward*, in which the U.S. Supreme Court barred the tort claims of the plaintiff, a land buyer, against the defendant, a lawyer hired by the previous landowner, who had wrongly certified that the property his client owned was unencumbered.[38] The court concluded that the parties lacked any pre-existing legal relationship to create liability for purely economic damages.[39] The modern ELD originated in 1965, in *Seely v. White Motor Co.*, where the Supreme Court of California applied the ELD as a limiting doctrine in a product liability case to ensure that a defective product would not subject the defendant, a manufacturer, to a chain of unlimited economic liability.[40] Because the ELD ap-

---

[32] *See infra* notes 25–149 and accompanying text.

[33] *See infra* notes 37–48 and accompanying text.

[34] *See infra* notes 49–99 and accompanying text.

[35] *See infra* notes 100–118 and accompanying text.

[36] *See infra* notes 119–138 and accompanying text.

[37] *See infra* notes 139–149 and accompanying text.

[38] *See* 100 U.S. 195, 195–98 (1879) (holding the lack of privity between the parties bared for tort liability). In 1879, in *Savings Bank v. Ward*, the defendant, a lawyer, had been paid by the previous landowner of a piece of property to certify that it was unencumbered. *Id.* at 195. The previous landowner, however, had transferred the land. *Id.* The defendant and plaintiff, the person buying the land, never had any communication between one another. *Id.* The previous landowner used the defendant's certification to obtain a loan from the plaintiff, placing the land as collateral. *Id.* After the loan had not been paid, the plaintiff sought to claim the land but could not. *Id.*

[39] *See id.* at 207 ("Suffice it to say these parties never met, and there was no communication of any kind between the defendant and the brokers, or the lenders of the money.").

[40] *See* 403 P.2d 145, 151 (Cal. 1965); Vincent R. Johnson, *The Boundary-Line Function of the Economic Loss Rule*, 66 WASH. & LEE. L. REV. 523, 557 n.66 (2009) (explaining that one branch of the ELD developed from product liability doctrines); Sawaya, *supra* note 27, at 1076 & n.5 (describing the ELD as a doctrine originating in product liability). In 1965, in *Seely v. White Motor Co.*, the Supreme Court of California first adopted the ELD as a bar against purely economic claims against the defendant, a manufacturer of a defective product. *See* 403 P.2d at 151 (barring the plaintiffs' tort

plied to bar additional tort claims in *Seely*, it restricted the plaintiffs, owners of a car that the defendant manufactured, to an express warranty claim.[41] Although the legal relationship between the parties remains relevant today, the ELD has evolved into a more ubiquitous doctrine, operating more like a blanket term for the prohibition of economic damages in torts.[42]

Under this blanket, there are two unique ways the ELD operates in the law: the "stranger paradigm" and the "contracting parties paradigm."[43] The first version of the ELD—the stranger paradigm—governs when two parties have no pre-existing legal relationship defining the duties owed between them.[44] The second version—the contracting parties paradigm—governs when the parties have a contract governing the rights and duties owed between them.[45] In certain instances, however, the nature of the relationship between the two parties does not fit squarely within either of these paradigms.[46] In such circumstances, a court must decide whether the level of privity between the

---

claims). The plaintiffs in *Seely* purchased a truck with defective brakes. *Id.* The truck crashed, and the plaintiffs sued the defendant for business losses resulting from their inability to use the truck. *Id.* at 150. The court held that the newfound restriction in economic damages barred the plaintiffs' negligence claims. *Id.* at 151. The court noted, however, that the plaintiffs could proceed under a theory of express warranty. *Id.*

[41] *See* 403 P.2d at 151 (holding that the plaintiff may pursue a cause of action under express warranty).

[42] *See* Herbert Bernstein, *Civil Liability for Pure Economic Loss Under American Tort Law*, 46 AM. J. COMPAR. L. 111, 125–126 (1998) (stating that the law surrounding the ELD is not uniform and not well settled); Sharkey, *supra* note 18, at 344 (describing the ELD, not as a singular rule, but as a general doctrine that applies somewhat differently in the two different paradigms).

[43] *See* Sharkey, *supra* note 18, at 344 (defining the two paradigms of the ELD); Catherine M. Sharkey, *In Search of the Cheapest Cost Avoider: Another View of the Economic Loss Rule*, 85 U. CIN. L. REV. 1017, 1019–34 (2018). *See generally* Dobbs, *supra* note 20, at 715–28 (describing the competing policy goals and rules when the parties are strangers or when the parties have a contractual relationship). Professor Catherine M. Sharkey was the originator of the terms "stranger paradigm" and "contracting parties paradigm." *See* Sharkey, *supra* note 18, at 344. Since the initial incarnation of these terms, Professor Sharkey has broadened the categories and expanded the contracting parties paradigm to the consensual paradigm. Sharkey, *supra*, at 1029–34. Under this approach, the consensual paradigm includes both instances in which a party is in direct privity and the product liability ELD. *See id.* (explaining the consensual parties paradigm). For the purposes of this Note, the contracting parties paradigm is the more appropriate nomenclature, as product liability does not apply to data breach litigation. *See In re* Marriott Int'l, Inc., Costumer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 475–76 (D. Md. 2020) (stating that data breach litigation is different from product liability litigation because the product that the consumer receives in return for their data is not defective).

[44] *See* Sharkey, *supra* note 18, at 348 ("The 'stranger economic loss rule' posits that, as between parties with no contractual or special relationship, there is no duty to avoid negligent infliction of purely financial losses." (quoting Dobbs, *supra* note 20, 715)); Sharkey, *supra* note 43, at 1019–34 (describing the two paradigms and their operation in the law).

[45] Sharkey, *supra* note 18, at 344–45 (stating that the contracting parties paradigm is implicated when the parties have previously allocated the risks and responsibilities of each party, typically through contract).

[46] *See id.* at 366 (describing data breach litigation as a common example in which the facts of the case fit squarely within neither of the two paradigms). *See generally* Dobbs, *supra* note 20, at 715–28 (explaining issues that arise between subcontractors and contractors on construction projects).

parties implicates either the contracting parties paradigm or the stranger paradigm.[47] How the court resolves this third-party problem may determine if the ELD applies, thus potentially barring the tort claims of the plaintiff.[48]

B. The Paradigms: One Rule, or Two Rules, or Three Rules

The varying applications of the ELD—and their focus on the legal relationship between the plaintiff and defendant—is necessary to analyze their application in data breach litigation, as the paradigm the court places the plaintiff and defendant in will implicate one of two generally accepted exceptions to the rule.[49] Subsection 1 of this Section explores the stranger paradigm—when no pre-existing legal or contractual relationship exists—which illustrates the ELD's policy goal of protecting defendants from unforeseeable plaintiffs.[50] Subsection 2 discusses the contracting parties paradigm—when a pre-existing legal relationship exists—which highlights the ELD's encouragement of private ordering between parties.[51] Subsection 3 explains the third-party problem, how courts have traditionally approached it, and why it persists as a tricky analytical issue in each case.[52]

1. The Stranger Paradigm: When Two Strangers Walk into a Courtroom

The stranger paradigm applies when there is no pre-existing contractual or legal relationship between parties.[53] Under the stranger paradigm, when one stranger sues another for economic damages, the ELD typically bars the plain-

---

[47] *See* Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 813–16 (7th Cir. 2018) (deciding in a data breach litigation case whether the facts of the payment credit card system more accurately reflected a stranger paradigm or a contracting parties paradigm); Sharkey, *supra* note 18, at 366 (explaining that in the third-party problem, the facts of the case fit neatly within either paradigm).

[48] *See* Jay M. Fienman, *The Economic Loss Rule and Private Ordering*, 48 ARIZ. L. REV. 813, 815 (2006) (stating that the third-party problem involves a network of contracts); Sharkey, *supra* note 18, at 366 (noting that, depending on the availability of ELD exceptions, a jurisdiction's choice of paradigm may be outcome-determinative); Sharkey, *supra* note 43, at 1034 (explaining how and why choice of paradigm is key). *Compare Cmty. Bank of Trenton*, 887 F.3d at 813–16 (adopting explicitly the contracting parties paradigm in a third-party problem, and then applying the ELD to bar the negligence claims of the defendant), *with In re* Arby's Rest. Grp. Inc. Litig., C.A. No. 17-cv-0514, 2018 WL 2128441, at *12 (N.D. Ga. Mar. 5, 2018) (adopting implicitly the stranger paradigm in a third-party problem, and then not applying the ELD to bar the negligence claims of the plaintiff).

[49] *See infra* notes 53–251 and accompanying text (describing the ELD and how the ELD operates in data breach litigation).

[50] *See infra* notes 53–70 and accompanying text.

[51] *See infra* notes 71–87 and accompanying text.

[52] *See infra* notes 88–99 and accompanying text.

[53] *See* Sharkey, *supra* note 18, at 348 (describing the stranger paradigm as one where there is no pre-existing contractual or special relationship between the parties that could subject the defendant to tort liability for economic damages).

tiff's tort claims.[54] Some jurisdictions, however, have adopted exceptions to the ELD when operating in the stranger paradigm that reflect the existence of a common law independent duty between the two parties.[55]

a. Flat Bar: When the Stranger Paradigm Bars Purely Economic Claims

The traditional—and more rigid—approach to the ELD in the stranger paradigm creates an absolute bar to tort claims for purely economic damages when the plaintiff and defendant have no pre-existing legal relationship.[56] The 2001 case *532 Madison Avenue Gourmet Foods, Inc. v. Finlandia Center, Inc.* exemplifies this approach; the New York Court of Appeals applied the ELD between two parties with no pre-existing legal relationship.[57] In *532 Madison Avenue Gourmet Foods, Inc.*, one of the defendants, a construction company, had negligently caused the partial collapse of the side of a thirty-nine-story building.[58] To repair the fallout of the collapse, fifteen city streets and side streets were temporarily closed.[59] In response, the key plaintiff, a local deli, that suffered no property or personal damages, but rather only lost profits under the street closure, attempted to sue the defendant for economic damages originating from their alleged negligence.[60] The court—in dismissing the plaintiff's case—concluded that the plaintiff's economic loss existed outside the scope of any duty owed by the defendant.[61] In support of its decision, the court stated that extending such a duty would expose the defendant to extensive, possibly unlimited, liability.[62] Ultimately, because the defendant had no

[54] *See* Dobbs, *supra* note 20, at 715 ("[A] defendant owes no duty to exercise reasonable care for the pure stand-alone economic interests of strangers—that is to persons with whom the defendant has no relationship by contract, undertaking, or specific legal obligation."); Sharkey, *supra* note 18, at 348 (discussing the ELD implementation when strangers sue one another).

[55] *See* Tommy L. Griffin Plumbing & Heating Co. v. Jordan, Jones & Goulding, Inc., 463 S.E.2d 85, 88–89 (S.C. 1995) (holding that regardless of the two parties not having a pre-existing legal relationship, an independent duty exception to the stranger paradigm allowed the claims to proceed). *See generally* Sharkey, *supra* note 18, at 354–60 (describing all the exceptions courts have applied to the ELD when operating in the stranger paradigm).

[56] *See* Sharkey, *supra* note 18, at 354–60 (explaining the stranger paradigm and the exceptions commonly applied to the ELD within that paradigm).

[57] *See* 750 N.E.2d 1097, 1101 (N.Y. 2001) (stating that the plaintiffs could not bring purely economic damages against the defendants for their negligent actions).

[58] *Id.* at 1099. In 2001, in *532 Madison Avenue Gourmet Foods, Inc. v. Finlandia Center, Inc.*, the New York Court of Appeals explained that the collapse occurred at a construction site located in the commercial district of New York City. *Id.* Brick, mortar, and other construction materials fell into the streets below and put ninety-four holes in the building's south wall. *Id.* The fallout of the collapse shut down the surrounding area for approximately two weeks. *Id.*

[59] *Id.*

[60] *Id.* The chief plaintiff in this case represented a local deli that had to be shut down for five weeks as a direct result of the collapse. *Id.*

[61] *See id.* at 1103 (holding that there was no legal duty that could allow for economic damages).

[62] *Id.* The court listed all the parties that could potentially sue the defendants, which included the construction company, the building owner, and others, if it allowed economic damages in this in-

pre-existing legal relationship or duty owed to the plaintiff, the ELD applied, barring any tort claims for economic damages.[63] This inflexible manifestation of the stranger paradigm is the dominant application of the ELD when the parties have no pre-existing legal relationship.[64]

b. The Independent Duty Exception: When the Stranger Paradigm Allows Purely Economic Damages

Some jurisdictions, however, have adopted an "independent duty exception" to the ELD when operating within the stranger paradigm.[65] Under this exception, when the plaintiff can demonstrate that the defendant owed them a non-contractual independent duty of care, existing in the common law, then the ELD will not per se bar the plaintiff's tort claims.[66] In 1995, in *Tommy L. Griffin Plumbing & Heating Co. v. Jordan, Jones & Goulding, Inc.*, the Supreme Court of South Carolina held that the ELD did not bar the plaintiff's negligence claims asserting purely economic damages, as an independent duty of the defendant.[67] The court, operating within the stranger paradigm, held that the ELD does not apply when a "duty arising independently of any contract duties" exists.[68] The defendant—an engineer who had designed and supervised

---

stance. *Id.* The court noted that every actor who relied on the street for anything of economic value would be then permitted to sue the defendants. *See id.* (detailing the potential extent of parties that could claim economic damages).

[63] *See id.* (holding broadly that the lack of legal relationship made the ELD applicable, thus barring the claims).

[64] *See generally* Sharkey, *supra* note 18, at 354–60 (noting how courts often apply the ELD as a broad prohibition to recovery for economic damages).

[65] *See In re* Equifax, Inc., Customer Data Sec. Breach Litig., 371 F. Supp. 3d 1150, 1172 (N.D. Ga. 2019) (holding that there did exist an independent duty exception to the ELD); Dittman v. UPMC, 196 A.3d 1036, 1056 (Pa. 2018) (same); Tommy L. Griffin Plumbing & Heating Co. v. Jordan, Jones & Goulding, Inc., 463 S.E.2d 85, 88–89 (S.C. 1995) (relying on an independent duty exception to the ELD, thus not barring the claims); Sharkey, *supra* note 18, at 354–55 (describing the independent duty exception to the ELD).

[66] *See In re Equifax, Inc.*, 371 F. Supp. 3d at 1172 (describing the exception as allowing for economic damages when the plaintiff can show a pre-existing duty); *Dittman*,196 A.3d at 1056 (stating that the ELD did not apply when an independent duty of care applied); *Tommy L. Griffin Plumbing & Heating Co.*, 463 S.E.2d at 88–89 (stating that because the defendant owed the plaintiff an independent duty, the plaintiff could pursue economic damages); Sharkey, *supra* note 18, at 354–55 (explaining that the independent duty exceptions allows for economic damages).

[67] *See* 463 S.E.2d at 86–88 ("A breach of a duty arising independently of any contract duties between the parties, however, may support a tort action.").

[68] *See id.* at 88 (stating that there was no privity of contract between the parties, which resulted in an implicit adoption of the stranger paradigm). The 1995 case *Tommy L. Griffin Plumbing & Heating Co. v. Jordan, Jones & Goulding, Inc.* represents a third-party problem in which the Supreme Court of South Carolina implicated a stranger paradigm by stating that no direct privity existed. *See* Sharkey, *supra* note 18, at 345 n.17 (explaining the general third-party problem). *Compare Tommy L. Griffin Plumbing & Heating Co.*, 463 S.E.2d at 86–88 (explaining that the parties were in a construction project and both had contracts with the same general contractor), *with* BRW, Inc. v. Dufficy & Sons, Inc., 99 P.3d 66, 74 (Colo. 2004) (stating that because the parties were in an entanglement of con-

a construction project—owed an ongoing independent duty to the plaintiff, a contractor, to competently design and manage the project.[69] Because the plaintiff and defendant's relationship implicated its own independent duty of care, manifested from the common law, the ELD did not apply, and the plaintiff could proceed with the merits of its tort claims.[70]

2. The Contracting Parties Paradigm: When Courts Allow and Do Not Allow for Economic Damages Between Contracting Parties

The other main ELD paradigm—the contracting parties paradigm—is implicated when two parties have a pre-existing contract that governs the rights and duties owed between them and relates to the claims asserted against the defendant.[71] This paradigm is commonly implicated when the parties are both businesses or involved in a business transaction that requires a contract.[72] Courts in this paradigm attempt to ensure that the boundary between tort and contract law is maintained by restricting recovery to the contract terms agreed to by the parties, or under contract law more generally.[73] The principle policy

---

tracts, the case involved a third-party problem in which the parties' relationship should be governed by the contracts). Generally, construction projects and the network of contracts that spring from them present model third-party problems. Sharkey, *supra* note 18, at 345 n.17. Courts apply the ELD in such instances holding that contracts govern the relationships of the parties, thus implicating the contracting parties paradigm. *Dufficy & Sons, Inc.*, 99 P.3d at 74 (holding that the relationship should be governed by the terms of the contracts); Sharkey, *supra* note 18, at 345 (explaining how courts generally apply the ELD in construction projects). *Tommy L. Griffin Plumbing & Heating Co.* represents how a court can apply the ELD to near identical facts in a different jurisdiction and come out with inconsistent results as compared to the majority approach. *See* 463 S.E.2d at 86–88 (holding that no contractual privity or relationship existed between the parties); Sharkey, *supra* note 18, at 345 (noting the majority approach to the third-party problem in construction projects).

[69] *See Tommy L. Griffin Plumbing & Heating Co.*, 463 S.E.2d at 89 ("Under these facts, Engineer owed a duty to the contractor not to negligently design or negligently supervise the project.").

[70] *See id.* (holding that the ELD did not apply because the plaintiff had shown that an independent duty existed).

