Paul M. Vaaler* and Brad Greenwood

Do US State Breach Notification Laws Decrease Firm Data Breaches?

https://doi.org/10.1515/rle-2023-0038
Received May 1, 2023; accepted September 6, 2023; published online November 28, 2023

Abstract: From 2003 to 2018, all 50 states and the District of Columbia enacted breach notification laws (BNLs) mandating that firms suffering data breaches provide timely notification to affected persons and others about breach incidents and mitigation responses. BNLs were supposed to decrease data breaches and develop a market for data privacy where firms could strike their preferred balance between data security quality and cost. We find no systemic evidence for either supposition. Results from two-way difference-in-difference analyses indicate no decrease in data breach incident counts or magnitudes after BNLs are enacted. Results also indicate no longer-term decrease in data misuse after breaches. These non-effects appear to be precisely estimated nulls that persist for different firms, time-periods, data-breach types, and BNL types. Apparently inconsistent notification standards and inadequate information dissemination to the public may explain BNL ineffectiveness. An alternative federal regime may address these shortcomings and let a national BNL achieve goals state BNLs have apparently failed to meet.

Keywords: data security; breach notification laws; consumer privacy; difference in differences

JEL Classification: C23; M15; M48; M21; K2

1 Introduction

Consumer data breaches have become regular occurrences affecting some of the largest US firms. October 2013 saw 153 million consumer records exposed in a hack at the software publisher Adobe (Guardian 2013); October 2016 saw 412 million

***Corresponding author: Paul M. Vaaler**, Law School and Carlson School of Management, University of Minnesota Twin Cities, Mondale Hall, Room 412, 229 19th Avenue South, Minneapolis, MN, USA, E-mail: vaal0001@umn.edu. https://orcid.org/0000-0002-3566-6764
Brad Greenwood, School of Business, George Mason University, Fairfax, VA, USA

user accounts compromised at the online dating firm Adult Friend Finder (Computer World 2016); September 2017 saw the financial information of 147 million people exposed by a data breach at the credit assessment giant Equifax (Equifax 2019); and April 2021 saw personal information for 533 million Facebook users stolen (ITech 2021). Data breaches draw fines and enforcement actions from different regulators such as the US Federal Trade Commission (FTC), but the received wisdom from the legal community is that these penalties are insufficient to prompt firms to devote more time and money to assure greater data protection and consumer privacy (Winn 2009). If true, then the conventional understanding is troubling. As Becker (1968) noted more than 50 years ago, insufficient incentives for firms to desist from profitable activities that impose costs on society mean the activities will continue.

For their part, state legislatures in the US have sought to address data breaches by passing breach notification laws (BNLs) (Solove and Schwartz 2019). California passed the first BNL in 2003. As Table 1 shows, the next 15 years saw the other 49 states and the District of Columbia follow California's lead. As Kosseff (2017) and others (*e.g.*, Chesney 2021) have noted, these 51 BNLs vary on different coverage dimensions such as how data breaches are defined, when data breach notification requirements for firms are triggered, which individuals and organizations the firms must then notify, what liabilities firms then have, and what rights and remedies different individuals have in the wake of a data breach and notification.

But no matter how BNLs differ, they share a basic intuition. By compelling timely data breach disclosures, BNLs would identify and inform consumers, law enforcement officials, and other community members about compromised firms. Consumers and others harmed or potentially harmed by breaches could then take timely protective action by, for instance, purchasing credit monitoring services to look out for fraudulent charges. They and their representatives could use firm disclosures to investigate breach incidents more quickly and hold negligent firms accountable sooner through, for instance, individual and class action lawsuits for damages and injunctive relief. Firm disclosures could also let them "vote with their feet" by taking business to other firms investing more in data security.

By compelling timely notification and imposing costs for untimely notification, BNLs could deter firm data breaches in the near term. Over time, BNLs could also foster development of a "market" for data privacy, where consumers could learn which firms are better and worse as data stewards. Firms could then position themselves in that market based on their own cost-benefit analysis of data breach likelihoods and prevention. Through these processes, BNLs could curb data breach numbers and permit firms to strike their own balance between data security quality and cost. BNLs could let state lawmakers meet Becker's (1968) challenge of using regulation to set standards and provide information so that individuals could

Table 1: Summary information on state BNLs.

State	Citation	Year	Trigger for notification	No harm exception	Individual notification	Owner notification	AG