[71] *See* Dobbs, *supra* note 20, at 723 (detailing when the contracting parties rule applies under the ELD); Sharkey, *supra* note 18, at 361–66 (explaining that the contracting parties paradigm is implicated when there exists some contractual relationship).

[72] *See* Sharkey, *supra* note 18, at 361–66 (explaining that a contractual relationship implicates the contracting parties paradigm); *see also, e.g.*, Silverpop Sys., Inc. v. Leading Mkt. Techs., Inc., 641 F. App'x 849, 852 (11th Cir. 2016) (per curiam) (applying the contracting parties paradigm when both parties were businesses).

[73] *See, e.g.*, *Silverpop Sys., Inc.*, 641 F. App'x at 854 (holding that the ELD applied, as the two parties had a contract governing their relationship); *In re* Sony Gaming Networks & Consumer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 819–20 (S.D. Cal. 2014) (concluding that the ELD applied, and noting that a contract between the two parties existed); Springfield Hydroelectric Co. v. Copp, 779 A.2d 67, 69 (Vt. 2001) (holding that the existence of a contract precluded tort liability for strictly economic damages); Sharkey, *supra* note 18, at 361–66 (explaining that when operating within the contracting parties paradigm, courts generally apply the ELD to bar claims). *Contra* Portier v. NEO Tech. Sols., No. 17-cv-30111, 2019 WL 7946103, at *17–22 (D. Mass. Dec. 31, 2019) (noting that despite the existence of a contract, the California ELD did not bar the tort claims of the plaintiffs).

rationales in this paradigm are to respect contracts and to encourage private ordering more broadly.[74]

a. The Contracting Parties Paradigm: When the Economic Loss Doctrine Bars Claims

The typical application of the ELD within the contracting parties paradigm bars all tort claims, and restricts recovery to the contract and contract law.[75] For example, in 2001, in *Springfield Hydroelectric Co. v. Copp*, the Vermont Supreme Court concluded that the ELD applied, and it thus barred tort claims, citing the existence of a contract with the defendants.[76] This contract governed the legal duties that the defendants owed to the plaintiffs regarding the management of a trust pool.[77] The enumeration of these duties in contract caused the court to implicitly adopt a contracting parties paradigm.[78] The court—expressing caution—held that the defendants' negligence amounted only to a breach of contract, and thus applied the ELD because the plaintiffs

---

[74] *See* Fienman, *supra* note 48, at 969 (explaining the ELD's policy goal of promoting private ordering by contract).

[75] *See* Sharkey, *supra* note 18, at 361–66 (noting how courts will commonly apply the ELD in the contracting parties paradigm because the contract governs the rights and duties owed between the two parties).

[76] *See* 779 A.2d at 71 (holding that the ELD applied and that the plaintiffs could obtain remedies under contract law). In 2001, in *Springfield Hydroelectric Co. v. Copp*, the Vermont Supreme Court considered the special relationship exception to the ELD in the contracting parties paradigm. *Id.* The court, however, did not offer much analysis on the issue. *See id.* (briefly discussing the special relationship, and concluding it did not apply without further rationale). The court noted that when a contract defines duties, courts rarely allow for damages existing outside of contract law, or even beyond the contract itself. *See id.* (noting broadly that contracting principles better govern the relationship).

[77] *Id* at 69. The plaintiffs in *Springfield Hydroelectric Co.* were owners of small hydroelectric power facilities. *Id.* The defendants were former employees of Vermont Power Exchange, a purchasing agent for Vermont's Public Service Board. *Id.* The plaintiffs collectively had entered into a "power purchase agreement" with the defendants to facilitate the sale of energy. *Id.* The general agreement established a trust fund that would serve as a safety net for producers who had to shut down before satisfying the terms of their agreement. *Id.* Upon successful completion of a thirty-year sale agreement, the hydroelectric producer would receive repayment of the money that they contributed to the trust pool. *Id.* The defendants were in charge of managing the trust fund; however, Vermont's Public Service Board was solely allowed to distribute the trust fund to struggling producers. *Id.* In 1988, the defendants approved a new hydroelectric facility to go online. *Id.* One year later, in 1989, that producer defaulted and received payment from the trust pool of $161,144. *Id.* The plaintiffs alleged that the defendants had negligently allowed the producer to go online, causing them economic damages in the form of reduced value of the trust fund. *Id.*

[78] *See id.* at 70 (stating that contracting principles more accurately governed the relationship between the parties in the case); *see also* Sharkey, *supra* note 18, at 361–66 (stating that when a contract governs the allocation of risks, rights, and damages between the parties, it implicates the contracting parties paradigm).

only suffered economic damages.[79] Thus, the plaintiffs could only obtain damages specified within the contract.[80]

b. A Special Duty: When the Contracting Parties Paradigm Does Not Bar Claims

Certain jurisdictions, however, obfuscate the distinction between tort and contract law by allowing a "special duty" or "special relationship" exception to the ELD.[81] Jurisdictions adopting this approach allow tort claims for economic damages when the plaintiff can prove that there exists a special relationship between the parties.[82] The special relationship exception operates as a higher standard of proof for plaintiffs than the independent duty exception.[83]

In 1979, in *J'Aire Corp. v. Gregory*, the Supreme Court of California detailed a framework for determining whether a special relationship existed.[84] The court outlined six factors: (1) the extent to which the defendant intended to affect the plaintiff with their actions, (2) the foreseeability of the harm, (3) the degree of certainty of the plaintiff's injury, (4) the closeness of the nexus be-

---

[79] *See Springfield Hydroelectric Co.*, 779 A.2d at 71 ("We have been careful to maintain a dividing line between contract and tort theories of recovery.").

[80] *See id.* at 71–72 (stating that courts should maintain the barrier between tort and contract, and concluding that the ELD applied).

[81] *See* Portier v. NEO Tech. Sols., No. 17-cv-30111, 2019 WL 7946103, at *16–22 (D. Mass. Dec. 31, 2019) (stating that despite the existence of a contract between the parties, the ELD did not bar tort claims for purely economic damages by the defendants because a special relationship exception applied); Sharkey, *supra* note 18, at 365–66 (explaining the special relationship exception to the contracting parties paradigm). Some courts have adopted the independent duty exception when adopting exceptions to the ELD in the contracting parties paradigm. Dittman v. UPMC, 196 A.3d 1036, 1054 (Pa. 2018) ("[I]f the duty arises independently of any contractual duties between the parties, then a breach of that duty may support a tort action.").

[82] *See Portier*, 2019 WL 7946103, at *17–22 (applying the special relationship test, and finding that the ELD did not bar the tort claims of the plaintiffs against the defendants in data breach litigation). *But see In re* Sony Gaming Networks & Consumer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 966–74 (S.D. Cal. 2014) (holding that because a special relationship was not satisfied, the plaintiffs were restricted to a remedy under contract law).

[83] *See* Sharkey, *supra* note 18, at 366 (stating the special relationship test is a higher threshold); *see also* Enslin v. Coca-Cola Co., 136 F. Supp. 3d 654, 672 (E.D. Pa. 2015) (holding that the special relationship exception should only be implicated when a great imbalance of power exists), *aff'd*, 739 739 F. App'x 91 (3d Cir. 2018).

[84] *See* 598 P.2d 60, 63 (Cal. 1979) (detailing a six-factor test to determine whether a special relationship exists between the parties, which would not bar a tort claim by the plaintiff). In 1979, in *J'Aire Corp. v. Gregory*, the Supreme Court of California explained that the plaintiff operated a restaurant at the county airport. *Id.* at 62. The defendant was a contractor hired by the county and tasked with repairing the heating and cooling system of the airport. *Id.* The defendant failed to complete the work in the reasonable time as defined in the contract. *Id.* The plaintiff could not operate their restaurant during the construction of the heating and cooling system, suffering economic losses. *Id.* The plaintiff then sued for negligent performance of a contract—despite having no contractual privity. *Id.* Although this was not a traditional economic loss case in the contracting paradigm, it highlights what exactly a special relationship is. *Id.*

tween the defendant's actions and the plaintiff's injury, (5) the moral blame of the defendant's conduct, and (6) an overall objective of preventing future harm.[85] A court should consider these factors holistically in determining whether a special relationship exists.[86] When the collective weight of the six factors leads to an affirmative finding of a special relationship, the ELD will not apply, allowing tort claims to proceed.[87]

3. The Third-Party Problem: The Grey Area Between the Two Paradigms

When case facts fail to match either the contracting parties paradigm or the stranger paradigm, the third-party problem arises.[88] Typically, the "third-party problem" occurs when the two parties lack a direct contractual relationship, but are bound by an entanglement of contracts with a common third-party.[89] The parties have some privity due to mutual contractual relationships with a mutual party; however, there is no direct agreement governing the relationship between the plaintiff and defendant.[90] A court must decide either that the multiple contracts create contractual privity between the parties—implicating the contracting parties paradigm—or that the entanglement of contracts does not amount to direct privity—implicating the stranger paradigm.[91] The court's characterization of the privity level of the parties can be essentially outcome-determinative as to whether tort claims may proceed, as the exception in the contracting parties paradigm creates a higher burden of proof for plaintiffs.[92]

---

[85] *Id.* at 63.

[86] *See id.* (examining the six factors that courts review holistically to determine whether a special relationship existed between the two parties).

[87] *See id.* (finding that because the plaintiff was able to show that the six factors have been met the ELD does not bar the claims due to the existence of a contract); *Portier*, 2019 WL 7946103, at *17–22 (holding that the six factors had been satisfied by the plaintiffs, so ELD did not bar their negligent claim for economic damages).

[88] *See* Dobbs, *supra* note 20, at 726 (illustrating issues with the ELD between a subcontractor, contractor, and designer); Fienman, *supra* note 48, at 815 (describing the third-party problem); Sharkey, *supra* note 18, at 366 (explaining that third-party problems do not fit squarely within either of the two paradigms).

[89] *See* Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 813–15 (7th Cir. 2018) (holding that if the facts of a case fit squarely within neither of the two paradigms, a court must determine which to apply); Sharkey, *supra* note 18, at 366 (stating courts must decide which paradigm to operate in).

[90] *See Cmty. Bank of Trenton*, 887 F.3d at 821 (arguing that the parties were loosely bound in a "web of contracts" with one another); Sharkey, *supra* note 18, at 362 (explaining that courts may find the parties in situations where de facto privity exists).

[91] *See Cmty. Bank of Trenton*, 887 F.3d at 821 (stating that the facts of the case created a contracting parties paradigm); Sharkey, *supra* note 18, at 366 (describing that courts must pick which paradigm to adopt in a third-party problem).

[92] *See Cmty. Bank of Trenton*, 887 F.3d at 821 (adopting the contracting parties paradigm, which precludes tort liability); Silverpop Sys., Inc. v. Leading Mkt. Techs., Inc., 641 F. App'x 849, 850–51 (11th Cir. 2016) (per curiam) (stating that because the parties had a contract governing the duties owed between the two parties, the independent duty exception should not apply); Sharkey, *supra* note

The third-party problem frequently arises regarding negligence claims between a subcontractor, a general contractor, and the contracting party.[93] For instance, in 2004, in *BRW, Inc. v. Dufficy & Sons, Inc.*, the Colorado Supreme Court held that the ELD barred claims by the plaintiff, a steel subcontractor, against the defendants, the original designers and inspectors of a construction project.[94] The plaintiff and defendants had no direct privity, only indirect privity through mutual contracts with an intermediary general contractor.[95] The plaintiff alleged that the defendants had negligently caused them economic damages.[96] The court reasoned that the plaintiff—by entering into a network of contracts—was bound by the rights and duties enumerated in the original general contractor's contract.[97] The court noted that the contract governed the duty to reasonably design the project and established the applicable standard of care; therefore, the court concluded that the plaintiff's remedies must be rooted in the contract.[98] Accordingly, the court dismissed the plaintiff's negligence claims, and restricted the plaintiff's recovery to claims originating under contract law.[99]

C. Policy: How the Economic Loss Doctrine Promotes Private Ordering and Ensures That the Plaintiff Is Foreseeable

The contracting parties and stranger paradigms' reliance on the relationship between the parties reflects the unique policy goals that rationalize their

---

18, at 366 (arguing an adoption of a paradigm could skew the probability of success for the plaintiff, especially if the courts allow for an exception in the stranger paradigm).

[93] *See Cmty. Bank of Trenton*, 887 F.3d at 815 (explaining that the relationship between the plaintiffs and defendant was analogous to the relationship between a contractor and subcontractor); BRW, Inc. v. Dufficy & Sons, Inc., 99 P.3d 66, 74 (Colo. 2004) (holding that by entering into a "network of interrelated of contracts," the plaintiff, a subcontractor, could not sue under a cause of action outside of the contract); Dobbs, *supra* note 20, at 723 (stating that the third-party problem arises surrounding the series of contracts commonly found in construction projects).

[94] 99 P.3d at 68–71. In in 2004, in *BRW, Inc. v. Dufficy & Sons, Inc.*, the Colorado Supreme Court, explained that the City of Denver had contracted with one of the defendants, the engineering firm BRW, Inc., to design two steel bridges. *Id.* at 68. The defendant submitted the design of the two bridges to Denver, which then solicited construction bids. *Id.* Edward Kramer & Sons won the bid, and then hired Anko Metal Services to conduct a variety of services related to the steel needed for the bridge. *Id.* Anko Metals Services then hired the plaintiff. *Id.* The defendant then hired co-defendant Professional Service Industries, Inc. to supervise the construction project. *Id.* at 70. The contract that the plaintiff agreed to contained specific provisions that required the plaintiff to follow the plans of the defendant. *Id.* at 69.

[95] *Id.* at 68. The only relevant party the plaintiff had direct privity with was Anko Metals Services, who was still two steps removed from BRW, Inc. *Id.* (describing the contractual web).

[96] *Id.* The plaintiff alleged that BRW, Inc.'s plans had failed to account for the local climate, resulting in undue delays. *Id.* at 70.

[97] *See id.* at 73 (finding that the original contract stated the allegedly breached duty, and noting it thus governed any ensuing claims).

[98] *See id.*

[99] *See id.* at 74 (dismissing the negligence claims of the plaintiff due to the ELD).

existence.[100] The contracting parties paradigm is concerned with the contractual relationship between the plaintiff and defendant, with the goal of promoting private ordering.[101] Likewise, the focus on the non-existence of any legal relationship in the stranger paradigm stems from the policy rationale to prevent unforeseeable and the potentially unlimited liability that purely economic damages can cause.[102]

First, private ordering—the policy goal underpinning the contracting parties paradigm—is deeply rooted in contract law and reflects a fundamental desire to let individuals freely establish duties and damages between themselves through contract instead of tort.[103] Proponents of private ordering assert that economic actors are better allocators of their own risks and benefits than the courts through enforcement of tort liability; thus, the ELD should strictly bar tort damages when the parties have allocated risk through contract.[104] In this sense, the ELD has a "bargain-forcing function[]" that promotes private contracting by restricting the potential for tort recovery.[105] Further, when two parties have privity, the ELD serves as a "boundary-line" between tort and contract law, preventing contract law from "drown[ing] in a sea of tort."[106] This theory operates soundly in product liability litigation, where a contractual remedy is typically readily available, either through a warranty or the Uniform

[100] *See* Sharkey, *supra* note 43, at 1019–34 (explaining the general policy justifications for the ELD under the two paradigms). *See generally* Dobbs, *supra* note 20, at 715–28 (explaining the broad justifications for the ELD); Fienman, *supra* note 48, at 814 (discussing the ELD in the context of private ordering).

[101] *See generally* Dobbs, *supra* note 20, at 715–28 (listing overarching policy rationales for the ELD); Fienman, *supra* note 48, at 814 (providing background on the ELD and private ordering).

[102] *See* Sharkey, *supra* note 43, at 1019–1034 (describing some general policy rationales for the ELD).

[103] Johnson, *supra* note 40, at 546–47 (stating that private ordering was an impetus in the adoption of the ELD); Sharkey, *supra* note 43, at 1033.

[104] *See* Dobbs, *supra* note 20, at 714 (offering that where a contract exists, its terms shall be respected); Fienman, *supra* note 48, at 814 (noting the policy rationale behind private ordering); Johnson, *supra* note 40, at 546–47 (explaining private ordering); Sharkey, *supra* note 43, at 1034 (restating that in the contract parties paradigm, a default no-tort-liability rule applies). If the contract terms, risks, and provisions are all valid, then the court should not seek to impose anything further than what the parties agreed to and should "[s]imply honor the contract itself." Dobbs, *supra* note 20, at 714.

[105] *See* Johnson, *supra* note 40, at 547–48 ("[T]he economic loss rule performs critical bargain-forcing functions."). By eliminating the possibility of tort recovery, the ELD allows parties to readably allocate damages for non-compliance. *Id.* The certainty of contractually enumerated damages promotes the efficient allocation of resources, and it provides assuredness for businesses' economic calculations. *Id.* Allowing tort damages would only increase transaction costs by fostering uncertainty in potential liability and reducing the strength of bargained-for contractual terms. *Id.*

[106] *See* E. River S.S. Corp. v. Transamerica Delaval, Inc., 476 U.S. 858, 866 (1986) (stating that the ELD sets a border between two types of law). The ELD protects the line by ensuring that, when both contract and tort theories apply, there is no overlap. *See* Sawaya, *supra* note 27, at 1087–90 (explaining the "boundary-line" function of the rule).

Commercial Code.[107] In less traditional fields, such as data breach litigation, doubts have been raised over the efficacy of private ordering.[108] This is primarily due to data-related contracts' reliance on contracts of adhesion, with inherent bargaining power imbalances between individual consumers and multinational corporations.[109]

Secondly, the ELD embodies a concern—underlying the stranger paradigm—that purely economic damages expose parties to unforeseeable and unlimited liability.[110] Under the stranger paradigm, where the parties have no preexisting legal relationship, the ELD attempts to limit damages that exist outside the bounds of foreseeability.[111] Although it may be foreseeable to a negligent driver that they may damage the delivery truck next to them, it is not as foreseeable that the craftsman—relying on the truck's delivery of wood—may suffer economic damages to their business following an accident.[112] In 1985, as the Pennsylvania Superior Court in *Aikens v. Baltimore & Ohio Railroad*

---

[107] Johnson, *supra* note 40, at 551. In today's highly commercialized society, in most transactions, there will be a contractual remedy available. *Id.* For instance, if an individual buys paint that does not stick to the wall, then that individual will have claims under contract through the paint's warranty. *Id.* The Uniform Commercial Code (UCC) supports this. *Id.* The UCC provides a breadth of options for consumers to seek claims resulting from a defective product. *Id.*

[108] *See* Emily Frye, *The Tragedy of the Cybercommons*, 58 BUS. LAW. 349, 367 (2002); Sales, *supra* note 1, at 1535 (describing the issues with private ordering in the internet economy). Typically, the warranties that provide a remedy for most consumers are not available in the cybersecurity industry. Frye, *supra*, at 367; Sales, *supra* note 1, at 1534. Software companies generally operating under a licensing system does not provide the same recourse for injured parties with defective products in traditional cases. Frye, *supra*, at 367; Sales, *supra* note 1, at 1534.

[109] *See* Frye, *supra* note 108, at 367 (explaining the issues that private parties encounter when contracting in the digital economy); Sales, *supra* note 1, at 1535 (illustrating private ordering can be ineffective due to the high transaction costs).

[110] *See* Dobbs, *supra* note 20, at 715 (stating some of the rationales underlying the paradigm); Sharkey, *supra* note 43, at 1022–29 (justifying the stranger paradigm). There is further justification for the stranger paradigm under a more theoretical approach. Sharkey, *supra* note 43, at 1022–24. The theoretical approach posits that society puts greater value on property and persons than on economic damages. *See id.*

[111] *See* 532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc., 750 N.E.2d 1097, 1103 (N.Y. 2001) (fearing that implementation of liability would unleash a chain of liability to all parties who have suffered even minor harm); Dobbs, *supra* note 20, at 715 (describing the policy goals of the stranger paradigm). Theoretically, economic loss can be an endless chain. Dobbs, *supra* note 20, at 715. For instance, individual A acts negligently resulting in economic damage to individual B. *Id.* As a result, individual B does not make their credit card payment to the bank. *Id.* The bank, as a result, has to increase the interest rate on their credit card to be able to cover for the losses of individual B's non-payment. *Id.* This then could result in another bank customer cutting back on the amount of cheeseburgers they buy from a local burger joint—that would then also suffer economic harm. *Id.* This hypothetical illustrates the potential chain that could be unleashed. *Id.* The ELD serves a vital function to curtail and place a limit on the liability that an individual can face from their negligent behavior. *Id.*

[112] *See* Dobbs, *supra* note 20, at 713 (illustrating an example of the stranger rule). This hypothetical's facts were adopted from the 2000 case *Aikens v. Debow*. *See generally* 541 S.E.2d 576 (W. Va. 2000).

Co. noted, "To allow a cause of action for negligent cause of purely economic loss would be to open the door to every person in the economic chain of the negligent person or business to bring a cause of action."[113]

Courts developed the ELD to foster predictability and efficiency in economic relationships.[114] They founded the doctrine upon two core assumptions.[115] First, that parties to a contract can reasonably negotiate for the rights and duties delineated in that contract.[116] Second, that it is not foreseeable who may suffer economic damages from a defendant's negligent conduct.[117] As economic transactions have changed in the digital age, serious doubts have been raised as to the validity of these assumptions, specifically in the context of data breach litigation.[118]

D. The State of Cybersecurity and Data Breach Litigation

A data breach, and any subsequent litigation, undercuts the ELD's core assumptions by removing the issue of foreseeability and challenging the feasibility of private ordering.[119] A data breach occurs when data stored on a data controller or processor's server is accessed without approval or exposed to a third party.[120] Data breaches have increased at a staggering rate; the amount of PII exposed doubled between 2018 and 2019, and the number of data breaches increased by seventeen percent in that single year.[121] These breaches expose data at an astounding scale; in the last six years, five separate data breaches each exposed over five hundred million people's PII.[122]

---

[113] Sharkey, *supra* note 18, at 348 (quoting Aikens v. Balt. & Ohio R.R. Co., 501 A.2d 277, 279 (Pa. Super. Ct. 1985)).

[114] *See* Goodman, *supra* note 20, at 4–5 (describing the history of the ELD in product liability cases).

[115] *See* Dobbs, *supra* note 20, at 715 (noting the rationales of the paradigm); Johnson, *supra* note 40, at 546–47 (arguing that private ordering is an impetus for the doctrine); Sharkey, *supra* note 43, at 1022–29 (justifying the stranger paradigm).

[116] *See* Johnson, *supra* note 40, at 546–47 (discussing how the ELD promotes private ordering when parties negotiate for contracts).

[117] *See* 532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc., 750 N.E.2d 1097, 1103 (N.Y. 2001) (noting how the imposition of liability would allow recovery by unforeseeable plaintiffs); Dobbs, *supra* note 20, at 715 (describing the policy goals of the stranger paradigm).

[118] *See infra* notes 258–299 and accompanying text.

[119] *See In re* Marriott Int'l, Inc., Costumer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 475–76 (D. Md. 2020) (distinguishing data breach litigation from product liability litigation); Frye, *supra* note 108, at 367 (elaborating upon how the cybersecurity industry is different from other industries).

[120] *See* Commission Regulation 2016/679, *supra* note 3, at 33 (defining a data breach); Alison Grace Johansen, *What Is a Data Breach?*, NORTON (Mar. 10, 2020), https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html [https://perma.cc/5H7Z-2SRU] (same).

[121] *See* IDENTITY THEFT RES. CTR., *supra* note 12, at 2 (detailing data breach statistics across a variety of different industries); Caban, *supra* note 12 (discussing the trend of data breaches in the healthcare industry).

[122] *See* Abi Tyas Tunggal, *The 52 Biggest Data Breaches*, UPGUARD, https://www.upguard.com/blog/biggest-data-breaches [https://perma.cc/MYX5-TQHB] (Feb. 15, 2021) (listing the top fifty-two

Generally, there are three main categories of data breaches: (1) malicious attacks, (2) computer glitches, and (3) human error.[123] The complexity of intertwined computer systems, the rate of innovation, and human fallibility render even the most sophisticated cybersecurity firewalls susceptible.[124] Cybersecurity professionals are in a never-ending metaphorical arms race with hackers to ensure that their defensive cybersecurity systems remain more capable than the hackers' offensive systems.[125]

The defensive capabilities of data controllers and processors, however, are no longer well matched to hackers' offensive capabilities due to chronic underinvestment.[126] Some scholars have maintained that the inadequate cyber-

---

data breaches that have occurred). As of February 2021, the top five data breaches are: (1) CAM4 data breach in 2020, which exposed 10.88 billion PII, including the full names and sexual orientation of users, (2) Yahoo data breach in 2017, which exposed three billion users' passwords and security questions, (3) Aadhaar in 2018, which exposed 1.1 billion biometric data, (4) First American Financial Corporation in 2019, which exposed 885 million records of users, and (5) Verifications.io in 2019, which exposed 763 million users' data. *Id.*

[123] *See* PONEMON INST., IBM SEC., COST OF A DATA BREACH REPORT 8, 15 (2019), https://www.ibm.com/downloads/cas/RDEQK07R [https://perma.cc/3YEW-8599] (explaining the three general causes of data breaches).

[124] *See* MAJORITY STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 115TH CONG., REP. ON THE EQUIFAX DATA BREACH 54 (Comm. Print 2018), https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf [https://perma.cc/E6BZ-6RN7] (describing the Equifax data breach, the issues that arose between the interaction of complex software with outdated systems, and how those two systems were patchwork, making them not work well with one another); N.Y. CYBER TASK FORCE, COLUMBIA SCH. OF INT'L & PUB AFFS., BUILDING A DEFENSIBLE CYBERSPACE 4–7 (2017), https://www.sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF [https://perma.cc/9ZJT-S5DA] (explaining the problems that entities face when trying to secure their networks from data breaches); Jeffery L. Vagle, *Cybersecurity and Moral Hazard*, 23 STAN. TECH. L. REV. 71, 86 (2020) (stating that there is a correlation between the complexity of a software system and security issues with that system).

[125] *See* Roman V. Yampolskiy, *AI Is the Future of Cybersecurity, for Better and for Worse*, HARV. BUS. REV. (May 8, 2017), https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse [https://perma.cc/3M29-D2DR] (describing the rise and innovation of cybersecurity artificial intelligence as an arms race between hackers and industry). Governments are joining the arms race by investing resources into their defensive and offensive capabilities. *See* Anthony Craig & Brandon Valeriano, *Conceptualizing Cyber Arms Races*, 2016 8TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT: CYBER POWER 141, 146, 153 (N. Pissanidis et al. eds., 2016) (detailing that the United States, South Korea, and North Korea have built up their cyber weaponry). In 2019, 23% of recorded data breaches involved nation-state attackers. VERIZON, 2019 DATA BREACH INVESTIGATIONS REPORT: EXECUTIVE SUMMARY 2 (2019), https://d110erj175o600.cloudfront.net/wp-content/uploads/2019/05/2019-DBIR-Executive-Summary.pdf [https://perma.cc/D398-VECM]. An attack by a nation-state raises unique hurdles for data controllers and entities, as their capabilities typically far surpass that of a single hacker. *See The Nation State Actor Has a 'License to Hack'—and They Use It Target Their Adversaries*, BAE SYS., https://www.baesystems.com/en/cybersecurity/feature/the-nation-state-actor [https://perma.cc/2KU7-2RXQ] (identifying that the resources at the disposal of a nation-state allows it to engage in complex attacks on a wide variety of fronts).

[126] *See* KELLY BISSELL ET AL., ACCENTURE SEC., INNOVATE FOR CYBER RESILIENCE: LESSONS FROM LEADERS TO MASTER CYBERSECURITY EXECUTION 8 (2020) (providing an overview of the cybersecurity market), https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf#zoom=40 [https://perma.cc/WAP5-B4CL]; NASDAQ, CYBERSECURITY: INDUSTRY

security practices and investments by data controllers and processors are a result of the moral hazard that exists between the data controllers and processor and data sources.[127] Under this theory, the absence of sufficient civil liability for data controllers and processors, following a data breach, encourages them to shift the negative externalities of weak cybersecurity systems onto the consumer or other entities.[128] The market incentives promote innovation and profit at the expense of cybersecurity.[129] For instance, following a data breach that exposed the credit card numbers of fifty-six million Americans, Home Depot suffered only twenty-five million dollars in liability—0.1% of their net reve-

---

REPORT & INVESTMENT CASE—HXR 3–4 (2020), https://www.nasdaq.com/docs/2020/04/23/Cybersecurity-Industry-Report-Investment-Case-HXR.pdf [https://perma.cc/CUZ2-P59N] (detailing how the aggregate value of cybersecurity venture deals has dropped from $8 billion in 2017 to just over $5 billion in 2019, despite a consistent rise in the data breach losses); Nathaniel Grow & Scott J. Shackelford, *The Sport of Cybersecurity: How Professional Sport Leagues Can Better Protect the Competitive Integrity of Games*, 61 B.C. L. REV. 474, 477–81 (2020) (noting that the lack of cybersecurity investment within professional sports has left teams and fans exposed to cybersecurity breaches); Sales, *supra* note 1, at 1508 ("Companies face little risk of liability to those who are harmed by attacks on their systems or products, and they therefore have weaker incentives to identify and patch vulnerabilities."); Vagle, *supra* note 124, at 86 (arguing that the main focus of manufacturers of products in the digital space is innovation rather than cybersecurity); Benjamin Dean, *Why Companies Have Little Incentive to Invest in Cybersecurity*, THE CONVERSATION (Mar. 4, 2015), http://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570 [https://perma.cc/WEM2-L2DN]. Admittedly, the total value of cybersecurity investment by data controllers and processors has increased in recent years. *See* NASDAQ, *supra*, at 3 (reviewing market investment growth in cybersecurity). The rise in investment should be viewed together with the fact that across seventeen core components of cybersecurity, the average price of those components has increased by 25%. BISSEL ET AL., *supra*, at 8. Additionally, increased investment has not translated to heightened sufficiency of cybersecurity systems. *Id.* For instance, the bottom 74% of companies in terms of cybersecurity standards, on average, reported that only 55% of their business is secure as well as only 55% of them detected breaches while in progress. *Id.*

[127] *See* Vagle, *supra* note 124, at 190–91 (arguing that issues with poor cybersecurity investments stem from inadequate liability); Dean, *supra* note 126 (defining the problem as a moral hazard, where there is an incentive to shift losses onto the consumer). A moral hazard "occurs when one person or organization takes greater risks because others bear the burden or costs of those risks." Dean, *supra* note 126.

[128] *See* David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 980–82 (2016) (arguing that the ELD results in the inability to control the externalities that arise from data breaches and poor cybersecurity); Sales, *supra* note 1, at 1508 (arguing that companies face minimal liability for data breaches).

[129] *See* Vagle, *supra* note 124, at 92–95; Alex Blau, *The Behavioral Economics of Why Executives Underinvest in Cybersecurity*, HARV. BUS. REV. (June 7, 2017), https://hbr.org/2017/06/the-behavioral-economics-of-why-executives-underinvest-in-cybersecurity [https://perma.cc/FV3P-DBN5]. The market incentivizes innovation and rewards the first company to introduce their product to the consumer. Vagle, *supra* note 124, at 90 n.79. Stakeholders in the decision-making process often have incentives to neglect cybersecurity for the increased profits that unbridled innovation and speed can bring to their companies. *Id.* at 92–95; Blau, *supra*. In most cases, the return on investment in innovation and speed programs dwarfs the typical return on cybersecurity investment. *See* Vagle, *supra* note 124, at 92–95 (describing the typical pattern among companies to promote innovation at the expense of cybersecurity); Blau, *supra* (identifying the incentives that executives have to prioritize profit).

nue.[130] Credit unions tasked with indemnifying their customers, however, suffered sixty million dollars in damages as a result of the Home Depot breach.[131] Proponents of increased civil liability for data controllers and processors allege that tougher penalties will counteract the perverse market incentives of the cybersecurity market by making the potential liability costs of underinvestment significantly greater than the cost of adequate investment upfront.[132]

The roadblocks for plaintiffs who wish to bring tort, statutory, or contract-based claims all contribute to the lack of liability for data controllers and processors post-breach.[133] The lack of federal cybersecurity regulation has resulted in civil liability, arguably acting as the invisible hand influencing data controllers and processors' decisions regarding cybersecurity.[134] Data breach lawsuits are typically either dismissed before trial or settled; no consumer data breach litigation case has ever been tried.[135] As a result, the factual question of the actual adequacy of the data controller or processor's systems is generally not a determinative factor for the lawsuit outcome.[136] Instead, success hinges on the ability of the plaintiff to overcome procedural hurdles involving doctrines—like the ELD—that were developed in a different economic age and thus ill-suited for resolving cybersecurity matters.[137] Dismissal leaves little

---

[130] *See* Dean, *supra* note 126 (illustrating the liability that Home Depot faced following an internal data breach).

[131] *See id.* (describing the costs that third parties faced as a result of the Home Depot breach).

[132] *See* Keith N. Hylton, *Property Rules, Liability Rules, and Immunity: An Application to Cyberspace*, 87 B.U. L. REV. 1, 14 (2007) (arguing that the imposition of liability economically is efficient to combat externalities); Opderbeck, *supra* note 128, at 980–82 (explaining the theory around increased liability).

[133] *See* Sales, *supra* note 1, at 1535–38 (arguing that incentives to invest in data security are weak because data breaches do not automatically create civil liability, and attributing this to the ELD and the inadequacy of contract law as a viable cause of action).

[134] *See* Joseph V. DeMarco & Bryan A. Fox, *Data Rights and Data Wrongs: Civil Litigation and the New Privacy Norms*, 128 YALE L.J.F. 1016, 1025 (2019), https://www.yalelawjournal.org/pdf/DeMarcoFox_6vcfc47c.pdf [https://perma.cc/J5ZY-DGT5] (arguing that because there is no applicable federal regulation, civil liability is the predominate default driver of cybersecurity and data privacy standards).

[135] *See, e.g.*, *In re* Anthem, Inc. Data Breach Litig., 327 F.R.D. 299, 318–19 (N.D. Cal. 2018) (describing the lack of precedent of data breach litigation at trial while discussing whether a proposed settlement should be approved); Brief of the Chamber of Commerce of the United States as *Amicus Curiae* in Support of Appellees at 21–25, Attias v. CareFirst, Inc., 863 F.3d 620 (D.C. Cir. 2017) (No. 16-7108) (explaining that data breach class action lawsuits are generally decided at the settlement stage, not on the merits).

[136] *See In re Anthem, Inc.*, 327 F.R.D. at 317 (explaining how the outcome of litigation seldom rests on the actual adequacy of the cybersecurity systems).

[137] *See id.* at 317–18 (attributing the lack of precedent to most cases settling post pre-trial motions); David Balser et al., *INSIGHT: Data Breach Litigation Trends to Watch*, BLOOMBERG L. (Mar. 4, 2019), https://news.bloomberglaw.com/privacy-and-data-security/insight-data-breach-litigation-trends-to-watch [https://perma.cc/7FTV-C2P6] (stating that plaintiffs will continue to struggle to establish standing); Andrew C. Glass & Matthew N. Lowe, *Deepening the Divide: D.C. Circuit Continues Circuit Split Regarding Standing in Data Breach Class Action Based on Risk of Future Harm*, NAT'L L. REV. (July 9, 2019), https://www.natlawreview.com/article/deepening-divide-dc-circuit-

recourse for data breach victims, as the provisions of data-related contracts generally do not include enumerated damages—thus victims have few avenues for statutory-based recovery.[138]

E. The Payment Card Industry's Data Security Standards: Think Before You Swipe

A recurring manifestation of the third-party problem in data breach litigation, due to the ubiquity of the credit payment networks, is the Payment Card Industry Data Security Standards (PCI-DSS).[139] The PCI-DSS is a comprehensive governing scheme—advanced by credit card associations, such as Visa or Mastercard—that establish cybersecurity standards for the securing of individuals' credit card data.[140] There are five actors within the PCI-DSS system: (1) the bank card associations, (2) the card-issuing banks, (3) the cardholders, (4) the acquiring banks that operate the payment networks, and (5) the merchants or retailers.[141] The damages provisions in the individual contracts between parties in the credit card payment network enforces the PCI-DSS.[142] For example,

---

continues-circuit-split-regarding-standing-data-breach [https://perma.cc/2CQT-FM3Q] (describing a circuit split over plaintiffs' ability to get standing in data breach litigation).

[138] *See In re Anthem, Inc.*, 327 F.R.D. at 317–19; Brief of the Chamber of Commerce of the United States as *Amicus Curiae* in Support of Appellees, *supra* note 135, at 23–24 (illustrating how data breach litigation is generally resolved through settlement). A successful defense of a motion to dismiss may all but guarantee some compensation for the damages caused by the data breach. *In re Anthem, Inc.*, 327 F.R.D. at 317–19.

[139] *See* Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 813–15 (7th Cir. 2018) (applying the ELD to data breach litigation involving the credit card payment network); *In re* Arby's Rest. Grp. Inc. Litig., C.A. No. 17-cv-0514, 2018 WL 2128441, at *12 (N.D. Ga. Mar. 5, 2018) (applying the ELD to a data breach lawsuit which involved the payment card industry's data security standards); Sharkey, *supra* note 18, at 366–68 (describing the credit card payment network as the incarnation of the third-party problem in data breach litigation).

[140] *See* PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARDS: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES 10 (2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2 [https://perma.cc/DG28-YNRH] ("The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment."); *PCI Security*, PCI SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/pci_security/ [https://perma.cc/A488-2XPV] (explaining that the major card associations founded the Payment Card Industry (PIC)).

[141] S. Indep. Bank v. Fred's, Inc., No. 15-CV-00799, 2019 WL 1179396, at *2–4 (M.D. Ala. Mar. 13, 2019) (reviewing the credit card payment system, the parties involved in the system, and the contractual commitments that come with the PCI-DSS). *See generally* PCI SEC. STANDARDS COUNCIL, *supra* note 140, at 5 (stating that the PCI-DSS applies to all parties involved in the processing, holding, or securing of credit card data).

[142] *See Fred's, Inc.*, 2019 WL 1179396, at *2–4 (explaining that the Payment Card Industry Data Security Standards' (PCI-DSS) contract has provisions that allow a party in the system to enforce the terms of the PCI-DSS against another party to the PCI-DSS that is in violation of the contract, or has suffered a data breach); Leonard Wills, *The Payment Card Industry Data Security Standards*, ABA J. (Jan. 3, 2019), https://www.americanbar.org/groups/litigation/committees/minority-trial-lawyer/practice/2019/the-payment-card-industry-data-security-standard/ [https://perma.cc/BQ4U-WG4D] ("Though the PCI DSS is not the law, it applies to merchants in at least two ways: (1) as part of a contractual

even though an acquiring bank[143] may not have a direct contract with an issuing bank,[144] through their contracts with the credit card associations, both parties agree to operate in compliance with the guidelines that the PCI-DSS framework establishes.[145] Included within the PCI-DSS are provisions such as fines on individuals that fail to comply with the scheme, standards for securing credit card data, and indemnification provisions that allow injured parties to recover damages.[146] To be involved in the credit card payment network, a retailer or bank must agree to adhere to all the provisions and standards set by the PCI-DSS.[147] The PCI-DSS presents a common manifestation of the third-party problem in data breach litigation, and highlights notable policy issues due to the diversity of the parties involved ranging from an individual consumer to massive corporations such as Visa.[148] Application of the ELD to the PCI-DSS has been a common challenge for multiple courts across multiple jurisdictions and thus has resulted in widely varying outcomes for injured plaintiffs.[149]

II. DATA BREACH & THE ECONOMIC LOSS DOCTRINE: THE PERFECT STORM FOR CIRCUIT SPLITS

The complex nature of data breach litigation has resulted in a perfect storm for widely differing applications of the ELD in data breach litigation across jurisdictions, despite comparatively similar facts.[150] The lack of uni-

---

relationship between a merchant and card company, and (2) states may write portions of the PCI DSS into state law.").

[143] *Glossary*, PCI SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/pci_security/glossary [https://perma.cc/4ZT3-T8CM] (defining "acquiring bank" as "a financial institution, that processes payment card transactions for merchants").

[144] *See id.* (defining "issuer bank" as an "[e]ntity that issues payment cards or performs, facilitates, or supports issuing services").

[145] *See Fred's, Inc.*, 2019 WL 1179396, at *2–4; Wills, *supra* note 142 (illuminating that the PCI-DSS applies to all involved parties through contract).

[146] *See* Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 809 (7th Cir. 2018) (explaining that parties within the PCI-DSS may be fined for noncompliance); Jeff Petters, *What Is PCI Compliance: Requirements and Penalties*, VARONIS, https://www.varonis.com/blog/pci-compliance/ [https://perma.cc/82KZ-XKB3] (Mar. 29, 2020) ("Fines vary from $5,000 to $100,000 per month until the merchants achieve compliance.").

[147] *See* Petters, *supra* note 146 (describing the indemnification process for injured parties within the system).

[148] *See* Sharkey, *supra* note 18, at 348, 367–72 (describing the complexity of the third-party problem and suggesting that courts have often misapplied the ELD in that context).

[149] *See id.* at 371 (discussing how courts have misapplied the ELD in data breach litigation).

[150] *See, e.g.*, *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1172–77 (D. Minn. 2014) (applying the ELD of eleven different states in a data breach class action, and finding that, in six of the states, the ELD would bar the plaintiffs' negligence claims, and in five of the states, the ELD would not bar such claims for various reasons). *See generally* MATTHIESEN, WICKERT & LEHRER, S.C., ECONOMIC LOSS DOCTRINE IN ALL 50 STATES 13–36, https://www.mwl-law.com/wp-content/uploads/2018/02/ECONOMIC-LOSS-DOCTRINE-CHART-1.pdf [https://perma.cc/65AP-A6WG] (2021) (listing the ELD rules of all fifty states).

formity in the application of the ELD and its exceptions has resulted in a plaintiff's success hinging on the particular approach of the jurisdiction where their claims are brought, instead of on the merits of their case.[151] It is common in data breach litigation class actions, in which all class members suffered the same injury from the same breach, for one group of plaintiffs to have their case dismissed under one state's law, foreclosing damages, while a similar group is permitted to proceed.[152]

For instance, in 2014, in *In re Target Corp. Customer Data Security Breach Litigation*, the U.S. District Court for the District of Minnesota grappled with a multi-jurisdictional class action in which the court had to decide whether to apply the ELD to the negligence claims of plaintiffs from eleven different states.[153] Operating within the stranger paradigm, the court found that six of the plaintiff's states do not permit any ELD exceptions; thus, the ELD resulted in the dismissal of those claims.[154] In the other five states' ELD doctrines, various exceptions allowed those plaintiffs' claims to survive dismissal.[155] Even within the five states that did not apply the ELD, the courts' rationale as to why ranged from invoking fiduciary duty exceptions to citing a pure independent duty exception.[156] The plaintiffs from the six states where the ELD would bar their tort claims had suffered the exact same damages, from the same breach event, as their co-plaintiffs, yet were left with a singular via-

---

[151] *See, e.g.*, *In re Target Corp.*, 66 F. Supp. 3d at 1172–77 (holding that the ELD's exceptions would only permit plaintiffs in five of the eleven states at issue to proceed with their tort claims).

[152] *See, e.g.*, *id.*

[153] *See id.* In 2014, in *In re Target Corp. Customer Data Security Breach Litigation*, the U.S. District Court for the District of Minnesota emphasized that the Target data breach represented one of the largest in history at the time, exposing the credit card data of 110 million customers. *Id.* at 1158. The court recounted that the breach exposed the credit card numbers of all Target customers over a three-week holiday season period. *Id.* The Target customer plaintiffs alleged that, due to the data breach, they experienced credit card charges, late fees, and card replacement fees, as well as the burden of credit monitoring. *Id.*

[154] *See id.* at 1172–76 (distinguishing the current facts from cases where the parties had quasi-privity, and dismissing the claims of three different states); Sharkey, s*upra* note 18, at 348 (articulating what the stranger paradigm is). The court's adoption of a stranger paradigm is most explicit in their judgement of the application of Pennsylvania's ELD. *See In re Target Corp.*, 66 F.3d at 1175–76. The defendant sought to invoke prior state case law surrounding data breaches in the credit card payment system where the plaintiff and defendant were both financial institutions found to have quasi-privity due to the PCI-DSS. *Id.* at 1175. The court found that the existence of privity made application of the ELD "more straightforward," as the parties were financial institutions engaged in lengthy contracts, rather than consumer retailers whose only contractual privity manifested from Target purchases. *Id.* The court noted that this lack of privity, however, did not foreclose the possibility of an exception for the Pennsylvania plaintiffs. *See id.* 1175–76 (allowing the Pennsylvania plaintiffs' claims to survive dismissal).

[155] *See In re Target Corp.*, 66 F.3d at 1172–76 (refusing to dismiss the ELD of five states, as the plaintiffs had sufficiently pled that an ELD exception might apply).

[156] *See id.* (applying the ELD exceptions of five states, ranging from the fiduciary duty, special relationship, and traditional independent duty exceptions to the plaintiffs' negligence claims).

ble claim of unjust enrichment.[157] Their co-plaintiffs from states that would not apply the ELD in this context, however, could still pursue negligence claims, thus giving them greater leverage in settlement negotiations.[158]

In the years since *In re Target Corp.*, state supreme courts have routinely adopted more pliable versions of the ELD to permit exceptions in data breach litigation.[159] In the seminal 2018 decision *Dittman v. UPMC*, the Supreme Court of Pennsylvania expanded Pennsylvania's ELD to provide an independent duty exception.[160] Under the commonwealth's independent duty exception, the ELD would not apply if the plaintiffs, employees of a medical center, could sufficiently plead that the defendant, the medical center, owed them a duty of care.[161] To reach this holding, the Pennsylvania Supreme Court had to distinguish precedent that endorsed a more restrictive version of the ELD.[162] No precedent had expressly held that an independent duty exception existed; instead, the court relied on prior language that simply alluded to the practical reality that under some undefined circumstances the ELD should not apply.[163]

Dittman highlights the hurdles that plaintiffs face in data breach litigation and illustrates how courts have struggled to allow for the imposition of liability while preserving consistency with ELD precedent and policy goals.[164] This Part

---

[157] *See id.* at 1178–79 (holding that plaintiffs' claims of unjust enrichment were plausible enough to survive dismissal, but dismissing most of the plaintiffs' causes of actions).

[158] *Id.*; Laura Inglis et al., *Experiments on the Effects of Cost Shifting, Court Costs, and Discovery on the Efficient Settlement of Tort Claims*, 33 FLA. ST. U. L. REV. 89, 91 (2005) (explaining the economic decisions that typically underlie settlements).

[159] *See* 66 F.3d at 1178–79; Jason M. Rand, *"Common Law Duty to Protect Employee Data Undercuts Contractual Liability Exclusion,"* CYBERINSURANCE L. BLOG (Dec. 3, 2018), https://www.databreachninja.com/common-law-duty-to-protect-employee-data-undercuts-contractual-liability-exclusion/ [https://perma.cc/UY8T-L9ET] (noting that a spring of cases has shown that courts are routinely finding ways to impose liability in data breach litigation).

[160] *See* 196 A.3d 1036, 1040 (Pa. 2018) (holding broadly that an independent duty exception to the commonwealth's ELD rule would apply, so long as the plaintiff could successfully plead that such a duty existed independently under the common law). In 2018, in *Dittman v. UPMC*, the Supreme Court of Pennsylvania was operating in the stranger paradigm of the ELD. *See id.* at 1054 (stating that the applicable duty did not come from contract law). The court held that if a duty arises through contract, it will preclude tort remedies; however, if that duty exists in the common law, then the ELD will not bar the claims. *Id.* The court concluded that the employment contract did not establish any duties related to the securing of data. *See id.* (stating that contract law did not govern).

[161] *Id.* at 1055.

[162] *See id.* at 1054 (describing prior case law that had invoked a far more absolute version of the doctrine).

[163] *See id.* (quoting prior precedent that alluded to ELD exceptions). The court's final justification for a new independent duty exception came from a 1995 South Carolina Supreme Court decision, cited in a previous Pennsylvania ELD case. *Id.* In that case, the South Carolina Supreme Court noted that, despite a potential ELD bar, economic recovery could come from a variety of tort claims. *Id.* Applying that reasoning, the Pennsylvania Supreme Court in *Dittman* concluded that there should and does exist an independent duty exception to the ELD. *Id.*

[164] *See id.* (highlighting that the common law is not stagnant, and noting that it is within the ability of state supreme courts to ensure that the law evolves with changing facts and times, as with the

further analyzes the ELD and data breach litigation by providing case illustrations where the ELD did and did not apply under both the stranger paradigm and contracting parities paradigm.[165] Section A discusses instances under both paradigms where courts have applied the ELD to bar a plaintiff's tort claims for data breach litigation, as there was either no exception to the rule or the exception did not apply.[166] Section B explores instances where courts in both paradigms have decided not to apply the ELD to plaintiffs' tort claims in data breach litigation because there existed an applicable ELD exception under state law.[167]

A. Data Breach and the Economic Loss Doctrine: When Courts Have Applied the Economic Loss Doctrine in Data Breach Litigation

Courts have applied the ELD in data breach litigation under both the stranger and contracting parties paradigms.[168] The contracting parties paradigm is implicated when the parties in data breach litigation have a contract governing the rights and duties owed between them relating to the PII.[169] The stranger paradigm in data breach litigation is often implicated when the parties do not have direct contractual privity governing the rights and duties owed between them.[170] Subsection 1 of this Section examines when courts have applied the ELD in the contracting parties paradigm due to a contract governing the rights and duties between the plaintiff and defendant.[171] Subsection 2 analyzes when courts have applied the ELD in the stranger paradigm, as no independent duty existed between the parties.[172] Subsection 3 discusses when courts have applied the ELD to third-party problems involving the PCI-DSS, characterizing the parties as within the contracting parties paradigm and letting the terms and conditions of the PCI-DSS govern damages.[173]

1. Contracting Parties: When the Economic Loss Doctrine Applies to Contracting Parties in Data Breach Litigation

In the contracting parties paradigm, courts have routinely applied the ELD to data breach litigation cases in an effort to restrict recovery to contract

changing landscape of the digital economy and the unique facts it creates); Rand, *supra* note 159 (noting the trend for state supreme courts to allow for liability in data breach litigation).

[165] *See infra* notes 168–212 and accompanying text.

[166] *See infra* notes 213–251 and accompanying text.

[167] *See infra* notes 174–212 and accompanying text.

[168] *See infra* notes 174–212 and accompanying text.

[169] Sharkey, *supra* note 18, at 344–45 (defining the contracting parties paradigm).

[170] *See id.* at 344 (describing the stranger paradigm).

[171] *See infra* notes 174–197 and accompanying text.

[172] *See infra* notes 198–204 and accompanying text.

[173] *See infra* notes 205204–212 and accompanying text.

law, and the contract itself, by foreclosing tort recovery.[174] For example, in 2016, in *Silverpop Systems, Inc. v. Leading Market Technologies, Inc.*, the U.S. Court of Appeals for the Eleventh Circuit held that Georgia's ELD barred tort claims arising from a data breach where there existed contractual privity between the parties.[175] Georgia's ELD includes an independent duty exception; however, the court held that, when an independent non-contractual common law duty of care is supplanted by the terms of a contract, the ELD operates as a complete shield against tort liability for purely economic damages.[176] The plaintiff's negligence claim explicitly related to the defendant's duties—already established through contract—to reasonably safeguard the plaintiff's data.[177] The court held that for the plaintiff to recover damages resulting from the breach, they were confined to the contract terms and thus could not assert other tort liability.[178]

Similarly, in 2020, in *In re Marriott International, Inc., Customer Data Security Breach Litigation*, the U.S. District Court for the District of Maryland explained in dicta that the applicable state ELD barred tort claims for purely economic losses between two parties who have entered into a contract.[179] The

---

[174] *See* Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 815 (7th Cir. 2018) (explicitly adopting the contracting parties paradigm to bar the plaintiffs' tort claims); Silverpop Sys., Inc. v. Leading Mkt. Techs., Inc., 641 F. App'x 849, 850–51 (11th Cir. 2016) (per curiam) (applying the ELD to bar the tort claims of the plaintiff because their existed a contract between the parties); *In re* Marriott Int'l, Inc., Costumer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 475–76 (D. Md. 2020) (holding that the ELD barred the tort claims of the plaintiffs where a contract existed); *In re* Sony Gaming Networks & Consumer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 966–74 (S.D. Cal. 2014) (applying the ELD because the plaintiffs had not satisfied the exception to the ELD in the contracting parties paradigm); Sharkey, *supra* note 18, at 344–45 (defining the contracting parties paradigm as when a contract governs the rights and duties owed between the plaintiff and defendant).

[175] *See* 641 F. App'x at 853 (holding that the duty arose under the contract, which precluded tort liability due to the ELD). In 2016, in *Silverpop Systems v. Leading Market Technologies, Inc.*, the U.S. Court of Appeals for the Eleventh Circuit noted that the plaintiff had entered into a marketing services agreement that required the plaintiff to store personal data on the provider defendant's servers. *Id.* at 850. The contract contained provisions both limiting liability and governing the storage of the data. *Id.* In 2010, a data breach exposed the plaintiff's PII. *Id.*

[176] *See id.* at 853 (stating that the independent duty exception did not apply because the contract between the two parties governed the alleged duty owed to the plaintiff by the defendant, and, thus, the ELD barred other claims).

[177] *See id.* (holding that the contract between the defendant and the plaintiff governed the duties alleged to have broken).

[178] *Id.*

[179] *See* 440 F. Supp. 3d at 475–76 (stating, without officially deciding the issue, that Illinois' ELD would most likely bar negligence suits). In 2020, in *In re Marriott International, Inc., Costumer Data Security Breach Litigation*, the U.S. District Court for the District of Maryland explained that the defendant, a hotel chain, had acquired a smaller hotel chain to make it the largest hotel company in the world. *Id.* at 454–55. The data breach occurred at the acquired hotel chain's locations. *Id.* The plaintiffs, guests of the hotel or users of other hotel services, would provide their name, address, phone number, payment information, other personal preferences, and in some cases passport information, when checking in or booking a room. *Id.* The ensuing data breach occurred continuously both before the acquisition and after from the years 2014 to 2018. *Id.* The breach exposed the data of all customers

defendant, a hotel chain, had agreed to "reasonable organizational, technical and administrative measures to protect [its customers'] Personal Data" in a contract with the plaintiffs, customers of Marriott properties and other services.[180] Despite the defendant's attempts to ensure data security, a breach exposed roughly 383 million visitor records, twenty-four million passport numbers, and nine million credit and debit card numbers.[181] After a detailed analysis of the applicable Illinois ELD in regards to the Illinois plaintiffs, the court stated that the ELD would most likely bar those affected customers' claims, before noting that the Illinois Supreme Court may be amenable to changing the state's ELD.[182]

The district court acknowledged policy considerations weighing against application of the ELD but declined to make a pronouncement on the issue; it instead dismissed the Illinois plaintiffs' case on the theory that, under Illinois law, the defendant owed no independent non-contractual duty to the plaintiffs.[183] The Illinois Supreme Court had initially adopted the ELD to protect manufactures from the potentially unlimited economic damages that could arise from defective products.[184] The court characterized that policy concern as inapplicable in the context of data breaches, however, because the claims at issue were not alleging defects in the defendant's core product—hotel rooms—but rather a separate harm from their handling of plaintiffs' data.[185] The court did not definitively rule on the applicability of the ELD to data breaches; how-

---

at the acquired hotels location from the years 2014 to 2018. *Id.* The plaintiffs sued as a collective class ranging across seven states. *Id.* The court applied Illinois law to the Illinois plaintiffs. *Id.*

[180] *Id.* at 483 (alteration in original) (quoting Second Amended Consolidated Complaint ¶ 317, *id.* (No. 19-md-2879)).

[181] *Id.* at 454–55.

[182] *See id.* at 475–76 (stating that without deciding on the issue that the Illinois Supreme Court may very well apply the ELD to bar tort claims in data breach litigation, but laying out a policy argument distinguishing the ELD from other types of tort claims). The *In re Marriott* court noted that the ELD was created in response to product liability litigation in Illinois. *Id.* The court noted that in the unique context of data breach litigation, however, the data product itself is never damaged, thus identifying one reason why the Illinois Supreme Court should rework this ill-fitting doctrine. *Id.*

[183] *See id.* at 475 ("Data security breach cases are unique in many ways."). First, the court noted that data breach litigation is relatively new and that the doctrine surrounding it is not settled. *See id.* (noting that the transition to a digital economy has been recent). Secondly, the court sought to distinguish product liability litigation from data breach litigation because in data breach litigation the product itself is not damaged. *See id.* at 475–76 (distinguishing data breach litigation from product liability litigation).

[184] *Id.* at 475–76 (stating that the ELD was first implemented in product liability suits to protect a manufacturer of a defective product from the potentially unlimited liability that could arise if a court allowed economic losses due to the defective nature of the product without any further damages to property or persons).

[185] *Id.* ("When the hotel induces the consumer to book a room online, and to hold the reservation by providing a bank card and other personal information, but fails to protect that information from hackers, the injury sustained by the consumer has nothing at all to do with the quality or fitness of the 'product' purchased—the hotel room.").

ever, it dismissed the Illinois plaintiffs' claims for failure to demonstrate that an established exception to the ELD applied.[186]

Some jurisdictions provide for exceptions to the ELD in the contracting parties paradigm.[187] Most courts, however, still require plaintiffs to overcome the relatively high hurdle set by the special relationship test, which considers the six factors outlined in *J'Aire Corp. v. Gregory* in 1979, in the contracting parties paradigm to avail themselves of an ELD exception.[188] In 2014, in *In re Sony Gaming Networks & Customer Data Security Breach Litigation*, the U.S. District Court for the Southern District of California applied the ELD to bar the specific California plaintiffs' negligence claims against the defendants, despite California's established special relationship exception.[189] The plaintiffs, users of the PlayStation Network, had turned over PII and agreed to a terms-and-services contract in exchange for access to defendants', entities of Sony, free gaming network.[190] The plaintiffs, representing a multi-state class action, brought a combination of statutory-based and tort-based claims against the defendants following a data breach.[191] The court held that the ELD did not per se bar the tort claims of the California plaintiffs; however, the California plaintiffs

[186] *Id.* at 476 ("[I] find that based on the current state of Illinois law Defendants did not owe a duty to Plaintiffs to protect their personal information, notwithstanding that the Illinois Supreme Court itself has not spoken to the issue."). The district court dismissed the Illinois plaintiffs' negligence claims, leaving the affected customers without recourse or an available cause of action. *See id.* at 495 (dismissing the negligence claims of the Illinois plaintiffs). The plaintiffs from California, Florida, Georgia, Maryland, Michigan, New York, and Oregon, however, were able to proceed forward with their claims. *Id.* These plaintiffs' claims could proceed due to exceptions to the ELD and their ability to bring breach of contract claims. *Id.* at 495.

[187] *See, e.g.*, *In re* Sony Gaming Networks & Consumer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 966–74 (S.D. Cal. 2014) (holding that there was no special relationship because the plaintiffs had failed to plead facts).

[188] *See* Sharkey, *supra* note 18, at 366 (illustrating that, within the contracting parties paradigm, the special relationship test is a higher standard). *Compare* Portier v. NEO Tech. Sols., No. 17-cv-30111, 2019 WL 7946103, at *17–22 (D. Mass. Dec. 31, 2019) (holding that the plaintiffs had adequately pled that a special relationship existed with the defendants), *with In re Sony Gaming Networks*, 996 F. Supp. 2d at 966–74 (holding that the plaintiffs had failed to adequately plead that a special relationship existed between the plaintiffs and the defendants).

[189] *See* 996 F. Supp. 2d at 966–74 (applying the ELD to the negligence claims of the plaintiffs). In 2014, in *In re Sony Gaming Networks & Customer Data Security Breach Litigation*, the U.S. District Court for the Southern District of California explained that the plaintiffs were all users of the defendants' online gaming network. *Id.* at 954. To sign up for the gaming network, the defendants required users to agree to their terms of service and register for accounts using PII. *Id.* In April of 2011, hackers accessed the gaming network, shut it down for a period of four days, and stole the PII of many of the users. *Id.* None of the plaintiffs alleged that they suffered any financial harm because of the hacking. *Id.* at 956–57. The plaintiffs were "a nationwide putative consumer class." *Id.* at 953.

[190] *Id.* at 954.

[191] *See id.* at 953–54 (describing the causes of action that the plaintiffs alleged).

had failed to adequately plead that a special relationship existed and thus could not invoke an ELD exception.[192]

To determine whether a special relationship existed in *In re Sony Gaming Networks*, the court applied the *J'Aire* test.[193] In applying the special relationship test, a court must determine whether the combined weight of the nature of the relationship between the parties, the type of damages caused, and the policy goals implicated are such that additional tort liability should be imposed.[194] The California court held that the California plaintiffs had sufficiently pled the fourth, fifth, and sixth *J'Aire* factors: (4) there was a close connection between the defendants' conduct and the plaintiffs' injury, (5) moral blame could be attached to the defendants' conduct, as they knew of their security lapses, and (6) imposing liability would incentivize other data controllers and processors to sufficiently secure data.[195] The court, however, held that the plaintiffs had failed to sufficiently plead the first, second, and third *J'Aire* factors: (1) the actions of the defendants affected all potential consumers, not just the plaintiffs, (2) the plaintiffs' alleged injuries were not foreseeable to the defendant, and (3) there was not enough degree of certainty in the injuries.[196] Considering the six factors collectively, the court failed to find a special relationship between the parties, and it thus applied the ELD to the plaintiffs' negligence claims.[197]

---

[192] *See id.* at 973 (holding that the California plaintiffs had failed to sufficiently plead that a special relationship existed to permit their tort claims for purely economic damages). The U.S. District Court for the Southern District of California's holding in *In re Sony Gaming Networks* specifically related to the California plaintiffs. *See id.* (stating that California's ELD barred the tort claims of the plaintiffs). The court concluded that the Massachusetts plaintiffs' ELD claims were also barred because Massachusetts's ELD generally prohibited the claims brought by those plaintiffs. *See id.* at 967 (illustrating that the Massachusetts ELD generally prohibits economic damages and has few exceptions).

[193] *Id.* at 967 (determining that the California plaintiffs had not sufficiently shown that the six-factor special relationship exception applied to them).

[194] *See, e.g.*, J'Aire Corp. v. Gregory, 598 P.2d 60, 63 (Cal. 1979) (outlining the six factors and explaining the rationale behind them).

[195] *In re Sony Gaming Networks*, 996 F.2d at 972 (finding that the plaintiffs had adequately pleaded the *J'Aire* factors, which favored the plaintiffs' argument).

[196] *Id.* at 970–72 (holding that the California plaintiffs' claims were not enough for the court to determine that a special relationship existed between the two parties). The court's holding hinged on the California plaintiffs' abstract damage claims. *See id.* at 969–70 (noting that the California plaintiffs' alleged facts did not reach the plausibility standard). The court rejected the plaintiffs' allegation that the diminution in value of their gaming devices was a sufficient economic loss under the ELD's special relationship test. *Id.* For that reason, among others, the court held that the special relationship exception should not apply. *Id.*

[197] *Id.* at 966–74 (holding that, despite the plaintiffs pleading the fourth, fifth, and sixth factors adequately, their failure to establish the first three meant that a special relationship did not exist between the parties, and thus the ELD barred the plaintiffs' negligence claims).

2. Stranger Paradigm: When No Contract Governs the Parties' Relationship & the Economic Loss Doctrine Applies

When a court finds that two parties lack contractual privity—thus implicating a stranger paradigm—courts have applied the ELD to bar purely economic claims.[198] In these cases, no independent duty exception permits tort recovery.[199] Although the common law is slowing evolving, this approach remains the majority approach to the ELD.[200] For example, in 2008, in *Sovereign Bank v. BJ's Wholesale Club*, *Inc.*, the U.S. District Court for the Middle District of Pennsylvania applied Pennsylvania's ELD to bar a negligence claim resulting from a data breach, as the plaintiffs, banks that issued credit cards to their customers, claimed to have solely suffered economic damages.[201] The plaintiffs asserted that the foreseeability of the specific harm that befell them should trump the ELD because the facts did not implicate the stranger paradigm's policy goal of limiting unforeseeable liability.[202] The court rejected this argument by invoking the policy goal implicated by the stranger paradigm—the concern that allowing such negligence claims between parties without any contractual privity would permit "anyone 'in the economic chain'" to hold the defendant responsible for economic damages.[203] At the time of the *Sovereign Bank* decision, Pennsylvania's ELD did not include an independent duty exception; thus, the rigid application of the doctrine applied to dismiss the plaintiffs' tort claims.[204]

---

[198] *See* Sovereign Bank v. BJ's Wholesale Club, Inc., 395 F. Supp. 2d 183, 203–04 (M.D. Pa. 2005) (holding that the ELD barred the tort claims of the plaintiffs), *aff'd*, 533 F.3d 162 (3d Cir. 2008).

[199] *See, e.g.*, *id.* (baring the plaintiffs' tort claims).

[200] *See* MATTHIESEN, WICKERT & LEHRER, S.C., *supra* note 150, at 4 (describing the strict application of the ELD as being the majority rule after conducting a fifty-state survey of the ELD).

[201] 395 F. Supp. 2d at 203–04. In 2008, in *Sovereign Bank v. BJ's Wholesale Club*, *Inc.*, the U.S. District Court for the Middle District of Pennsylvania noted that the plaintiffs were banks within the credit card network. *Id.* at 188–89. The defendant was a retailer who had suffered a data breach that exposed the PII of their customers. *Id.* The plaintiffs proceeded under a third-party beneficiary breach of contract claims and a negligence claim against the defendant. *Id.* at 191. At no point did the plaintiffs claim that privity existed, resulting in the court's implicit adoption of a stranger paradigm approach. *See id.* (stating that the plaintiffs sought to plead equitable remedies of contract law, in that they were the third-party beneficiaries to the contract that defendant had signed); Sharkey, *supra* note 18, at 350–51 (categorizing *Sovereign Bank* as a stranger paradigm case).

[202] *See Sovereign Bank*, 395 F. Supp. 2d at 189–90 (arguing there was a high level of likelihood such a harm could occur); Sharkey, *supra* note 18, at 350–51 (noting that the plaintiffs sought to rely on the theory that the harm was foreseeable and that the ELD should not apply as a result).

[203] *See Sovereign Bank*, 395 F. Supp. 2d at 204 (quoting Aikens v. Balt. & Ohio R.R. Co., 501 A.2d 277, 279 (Pa. Super. Ct. 1985)) (fearing that the imposition of economic damages would allow for any actor in the economic chain to bring tort claims); Sharkey, *supra* note 18, at 350–51 (stating the arguments of the plaintiffs).

[204] *See Sovereign Bank*, 395 F. Supp. 2d at 205 ("We will therefore apply the economic loss doctrine to bar Sovereign's negligence claim."). *Compare id.* (applying the ELD to bar the negligence claims in a 2005 data breach litigation case), *with* Dittman v. UPMC, 196 A.3d 1036, 1040 (Pa. 2018)

3. Third-Party Problem: When Parties in Data Breach Litigation Are Linked by a Web of Contracts and the Economic Loss Doctrine Applies

Finally, some courts have applied the ELD in the third-party problem to data breach litigation involving the PCI-DSS system.[205] The PCI-DSS's complex web of contracts requires the court to make a choice between applying the contracting parties paradigm or the stranger paradigm.[206] For example, in 2018, in *Community Bank of Trenton v. Schnuck Markets, Inc.*, the U.S. Court of Appeals for the Seventh Circuit explicitly adopted the contracting parties paradigm and thus applied the ELD to bar the plaintiffs', financial institutions that issued credit and debit cards to customers, tort claims following a breach in the defendant's, a retailer, credit card processing system. [207] The court reasoned that since the PCI-DSS represents a set of contracts governing data storage, and includes damages for non-compliance, the system embodies an allocation of risk through contracting by sophisticated parties.[208] The plaintiffs' and defendant's rights and duties were thus mutually governed by the PCI-DSS through contract, despite that contract not being directly with one another.[209] The "web of contracts" at issue amounted to sufficient privity to implicate the contracting parties paradigm.[210] Accordingly, available remedies must be rooted in contract.[211] The court dismissed the plaintiffs' negligence claims and all

(holding that, in 2018, the Pennsylvania ELD includes an independent duty exception that allows negligence claims to proceed in data breach litigation).

[205] *See, e.g.*, Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 815 (7th Cir. 2018) (explicitly stating that the situation involved a third-party problem, and adopting the ELD to preclude the plaintiffs' claims, as the plaintiffs had only suffered economic losses due to the negligence of the defendant).

[206] *See id.*; Sharkey, *supra* note 18, at 366–68 (describing the credit card payment network as the incarnation of the third-party problem in data breach litigation).

[207] *See* 887 F.3d at 815 (holding that the ELD would bar the tort claims of the plaintiffs because they were operating within the contracting parties paradigm). In 2019, in *Community Bank of Trenton v. Schnuck Markets, Inc.*, the U.S. Court of Appeals for the Seventh Circuit observed that the plaintiffs, financial institutions that issued credit cards and debit cards to customers, alleged that the defendant, a grocery store, failed to secure data, causing them to incur financial losses by having to indemnify their customers. 887 F.3d at 807. Hackers had accessed seventy-nine of the defendant's one hundred stores, and allegedly stole the credit card information of twenty thousand customers. *Id.* at 810. The plaintiffs estimated to have incurred losses of approximately ten million. *Id.* at 811.

[208] *Id.* at 815 (holding that the parties had voluntarily entered into a "web of contracts" that would define the rights and duties owed between them, which included remedies for damages that would occur and standards for the storage of data).

[209] *Id.* (noting that a mutually agreed-upon standard governed the relationship between the parties).

[210] *Id.* (stating that the "web of contracts" within the PCI-DSS system amounted to quasi-privity between the two parties, and thus required the court to take a contracting parties paradigm approach).

[211] *See id.* at 823 (declining to allow damages outside of the contract).

theories that would have supplemented the plaintiffs' contractual remedies for the losses that they suffered due to the defendant's alleged negligence.[212]

B. When Courts Have Not Applied the Economic Loss Doctrine in Data Breach Litigation

Some courts, in assessing similar facts as found in the aforementioned cases, have not applied the ELD to data breach litigation, and have instead adopted a more pliable version of the doctrine with exceptions that permit tort recovery for economic damages.[213] Section B of this Part discusses instances in which courts did not apply the ELD in data breach litigation, despite the fact that plaintiffs were only asserting economic damages.[214] Subsection 1 reviews when courts in the contracting parties paradigm have not applied the ELD due to the existence of a special relationship between the parties.[215] Subsection 2 examines when courts in the stranger paradigm have not applied the ELD because there existed a non-contractual independent duty, arising from the common law, between the parties.[216] Subsection 3 analyzes when courts in a third-party problem have not applied the ELD because a court determined that there existed no contractual privity between the parties.[217] In these instances where a court has not applied the ELD, the courts permitted plaintiffs to move forward with the merits of their tort claims, and the incentives to settle greatly increased their probability of recovery.[218]

1. Contracting Parties Paradigm: When There Exists a Contract Between the Two Parties in Data Breach Litigation and the Court Did Not Apply the Economic Loss Doctrine

It has famously been said that the ELD is an attempt to "to prevent the law of contract and the law of tort from dissolving into the other."[219] Simply

---

[212] *Id.* at 826 ("We agree with the district court that neither Illinois nor Missouri would recognize any of the plaintiff banks' theories to supplement their contractual remedies for losses they suffered as a result of the Schnucks data breach."). By denying any supplemental damages greater than agreed to in the contract, the Seventh Circuit in *Community Bank of Trenton* was de facto applying the ELD as a border line between tort and contract law. *See id.* (denying any damages that would result in more than what was agreed to in the contract); Johnson, *supra* note 40, at 551–52 (arguing that the ELD serves as a "boundary-line" between tort and contract law).

[213] *See infra* notes 219–251 and accompanying text.

[214] *See infra* notes 219–251 and accompanying text.

[215] *See infra* notes 219–232 and accompanying text.

[216] *See infra* notes 233–242 and accompanying text.

[217] *See infra* notes 243–251 and accompanying text.

[218] *See infra* notes 219–251 and accompanying text.

[219] *See* R. Joseph Barton, Note, *Drowning in a Sea of Contract: Application of the Economic Loss Rule to Fraud and Negligent Misrepresentation Claims*, 41 WM. & MARY L. REV. 1789, 1796 (2000) (quoting Rich Prods. Corp. v. Kemutec, Inc., 66 F. Supp. 2d 937, 969 (E.D. Wis. 1999), *aff'd*, 241 F.3d 915 (3d Cir. 2001)).

put, the ELD restricts a plaintiff's recovery to solely damages delineated in the contract or those available through contract law.[220] Despite this, some courts have carved out a special relationship exception to the contracting parties paradigm.[221] This exception analyzes the relationship between the parties, the nature of harm done, and other policy implications to determine if tort liability should be permitted despite a readably enforceable contract.[222] In 2019, in *Portier v. NEO Technology Solutions*, the U.S. District Court for the District of Massachusetts did not apply the ELD to the plaintiffs' tort claims, despite their contractual privity with the defendants arising from an employment contract.[223] The plaintiffs in *Portier* were employees of the defendants, NEO Technology Solutions and affiliates, and their employment contract required them to turn over PII.[224] A phishing email scam resulted in a data breach exposing the plaintiffs' PII.[225] *Portier* involved two classes of plaintiffs, with one group located in Massachusetts and the other in California.[226] The court applied the *J'Aire* special relationship test to the plaintiffs located in California and determined that those plaintiffs had sufficiently pled that a special relationship existed.[227] Because the Massachusetts ELD foreclosed recovery for the Massachusetts plaintiffs, the court did not permit those plaintiffs to bring tort claims, despite the fact that these plaintiffs suffered the exact same harm from the data breach as did their California counterparts. [228]

---

[220] *See id.* (describing how the ELD separates contract and tort law).

[221] *See, e.g.*, Portier v. NEO Tech. Sols., No. 17-cv-30111, 2019 WL 7946103, at *17–22 (D. Mass. Dec. 31, 2019) (applying the special relationship test to the ELD in data breach litigation when the parties had a contractual relationship).

[222] *See, e.g.*, J'Aire Corp. v. Gregory, 598 P.2d 60, 63 (Cal. 1979) (detailing a six-factor test, which balances causation and the moral blame factors, with the policy impact of imposing liability).

[223] 2019 WL 7946103, at *17–22 (explaining that the parties had entered into an employment contract). In 2019, in *Portier v. NEO Technology Solutions*, the U.S. District Court for the District of Massachusetts explained that the plaintiffs were employees of the key defendant, NEO Technology Solutions—a tech company—and that the terms of their employment contract required them to turn over PII to the key defendant. *Id.* at *1. The vice president of that defendant company had opened a phishing email that resulted in the disclosure of the employees' tax forms. *Id.* The forms were password protected, but the hackers guessed the password. *Id.* The key defendant quickly discovered the breach and took steps to re-secure its systems. *Id.* The plaintiffs alleged that they had already suffered damages due to the breach and were likely to suffer damages further damages in the future. *Id.* at *2.

[224] *Id.* at *1 (explaining that a data breach had exposed the W2 forms of the plaintiffs).

[225] *Id.*

[226] *Id.*

[227] *Id.* at *17–22 (applying the *J'Aire* test to the negligence claims of the California plaintiffs). The district court did not apply the ELD to the Massachusetts plaintiffs' negligence claims. *Id.* at *20. As the law stood, however, the court could not affirmatively allow the plaintiffs' claims to go forward. *Id.* Yet the court predicted that, as the Supreme Court of Pennsylvania did in *Dittman v. UMPC*, the Massachusetts Supreme Judicial Court could adopt an exception to the ELD. *See id.* ("[I]t is likely that the Massachusetts Supreme Judicial Court . . . would apply *Dittman*'s reasoning and permit recovery for pecuniary losses due to Defendants' negligence in the circumstances presented here.").

[228] *See id.* at *17–30 (applying the ELD to the Massachusetts plaintiffs because Massachusetts law prohibited tort recovery for economic damages).

The court concluded that the California plaintiffs met all six *J'Aire* factors: (1) the defendants intended the transaction to specifically affect the plaintiffs, as the plaintiffs were required to turn over their data due to their employment status, (2) the defendant's previous data breaches made the harm foreseeable, (3) the plaintiffs sufficiently pled injury, (4) there was a temporally close connection between the defendant's conduct and the harm, (5) the moral blame was significant, as the defendant failed to take the necessary steps to protect the plaintiffs' data after requiring that plaintiffs hand over their data, and (6) imposing tort liability would incentivize employers to properly secure vulnerable employee data.[229] Accordingly, the court did not apply the ELD to the tort claims of the California plaintiffs.[230] The court dismissed, for unrelated reasons, all the statutory claims brought by the multi-state plaintiff class.[231] The Massachusetts plaintiffs were thus left without any viable cause of action, while the California plaintiffs' case proceeded forward due to the special relationship test.[232]

2. Stranger Paradigm: When No Contract Exists Between the Parties in Data Breach Litigation and the Economic Loss Doctrine Does Not Apply

When operating in the stranger paradigm, in which no pre-existing legal relationship exists, some courts have invoked an independent duty exception to the ELD in data breach litigation—holding that the defendant owed the plaintiff a duty to reasonably secure their data.[233] For example, in 2019, in *In re Equifax, Inc., Customer Data Security Breach Litigation*, the U.S. District Court for the Northern District of Georgia did not apply the ELD to the tort claims of plaintiffs, financial institutions, who lacked contractual privity with the defendant, Equifax and its affiliates.[234] First, the defendant sought to invoke *Community Bank of Trenton* and thus implicate a third-party problem, hoping to convince the court that the contracting parties paradigm should apply

---

[229] *See id.* at *17 (holding that the plaintiffs sufficiently pleaded that the six-factor test was met and that there existed a special relationship between the two parties that would allow for the plaintiffs to be able to bring tort claims for purely economic damages).

[230] *Id.* at *30.

[231] *Id.*

[232] *Id.*

[233] *See, e.g.*, *In re* Equifax, Inc., Customer Data Sec. Breach Litig., 371 F. Supp. 3d 1150, 1172 (N.D. Ga. 2019) (holding that the ELD would not apply to the plaintiffs' tort claims because defendants had an independent duty to reasonably secure data).

[234] *Id.* (stating that the ELD did not apply due to the existence of an independent duty owed between the two parties). In 2019, in *In re Equifax, Inc., Customer Data Security Breach Litigation*, the U.S. District Court for the Northern District of Georgia noted that the plaintiffs (financial institutions) alleged that the defendants (a credit reporting company and its affiliates) had failed to adequately secure PII that they relied on to value customers' credit scores. *Id.* at 1157. This inability to accurately determine customers' credit worthiness resulted in economic damages. *Id.* The data breach exposed 150 million individuals' PII. *Id.* The plaintiffs alleged that the defendants had been warned of vulnerabilities in their systems but failed to take steps to secure customer data. *Id.*

to limit recovery to the contractual provisions of the PCI-DSS.[235] The court, however, distinguished the case facts from the unique network of contracts created by the PCI-DSS.[236] The *In re Equifax, Inc.* court, citing to *Community Bank of Trenton*, found that in this case, the "sensitive data [was] collected and then disclosed by private, third-party actors who [were] not involved in the customers' or banks' direct transactions."[237] None of the pre-existing legal rights, duties, or remedies presented in *Community Bank of Trenton* existed between the parties in *In re Equifax, Inc.*[238] Accordingly, the court implicitly adopted the stranger paradigm.[239] The court then held that Georgia's ELD included an independent duty exception.[240] Prior cases had established that when an entity aggregates and then stores PPI, that entity has a duty to reasonably safeguard that data.[241] Therefore, the court did not apply the ELD to bar the plaintiffs' tort claims.[242]

3. Third-Party Problem: When There Exists a Web of Contracts in Data Breach Litigation and the Economic Loss Doctrine Does Not Apply

Finally, when confronted with the third-party problem in data breach litigation, some courts have found that the PCI-DSS does not suffice to create the sufficient level of privity that would implicate the contracting parties para-

---

[235] *Id.* at 1183–84 (explaining that the facts underlying defendants' argument resembled typical PCI-DSS third-party problems in which some sort of contract would bar the tort claims of both parties due to the ELD).

[236] *Id.* (elaborating that the plaintiffs did not have the contractual relationship common in most third-party cases).

[237] *Id.* (quoting Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 815 (7th Cir. 2018)). In *In re Equifax, Inc.*, the district court noted that at the core of the reasoning behind the court's ruling in *Community Bank of Trenton v. Schnuck Markets, Inc.* was the fact that the parties were involved in a network of contracts. *Id.* (describing the *Community Bank of Trenton* court's ruling as focused on the existence of a network of contracts); *see also Cmty. Bank of Trenton*, 887 F.3d at 815 (holding that the network of contracts voluntarily entered into by the parties precluded tort liability under the ELD).

[238] *Compare Cmty. Bank of Trenton*, 887 F.3d at 815 (stating that the plaintiffs had legal remedies through the "web of contracts"), *with In re Equifax, Inc.*, 371 F. Supp. 3d at 1183–84 (describing the plaintiffs as having no pre-existing legal remedies available under contract law).

[239] *See In re Equifax, Inc.*, 371 F. Supp. 3d at 1183–84 ("Thus, the Plaintiffs do not have the type of contractual remedies against the Defendants that the plaintiffs did against the retailer in *Schnuck*. Therefore, the Court finds Schnuck inapposite."); *see also* Sharkey, *supra* note 18, at 352 (describing the stranger paradigm as one where the parties have no pre-existing contractual relationship or similar legal relationship).

[240] *See In re Equifax, Inc.*, 371 F. Supp. 3d at 1172–73 (defining Georgia's ELD as containing an independent duty exception).

[241] *See id.* at 1171 ("It is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information . . . ." (quoting Brush v. Mia. Beach Healthcare Grp. Ltd., 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017))).

[242] *Id.* (holding the ELD would not apply). The court denied the defendants' motion to dismiss. *Id.* at 1185.

digm.[243] In these cases, the courts determined that the entanglement of contracts that constitute the PCI-DSS does not foreclose recovery, as a non-contractual independent duty exists between the parties.[244] In doing so, these courts adopted a stranger paradigm and, as a result, generally held that the ELD does not apply to the plaintiff's tort claims. [245]

For example, in 2018, in *In re Arby's Restaurant Group Inc. Litigation*, the U.S. District Court for the Northern District of Georgia allowed the plaintiffs to move forward with their negligence claim against the defendant, due to the independent duty exception.[246] *Arby's* involved two groups of plaintiffs: customers of the defendant's restaurants and issuing banks involved in the PCI-DSS system.[247] The court held that the ELD would bar neither plaintiff classes' negligence claims because no contract governed the rights and duties between the respective parties—an implicit adoption of the stranger paradigm.[248] For the plaintiffs that were issuing banks, the court expressly found no contractual relationship, despite the fact that both parties agreed to adhere to the PCI-DSS.[249] Furthermore, the court found that the only contract that existed between customer plaintiffs and the defendant, Arby's, stemmed out of the purchase of food that "does not address any allocation of risk or relevant contractual obligation or restriction."[250] This duty existed independent of any contractual obligation; therefore, the court held that Georgia's ELD permitted an independent duty exception.[251]

---

[243] *See, e.g.*, *In re* Arby's Rest. Grp. Inc. Litig., C.A. No. 17-cv-0514, 2018 WL 2128441, at *12–14 (N.D. Ga. Mar. 5, 2018) (holding that the ELD did not bar the plaintiffs' tort claims in the third-party problem involving the PCI-DSS).

[244] *See, e.g.*, *id.*; *see also* Sharkey, *supra* note 18, at 371 (describing the misapplication of the stranger paradigm).

[245] *See In re Arby's Rest. Grp.*, 2018 WL 2128441, at *12–14 (holding that the ELD does not bar claims for purely economic damages because no independent duty exception exists within the Northern District of Georgia).

[246] *See id.* (refusing to apply the ELD, and reasoning that the defendant owed the plaintiffs an independent duty to reasonably secure PII). In 2018, *In re Arby's Restaurant Group Inc. Litigation*, the U.S. District Court for the Northern District of Georgia observed that the plaintiffs were both consumers of the defendant's restaurant and issuing banks who had to indemnify customers for the data breach. *Id.* at *1. The defendant was a restaurant chain that operated over 950 facilities nationally. *Id.* Hackers gained access to the defendant's servers for seventy-three days and harvested the credit card information of millions of customers. *Id.* The plaintiffs alleged that the defendant was aware vulnerabilities in their systems but took no steps to secure them. *Id.*

[247] *Id.* at *1.

[248] *See id.* at *12–14 (holding that neither group of plaintiffs were in a contractual relationship with the defendant as to preclude any tort liability).

[249] *Id.* at *13 ("Arby's has pointed to no provision of the Visa and MasterCard Rules that establish a contract between Plaintiffs as issuing banks and Arby's as a merchant or acquirer.").

[250] *Id.* (defining the contractual relationship between the consumer and restaurant as not being broad enough to define data security duties).

[251] *Id.*

III. Rethinking the Economic Loss Doctrine in the Internet Age: Matching Policy with Practice

The ELD has been inconsistently applied in data breach litigation across jurisdictions; this has led to plaintiffs' success depending on which geographic location they suffered the damage in rather than on the merits of their arguments.[252] A consistent, unified approach to the ELD will align and promote the established policy goals of tort and data breach litigation.[253] Part III of this Note argues that the internet economy does not fit squarely under either the contracting parties or stranger paradigms and that plaintiffs whose PII was exposed should be presumed to have a special relationship with the defendant who collected or processed their data, resulting in an exception to the ELD bar.[254] Section A reasons that the traditional policy rationales underlying the ELD do not apply to data breach litigation as internet transactions do not involve private ordering and potential plaintiffs are foreseeable.[255] Section B argues that all data breach litigation should be considered within the contracting parties paradigm, as the transference of PII to a data controller or processor involves a contract.[256] Section C explains why a special relationship test, as opposed to complete ELD bar to tort liability, best matches policy with practice and promotes cybersecurity investment.[257]

A. Policy and Practice: How the Economic Loss Doctrine's Policy Goals Do Not Apply to Data Breach Litigation

Two overarching policy goals spurred the widespread adoption of the ELD: (1) promotion of private ordering and (2) protection from unforeseeable and unlimited liability. [258] Such fears—although highly relevant in the context

---

[252] *Compare* Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 815 (7th Cir. 2018) (applying the contracting parties paradigm, and barring the tort claims of the plaintiffs in data breach litigation surrounding the PCI-DSS), *and* Sovereign Bank v. BJ's Wholesale Club, Inc., 395 F. Supp. 2d 183, 203–04 (M.D. Pa. 2005) (same), *aff'd*, 533 F.3d 162 (3d Cir. 2008), *with In re Arby's Rest. Grp.*, 2018 WL 2128441, at *12–14 (holding that the plaintiffs' tort claims were not barred by the ELD in data breach litigation involving the PCI-DSS). *See generally* Sharkey, *supra* note 18 (describing all the different ways courts apply the ELD in data breach litigation).

[253] *See* Sharkey, *supra* note 43, at 1019–34 (describing the policy goals that underlie the ELD). *See generally* Dobbs, *supra* note 20, at 713–17 (explaining the numerous justifications for the ELD in the contracting parties and stranger paradigms); Fienman, *supra* note 48, at 814 (discussing the ELD and its effects on private ordering).

[254] *See infra* notes 258–330 and accompanying text.

[255] *See infra* notes 258–290 and accompanying text.

[256] *See infra* notes 291–299 and accompanying text.

[257] *See infra* notes 300–330 and accompanying text.

[258] *See* 532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc., 750 N.E.2d 1097, 1103 (N.Y. 2001) (fearing that an extension of liability would unleash a chain of liability to all parties who have suffered small harms); Dobbs, *supra* note 20, at 715 (justifying the stranger and contracting

of a negligent truck driver or construction company—are unfounded in the context of data breach litigation.[259] Data breach litigation currently centers on procedural hurdles, so evolving the ELD doctrine would allow lawsuits to focus on the adequacy of the cybersecurity security standards, promoting meaningful consumer protection.[260]

Firstly, unlike in traditional applications of the ELD, in data breach litigation the defendant data collector or processor can foresee a quantifiable class of potential plaintiffs with vulnerable data.[261] By its very nature, PII can be linked to an individual.[262] The plaintiff is no stranger to the defendant—instead, the plaintiff often is a central part of the business model of the data controller or processor.[263] For instance, social media companies' business models depend on their processing of PII to sell to advertisers for individualized targeted marketing.[264] Social media companies that collect PII do not aggregate PII but rather keep it deliberately hyper-individualized to ensure that their advertiser customers can effectively target specific demographics and individuals.[265] Unlike in product liability litigation, the defendant in data breach litigation

---

parties paradigms); Sharkey, *supra* note 43, at 1022–29 (explaining policy goals in the stranger and contracting parties paradigms).

[259] *See* Dobbs, *supra* note 20, at 713 (illustrating an example of the stranger rule). *Compare In re* Equifax, Inc., Customer Data Sec. Breach Litig., 371 F. Supp. 3d 1150, 1157, 1172 (N.D. Ga. 2019) (stating that the plaintiffs were a quantifiable group of financial institutions who had used the services of the key defendant, a credit reporting company), *with 532 Madison Ave. Gourmet Foods, Inc.*, 750 N.E.2d at 1103 (noting that the class of plaintiffs would be unknowable and stretch beyond human foreseeability).

[260] *See* Operdeck, *supra* note 128, at 981 (noting that the ELD and other procedural aspects result in little to no litigation challenging cybersecurity system reasonableness); Sales, *supra* note 1, at 1535–38 (arguing for civil liability to promote reasonable cybersecurity standards).

[261] *See* IDENTITY THEFT RES. CTR., *supra* note 12, at 2 (showing the prevalence of data breaches in the modern era); Caban, *supra* note 12 (describing how common data breaches are in the healthcare industry); Wagner, *supra* note 7 (explaining how companies use PII to specifically create advertisement profiles for particular users and how they keep that data on a quantifiable group of individuals).

[262] *See* Memorandum from Meglio III, Deputy Dir. for Mgmt., Off. of Mgmt. & Budget on Safeguarding Against and Responding to the Breach of Personally Identifiable Information to the Heads of Executive Departments and Agencies, *supra* note 4, at 1 n.1 (explaining that PII is data that can be linked to a specific individual).

[263] *See* Short & Todd, *supra* note 10, at 17 (explaining how PII has been considered one of the most valuable assets for companies undergoing sales, mergers, or bankruptcies); Brynjolfsson & McAfee, *supra* note 5 (describing how companies have incorporated the use of data into their business models); Wagner, *supra* note 7 (explaining how social media websites rely on the aggregation of PII to sell to advertisers).

[264] *See* Wagner, *supra* note 7 (describing the business model of social media companies).

[265] *See id.* (explaining generally the business model of social media companies); *see also A Deep Dive into Facebook Ads: How to Create, Optimize, and Test Facebook Ads*, NEIL PATEL, https://neilpatel.com/blog/deep-dive-facebook-advertising/ [https://perma.cc/FL2G-55YW]. Facebook gives advertisers exceptionally powerful tools to target certain demographics. *A Deep Dive into Facebook Ads: How to Create, Optimize, and Test Facebook Ads*, *supra*. An advertiser can target specific age groups, locations, genders, interests, connections, relationship statuses, languages, educations, and even workplaces. *Id.* This precision targeting increases an advertisement's effectiveness. *Id.*

does not open a Pandora's box of unlimited liability because only a quantifiable and identifiable class of plaintiffs will be subject to their alleged negligence.[266] Further, a data controller or processor can foresee the likelihood of the harm occurring from a breach.[267] The growing frequency of data breaches removes the unpredictability of the harm.[268] In a traditional tort setting, such as in the 2001 case *532 Madison Avenue Gourmet Foods, Inc. v. Finlandia Center, Inc.*, it stretched the boundaries of foreseeability for a construction company to be able to predict that, as a result of their negligent actions, a local deli would see decreased foot traffic.[269] In data breach litigation, however, companies are not only aware of the specific risk but actively take steps to prevent it.[270] By simply requiring passwords, a company acknowledges that there are actors who seek to breach their systems; furthermore, investments in cybersecurity can immediately and effectively mitigate these risks.[271]

Lastly, the ELD attempts to promote and respect contracts between private parties.[272] Generally, private ordering posits that it is most economically efficient for private parties to allocate risks and duties through a contract; therefore, any imposition of additional tort liability would be unnecessary and inefficient.[273] This theory simply does not hold up in most data breach litigation cases, as the fundamental assumption of private ordering is that parties negotiate for an ac-

---

[266] *See, e.g.*, *In re* Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 475–76 (D. Md. 2020) (distinguishing product liability litigation from the facts typically surrounding data breach litigation).

[267] *See In re* Equifax, Inc., Customer Data Sec. Breach Litig., 371 F. Supp. 3d 1150, 1172 (N.D. Ga. 2019) (declaring that the risk of a data breach is foreseeable to a data controller or processor); IDENTITY THEFT RES. CTR., *supra* note 12, at 2 (describing the prevalence of data breaches across industries); Caban, *supra* note 12 (noting the increase in data breaches in the healthcare industry).

[268] *See* IDENTITY THEFT RES. CTR., *supra* note 12, at 2 (discussing the rise in data breaches); Caban, *supra* note 12 (discussing the prevalence and frequency of data breaches in the healthcare industry).

[269] 532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc., 750 N.E.2d 1097, 1103 (N.Y. 2001) (arguing that the type of damage suffered and the plaintiffs would be unforeseeable to the defendant).

[270] *See, e.g.*, NASDAQ, *supra* note 126, at 5 (describing cybersecurity investment and the steps that companies have taken to prevent data breaches).

[271] *See* BISSELL ET AL., *supra* note 126, at 16–18 (noting how higher investments in cybersecurity correlate with a decreased threat of a breach); CyberAvengers, *Why Computer Passwords Are Still a Problem in 2019*, NEXTGOV (Jan. 11, 2019), https://www.nextgov.com/cybersecurity/2019/01/why-computer-passwords-are-still-problem-2019/154086/ [https://perma.cc/JRY2-PGTY] (noting that passwords are the foundation of most cybersecurity systems).

[272] Johnson, *supra* note 40, at 546–47 (describing the ELD as an attempt to promote private ordering); Sharkey, *supra* note 43, at 1033 (relaying the policy goals of the ELD in the contracting parties paradigm).

[273] Johnson, *supra* note 40, at 546–47 (arguing that ELD seeks to promote private ordering and parties allocating risk and rights through contract); Sharkey, *supra* note 43, at 1033 (explaining the policy goals of encouraging contracts).

ceptable contract, which is not applicable in this context.[274] Many of the contractual relationships that are common in data breach litigation involve "take it or leave it"[275] contracts.[276] A take-it-or-leave-it contract has standardized language and is offered as-is to all consumers as part of the terms of using a service.[277] Realistically, the individual does not possess the bargaining power to impose their interests effectively against data controllers or processors.[278] Collective action would be the only viable route for consumers to negotiate effectively; however, that is inefficient because the size of the class of individuals involved in the market would impose momentous transaction costs to doing business.[279] Further, it is fundamentally unrealistic to expect hundreds of millions of individuals to organize on the scale needed to effectively negotiate.[280] The ubiquity of

[274] *See* Vincent R. Johnson, *Credit-Monitoring Damages in Cybersecurity Tort Litigation*, 19 GEO. MASON L. REV. 113, 123–24 (2011) ("Consequently, the duties at issue in cybersecurity cases are, in large measure, not a proper subject for private ordering."). Data breach plaintiffs often pursue damages to recoup the cost of credit monitoring. *Id.* Many state statutes preclude the ability to waive rights related to PII. *Id.* at 123 n.60. In turn, this inhibits individuals' ability of the to engage in bargaining for a contract effectively. *Id.*

[275] *What Is a Take It or Leave It Contract?*, UPCOUNSEL, https://www.upcounsel.com/take-it-or-leave-it-contract [https://perma.cc/Q8CJ-TZF7]. Sometimes called a contract of adhesion, a take-it-or-leave-it contract is one that does not allow the customer to bargain for the terms. *Id.*

[276] *See In re* Marriott Int'l, Inc., Costumer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 453–55 (D. Md. 2020) (conditioning customers' ability to buy hotel rooms on assent to the terms of service regarding usage of their data); Portier v. NEO Tech. Sols., No. 17-cv-30111, 2019 WL 7946103, *17–22 (D. Mass. Dec. 31, 2019) (conditioning employment on turning over PII); *In re* Sony Gaming Networks & Consumer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 945 (S.D. Cal. 2014) (conditioning users' access to a gaming network on turning over PII).

[277] *See generally* MAYA WILEY ET AL., THE NEW SCH., TAKE IT OR LEAVE IT: HOW NYC RESIDENTS ARE FORCED TO SACRIFICE ONLINE PRIVACY FOR INTERNET SERVICES (2018), http://bmgxb.site/digital-equity-lab/take-it-or-leave-it.pdf [https://perma.cc/65H3-F6FJ] (describing how residents in NYC are given take-it-or-leave-it contracts with internet service providers, and identifying the associated privacy risks). For example, when an individual consumer approaches an Internet Service Provider to sign up, they are presented with a generic non-negotiable contract that mandates that, in exchange for internet access, the customer will provide consideration in the form of money and their own PII, arguably the latter being more valuable than the former. *See generally id.* (describing take-it-or-leave-it contracts in New York City's internet service industry).

[278] *See, e.g.*, Sales, *supra* note 1, at 1536–37 (arguing that most contracts in the digital sectors of the economy are forced upon consumers, and that bargaining would be nearly impossible due to the sheer number of people involved and the misalignment of all their incentives).

[279] *See* Johnson, *supra* note 274, at 123 n.60 ("Moreover, it is simply unrealistic to expect that bargaining to occur between individual consumers and the large corporations that play a pervasive role in modem life." (quoting Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 300 (2005))); Sales, *supra* note 1, at 1520 ("It would be prohibitively expensive, if not impossible, for companies to bargain with everyone who conceivably could be injured by cyber-attacks on their systems or products.").

[280] *See* Sales, *supra* note 1, at 1520 (illustrating the barriers to collective bargaining in contracts involving cybersecurity).

data collection would extrapolate the transaction costs of bargaining for cybersecurity across industries.[281]

More generally, policy considerations surrounding data breach litigation should encourage the removal of procedural hurdles.[282] Private civil liability has the potential to promote both reasonable cybersecurity systems and adequate cybersecurity investments.[283] Costly litigation over the application of the ELD, however, disincentivizes or bars parties from fully litigating the facts regarding the adequacy of cybersecurity systems; instead, it promotes settlement.[284] Litigation over what reasonable cybersecurity systems entail could spur effective private regulation in the absence of government action.[285] Additionally, imposing liability on negligent data controllers and processors would be socially optimal because it would promote investment in cybersecurity and attach liability to the least cost avoider, further promoting cybersecurity investment.[286] The data controller or processer is the party most able to prevent a PII data breach; therefore, they should be most liable when one occurs.[287] This is in juxtaposition to the current approach that imposes greater liability on passive parties in the system.[288] Consider the Home Depot data breach: greater

---

[281] *See* IDENTITY THEFT RES. CTR., *supra* note 12, at 2 (exploring data breaches across industries showing how many sectors of the economy collect PII); Sales, *supra* note 1, at 1520 (arguing that transaction costs are high to bargain for cybersecurity measures); Caban, *supra* note 12 (showing the amount of PII collected in the healthcare industry). Importantly, there are seven social media websites with over 250 million users. Priit Kallas, *Top 15 Most Popular Social Networking Sites and Apps [2021]*, DREAMGROW, https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/ [https://perma.cc/L3QY-AKSS] (Jan. 4, 2021). The costs of bargaining for cybersecurity standards or rights and remedies for data breaches would be impossibly high. Sales, *supra* note 1, at 1520 (arguing that the size of the classes involved raise transaction costs to an extremely high measure).

[282] *See* Sales, *supra* note 1, at 1535–38 (advocating for civil liability); Dean, *supra* note 126 (arguing that liability removes negative externalities in the market).

[283] *See* Sales, *supra* note 1, at 1535–38 (noting that liability would encourage investment in cybersecurity); Vagle, *supra* note 124, at 86 (same); Dean, *supra* note 126 (same).

[284] *See* Paula Hannaford-Agor, *Measuring the Cost of Civil Litigation: Findings from a Survey of Trial Lawyers*, VOIR DIRE, Spring 2013, at 22, 23 (noting that procedural hurdles drive up the costs of litigation); Inglis et al., *supra* note 158, at 91 (observing that increased court costs directly correlate with settlements).

[285] *See* Stephen Shavell, *Liability for Harm Versus Regulation of Safety*, 13 J. LEGAL STUD. 357, 358–64 (1984) (describing that liability can amount to private regulation). *See generally* Alan Charles Raul et al., *United States*, *in* THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 399–422 (Alan Charles Raul ed., 6th ed. 2019) (detailing the dearth of government regulation of cybersecurity).

[286] *See, e.g.*, BISSELL ET AL., *supra* note 126, at 16–18 (illustrating that investment and focus in cybersecurity does pay off); Sharkey, *supra* note 43, at 1033 (describing why attachment of liability to the cheapest cost avoider is advantageous); Paul Rosenzweig, *Cybersecurity and the Least Cost Avoider*, LAWFARE BLOG (Nov. 5, 2013), https://www.lawfareblog.com/cybersecurity-and-least-cost-avoider [https://perma.cc/9JQT-GBGW] (describing generally that data controllers and processors are in the best position to secure their systems from hackers).

[287] *See* Rosenzweig, *supra* note 286 (noting that data controllers and processors can most easily secure data storage systems and are also the least cost avoiders).

[288] *See id.* (noting that liability generally has not fallen on the least cost avoider).

liability fell onto federal credit unions because they were tasked with reissuing credit cards and indemnifying fraudulent transactions, as compared to Home Depot which stored and collected the underlying exposed PII.[289] Imposition of liability on data controllers or processors would create incentives to adequately secure PII and increase the potential return on their investment.[290]

B. Dismantling the Paradigm in Data Breach Litigation: There Are No Strangers Here

Courts' inconsistent adoption of ELD paradigms, as opposed to a uniform application, stems from the novelty of the relationship between the individual data sources and the parties collecting and storing data in data breach litigation.[291] The relinquishment of PII by data subjects is almost always a function of a transaction between two parties.[292] At some point, a data controller or processor has direct contractual privity with the individual whose PII is now the subject of litigation.[293] As one court put it, the parties are not "ships passing . . . in the night."[294] Courts that have adopted the stranger paradigm in data breach litigation are often trying to fit incompatible realties in a doctrinal box, as the nature of the internet economy means that there are no perfect strangers in data breach litigation.[295] Although the degree of separation may render the parties effectively strangers, an entanglement of contracts still exists.[296] Instead

---

[289] *See* Dean, *supra* note 126 (describing the fallout from the Home Depot data breach and identifying the parties that had the greatest financial burden).

[290] *See* Sales, *supra* note 1, at 1535–38 (noting that liability would increase investment in cybersecurity); Vagle, *supra* note 124, at 86 (explaining that liability encourages investment); Blau, *supra* note 129 (explaining that the return on investment in cybersecurity is often low for corporate executives); Dean, *supra* note 126 (arguing that liability defeats the moral hazard).

[291] *See* Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 807 (7th Cir. 2018) (explaining the network of contracts involved in the PCI-DSS); Silverpop Sys., Inc. v. Leading Mkt. Techs., Inc., 641 F. App'x 849, 851 (11th Cir. 2016) (per curiam) (elaborating on cybersecurity contracts); Sharkey, *supra* note 18, at 366–67 (noting that the relationship of parties in data breach litigation has resulted in diverging choices of paradigms); Meglio, *supra* note 17, at 1242 (describing how some states have laws that require data processors to clearly disclose privacy policies to consumers).

[292] *See* Meglio, *supra* note 17, at 1241 (explaining that contracts generally govern the relationship between data subjects and data controllers or processors).

[293] *See, e.g.*, *In re* Arby's Rest. Grp. Inc. Litig., C.A. No. 17-cv-0514, 2018 WL 2128441, at *12–14 (N.D. Ga. Mar. 5, 2018) (exploring how the PII exposed belonged to consumers who were in direct contractual privity with the defendant).

[294] *See Cmty. Bank of Trenton*, 887 F.3d at 815 (distinguishing the relationship between parties in data breach litigation from conventional applications of torts); Sharkey, *supra* note 18, at 365–67 (explaining that when a "web of contracts" exists, the contracting parties paradigm should apply); Meglio, *supra* note 17, at 1241 (noting that private contracts typically govern PII storage and collection).

[295] *See* Sharkey, *supra* note 18, at 366–78 (arguing that courts are often misapplying the stranger paradigm when clearly the contracting parties paradigm has been implemented).

[296] *See, e.g.*, *In re* Equifax, Inc., Customer Data Sec. Breach Litig., 371 F. Supp. 3d 1150, 1172 (N.D. Ga. 2019) (holding there was not the contractual web implicated by the PCI-DSS). In 2019, in

of an ad-hoc approach, where courts must determine the significance of the parties' separation, all data breach litigation should be presumed to fall under the contracting parties paradigm.[297] This approach addresses the inconsistency of ELD application, expediates courts' analysis, and reflects the facts of the internet economy.[298] Accordingly, the special relationship test should be the only determinative factor as to whether the ELD applies to data breach lawsuits.[299]

C. The Special Relationship Test: How It Should Be Applied in Data Breach Litigation

In data breach litigation, the special relationship test, taken together with the policy goals of the ELD, should create a presumption that the ELD does not apply.[300] When an individual gives over their PII, a contract typically exists with the data controller of processor that will govern the storage and collection of that PII.[301] On the one hand, a per se non-application of the ELD in data breach litigation would dissolve the line between tort and contract and parties, no matter how sophisticated, would be discouraged from contracting with another.[302] On the other hand, a flat bar would prejudice plaintiffs who cannot engage in private ordering and are bound by a take-it-or-leave-it contract.[303] By adopting a presumption against ELD application, both of these valid com-

---

In re Equifax, Inc., Customer Data Security Breach Litigation, the U.S. District Court for the Northern District of Georgia adopted the stranger paradigm due to the separation between the plaintiffs and the defendants; however, in reality all parties were bound in a network of contracts. *See id.*; BD. OF GOVERNORS OF THE FED. RSRV. SYS., CONSUMER'S GUIDE: CREDIT REPORTS AND CREDIT SCORES 1211, https://www.federalreserve.gov/creditreports/pdf/credit_reports_scores_2.pdf [https://perma.cc/VKA5-EEL9] (noting that credit reporting agencies collect PII from banks and lenders).

[297] *See* Sharkey, *supra* note 18, at 366–67 (describing the contracting parties paradigm as one where a contract governs relationships); Meglio, *supra* note 17, at 1241 (stating that contracts generally govern relationships between data subjects and controllers).

[298] *See Cmty. Bank of Trenton*, 887 F.3d at 813–15 (discussing at great length which paradigm to adopt); Sharkey, *supra* note 18, at 366–78 (explaining how often courts have to decide which paradigm to choose).

[299] *See* Portier v. NEO Tech. Sols., No. 17-cv-30111, 2019 WL 7946103, at *17–22 (D. Mass. Dec. 31, 2019) (applying the special relationship test within the contracting parties paradigm); Sharkey, *supra* note 18, at 374 (noting how some courts apply a special relationship exception in the contracting parties paradigm).

[300] *See* Sales, *supra* note 1, at 1535–38 (explaining that liability encourages investment); Vagle, *supra* note 124, at 86 (advocating for civil liability); Meglio, *supra* note 17, at 1236 (noting the lack of litigation over reasonableness); Dean, *supra* note 126 (arguing for liability).

[301] *See* Meglio, *supra* note 17, at 1241 (explain how contracts govern relationships between data subjects and data controllers).

[302] *See* Johnson, *supra* note 40, at 551–52 (discussing the "boundary-line" between tort and contract law).

[303] *See id.* (describing the ELD as upholding the border between tort and contract, and encouraging bargaining through the restriction of tort liability); Sales, *supra* note 1, at 1520 (describing the issues with private ordering in cybersecurity).

peting considerations are met: the ELD will still apply to bargained-for contracts, protecting private ordering, while simultaneously consumer plaintiffs will be able to pursue tort liability related to take-it-or-leave-it contracts.[304]

Although there are many incarnations of the special relationship test, in 1979, in *J'Aire Corp. v. Gregory*, the Supreme Court of California established a six-factor test that best balances the competing goals of respecting contracts and simultaneously acknowledging the inherent imbalance of economic power between parties in most data breach litigation.[305] The fifth and six *J'Aire* factors consider the general policy goals surrounding contract law and the specific policy concerns in the internet age, including private ordering, moral hazards, and the least cost avoider.[306] The first three factors of the *J'Aire* test aim to further the policy goals of preventing unlimited and unforeseeable liability.[307] When taken together, all six of the *J'Aire* factors allow courts to consider the ELD's general policy goals, policy goals specific to the contracting parties paradigm, and to data breach litigation.[308]

Furthermore, where defendants have an independent duty of care to reasonably secure data, courts should presume that the test is satisfied.[309] In 2018, in *Dittman v. UPMC*, the Supreme Court of Pennsylvania articulated that when a data controller or processor undertakes efforts to gather data, that effort equates to an affirmative obligation.[310] Under tort law, when an individual undertakes an affirmative obligation—such as saving a car crash victim—there

---

[304] *See* Johnson, *supra* note 40, at 551 (noting that the ELD should apply to maintain boundary and promote contracting); Sales, *supra* note 1, at 1520 (arguing for liability to encourage investment in cybersecurity and remedy market inefficiency).

[305] *See, e.g.*, 598 P.2d 60, 63 (Cal. 1979) (detailing a six-factor test that balances causation and damages with public policy goals of imposing liability and emphasizing the moral blame of the conduct).

[306] *See* Johnson, *supra* note 40, at 546–47 (explaining that the ELD promotes private ordering); Sharkey, *supra* note 43, at 1033 (describing the policy goals in the contracting parties paradigm).

[307] *See* Dobbs, *supra* note 20, at 715 (relaying policy goals of the stranger paradigm); Sharkey, *supra* note 43, at 1022–29 (describing the policy goals of the stranger paradigm).

[308] *See J'Aire Corp.*, 598 P.2d at 63 (including foreseeability into the six-factor test); 532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc., 750 N.E.2d 1097, 1103 (N.Y. 2001) (arguing that the ELD fends off unforeseeable damages); Dobbs, *supra* note 20, at 715 (describing the ELD protecting against unforeseeable damages). An inclusion of these factors prompts a court to consider more general ELD policy goals outside of the contracting parties paradigm's specific policy goals. *See J'Aire Corp.*, 598 P.2d at 63 (considering other factors); *532 Madison Ave. Gourmet Foods, Inc.*, 750 N.E.2d at 1103 (discussing the general policy goals); Dobbs, *supra* note 20, at 715 (explaining the broader policy goals).

[309] *See In re* Equifax, Inc., Customer Data Sec. Breach Litig., 371 F. Supp. 3d 1150, 1172 (N.D. Ga. 2019) (holding that there exists an independent duty to reasonably secure data); Dittman v. UPMC, 196 A.3d 1036, 1040 (Pa. 2018) (same).

[310] *See* 196 A.3d at 1041 (stating that the defendant had taken affirmative steps by collecting the data which under conventional tort law would amount to the creation of a legal duty owed between the parties).

then arises a duty from that action.[311] By taking on an affirmative obligation in storing the data, the data controller or processor takes on the risk of future harm.[312] Through this basic principle of tort law, when a data controller or processor voluntarily aggregates data, thus creating the risk of a data breach, they then owe the individual whose PII they collected a duty to reasonably secure that data.[313] This is further supported by the foreseeability of data breach risks and the reality that accessible precautions can be taken to reduce those risks.[314] Due to the prevalence of data breaches, data controllers and processors can reasonably foresee the risk of hacks, making it is fair to expect them to take steps to reduce that risk.[315] For instance, in 2019, *In re Equifax, Inc., Customer Data Security Breach Litigation*, the U.S. District Court for the Northern District of Georgia explained that the defendants were cognizant of the risk of a data breach and could have taken preventive measures to mitigate that risk.[316] The original contract may supplant this established duty of care through the standards set in its provisions; however, a presumption that the plaintiffs have

[311] *See id.* (comparing the defendant's actions of collecting the data to tort doctrines that will impose a duty of care for individuals who take affirmative acts).

[312] *See id.* (noting that the act of collecting the data created the risk of a data breach in the first place and furthermore created a duty to reasonable protect that data).

[313] *See id.* (noting that a party that voluntarily stores data takes on an affirmative obligation).

[314] *See In re Equifax, Inc.*, 371 F. Supp. 3d at 1172 (stating that the defendants should have been aware that a data breach was a foreseeable occurrence); *see also* Hapka v. Carecentrix, Inc., No. 16-cv-02372, 2016 WL 7336407, at *5 (D. Kan. Dec. 19, 2016) (stating that when a risk is foreseeable, the defendants have a duty to reasonably protect against that harm).

[315] *See In re Equifax, Inc.*, 371 F. Supp. 3d at 1172 (stating data controllers and processors can foresee breach risks); Fisher, *supra* note 17, at 230–31 (reasoning that defendants' knowledge and capacity to defend against a type of attack should result in a duty to take reasonable steps to prevent that type of data breach from occurring). A full exploration of the reasonableness of the data security is beyond the scope of this Note. *See* Fisher, *supra* note 17, at 230–34 (defining the standard). *See generally* JIM HARVEY ET AL., ALSTON & BIRD, THE CCPA COULD RESET DATA BREACH LITIGATION RISKS (2019), https://www.alston.com/-/media/files/insights/publications/2019/08/the-ccpa-could-reset-data-breach-litigation-risks.pdf [https://perma.cc/RTC5-AWHP] (describing how California and Illinois define reasonableness). Generally, however, the "risk/utility" approach establishes exceptions. Rick Lazio, Opinion, *Cybersecurity Risk: What Does a 'Reasonable' Posture Entail and Who Says So?*, CIO DIVE (July 22, 2019), https://www.ciodive.com/news/cybersecurity-risk-what-does-a-reasonable-posture-entail-and-who-says-so/559207/ [https://perma.cc/8RLH-FQL3]. The approach balances the costs of implementing cybersecurity measures against the harm caused if the data were exposed. *Id.* Under this approach, the reasonableness standard would be more fact specific, setting different standards for an entity storing solely email addresses from an entity storing social security numbers. *Id.*

[316] *See* 371 F. Supp. 3d at 1172 (stating that when a risk is foreseeable and steps can be taken to prevent such a risk, then the defendant should be liable for a breach of duty if they fail to take such steps); *see also* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1557–59 (2005) (arguing that data controllers and processors owe plaintiffs a duty of care for foreseeable cybersecurity intrusions). Some scholars have argued for a whole new negligence tort dubbed "negligent enablement of cybercrimes." *See* Rustad & Koenig, *supra*, at 1557–59.

satisfied the special relationship test reflects the reality of this affirmative obligation duty.[317]

In determining whether a special relationship does apply, the *J'Aire* test, particularly its moral blame and deterrence factors, gives considerable weight to the type of contract at issue.[318] Data breach litigation typically involves two types of contracts: a take-it-or-leave-it contract, as seen in the 2020 case *In re Marriott International, Inc., Costumer Data Security Breach Litigation* and the 2019 case *Portier v. NEO Technology Solutions*, or a bargained-for contract, as seen in the 2016 case *Silverpop Systems, Inc. v. Leading Market Technologies, Inc.*[319] When the parties bargain for a contract, the fifth and sixth factors should not be satisfied, and thus the ELD should bar claims beyond the scope of contractual rights and duties.[320] If the contract is take-it-or-leave-it, however, under most circumstances a special relationship exception should apply.[321] Imposition of civil liability will promote adequate cybersecurity standards and combat the negative externalities inherent in the internet economy.[322] Additionally, because the defendant has a common law duty to reasonably secure personal data, the *J'Aire* test should place significant weight on the moral blame attached to their conduct.[323]

---

[317] *See* Silverpop Sys., Inc. v. Leading Mkt. Techs., Inc., 641 F. App'x 849, 850–51 (11th Cir. 2016) (per curiam) (holding that there does exist an independent duty, but noting that the contract's enumeration of data security standards supplanted that duty).

[318] *See, e.g.*, *In re* Sony Gaming Networks & Consumer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 945 (S.D. Cal. 2014) (discussing moral blame and policy goals in reference to the type of contract between the parties); Sales, *supra* note 1, at 1520 (noting that in traditional cybersecurity, the lack of liability encourages less cybersecurity and more future harm); Dean, *supra* note 126 (arguing for the policy goal of increasing liability where a moral hazard exists because the third-party cannot bargain for the contract).

[319] *Compare Silverpop Sys., Inc.*, 641 F. App'x at 850–51 (noting that the case involved two entities entering a business relationship with bargained-for rights and remedies), *with In re* Marriott Int'l, Inc., Costumer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 475–76 (D. Md. 2020) (requiring consumers to agree to the contract in order to purchase a hotel room or other hotel services), *and* Portier v. NEO Tech. Sols., No. 17-cv-30111, 2019 WL 7946103, at *17–22 (D. Mass. Dec. 31, 2019) (mandating that employees turn over PII for employment).

[320] *Silverpop Sys., Inc.*, 641 F. App'x at 850–51 (holding that the ELD applied because the parties had bargained for their rights and remedies, and therefore their contract supplied any duties).

[321] *See Portier*, 2019 WL 7946103, at *17–22 (mandating employees turn over PII to gain employment); *see also In re Sony Gaming Networks*, 996 F. Supp. 2d at 945. In 2014, in *In re Sony Gaming Networks & Consumer Data Security Breach Litigation*, the U.S. District Court for the Southern District of California concluded that the policy prong of the *J'Aire* test had been met; however, due to the abstract nature of the plaintiffs' damage, the court concluded that the special relationship test had failed. 996 F. Supp. 2d at 945.

[322] *See* Operdeck, *supra* note 128, at 959 (arguing for civil liability in data breach litigation to promote cybersecurity investment); Sales, *supra* note 1, at 1535–38 (same); Vagle, *supra* note 124, at 86 (same); Dean, *supra* note 126 (same).

[323] *See Portier*, 2019 WL 7946103, at *17–22 (applying the test where there was a take-it-or-leave-it contract to allow plaintiffs to proceed with tort claims).

The PCI-DSS system occupies a grey area between take-it-or-leave-it contracts and bargained-for contracts.[324] Entry into the credit card payment network is contingent on adherence to the terms set by the PCI-DSS.[325] The parties within the network, however, have negotiated and planned business decisions around the contractual damages, duties, and remedies that they agreed to within the PCI-DSS.[326] The PCI-DSS enumeration of cybersecurity standards supplants the defendant's independent duty of care to reasonably secure the data.[327] Institutional and corporate plaintiffs do knowingly enter the web of contracts; therefore, generally the ELD should apply to data breach litigation involving the PCI-DSS.[328] Imposition of liability would shock the PCI-DSS system and upset settled expectations that underlie significant business decisions, despite the take-it-or-leave-it nature of the system at large.[329] Consumer plaintiffs' only interaction with the system is retail purchases; thus, they should not have the ELD applied to their data breach litigation claims.[330]

CONCLUSION

Courts developed the Economic Loss Doctrine (ELD) upon venerable ideals; however, its principles are ill-suited to the modern economy. The ELD sought to promote the well-meaning policy goals of foreseeability and private ordering. Since its incarnation in the law, the ELD has remained a cornerstone

---

[324] *See* Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 815 (7th Cir. 2018) (noting that the PCI-DSS is an allocation of rights and duties between private parties); PCI SEC. STANDARDS COUNCIL, *supra* note 140, at 5 (describing that all parties in the credit card payment network are subject to the PCI-DSS).

[325] *See* PCI SEC. STANDARDS COUNCIL, *supra* note 140, at 5 (noting that accessing the credit card payment network requires PCI-DSS compliance).

[326] *See Cmty. Bank of Trenton,* 887 F.3d at 815 (holding that because the defendant already has to bear the cost of data security under the PCI-DSS reimbursement provisions, imposing greater liability would not further policy goals); S. Indep. Bank v. Fred's, Inc., No. 15-CV-00799, 2019 WL 1179396, at * 2–4 (M.D. Ala. Mar. 13, 2019) (overviewing the PCI-DSS as an arrangement of risks, rights, and remedies); PCI SEC. STANDARDS COUNCIL, *supra* note 140, at 5 (stating the terms that all parties voluntarily agree to); Sales, *supra* note 1, at 1536 (stating that transactions costs are already incredibly high in the cybersecurity industry).

[327] *See, e.g.*, Silverpop Sys., Inc. v. Leading Mkt. Techs., Inc., 641 F. App'x 849, 850–51 (11th Cir. 2016) (per curiam) (holding that when a contract defines the duties owed between two parties, the contract will govern the duties owed, with no available no independent duty exception, which means parties must exclusively seek contract law remedies).

[328] *See, e.g.*, *Cmty. Bank of Trenton*, 887 F.3d at 815 (stating the entrance into the system is knowingly); PCI SEC. STANDARDS COUNCIL, *supra* note 140, at 5 (illustrating that the PCI-DSS applies to all parties who use credit card payment networks); Wills, *supra* note 142 (noting that the PCI-DSS applies to all parties through contracts).

[329] *See* Johnson, *supra* note 40, at 547–48 (arguing that the ELD serves to encourage bargaining so companies can best plan their business decisions and do not incur unexcepted liability).

[330] *See, e.g.*, *In re* Arby's Rest. Grp. Inc. Litig., C.A. No. 17-cv-0514, 2018 WL 2128441, at *12–14 (N.D. Ga. Mar. 5, 2018) (holding that the ELD should not apply to consumers' tort claims because the contract that they entered into was one relating to the purchase of goods, not the storage of data).

of tort law. The very same policy that inspired the ELD now dictates that it should have a diminished impact in data breach litigation. Plaintiffs and courts should no longer struggle with how and when to apply the ELD to tort claims for victims in data breach litigation. The adoption of the special relationship test will provide consistency in application and promote the litigation of the merit of the cases. Hopefully, the removal of procedural barriers will result in data breach litigation going to trial. This in turn will provide clarity to data controllers and processors as to what constitutes a reasonable cybersecurity system and will create liability for failure to reach the standard. These factors should result in fewer data breaches, fewer victims, and more security for personal identifiable information.

NICOLAS N. LABRANCHE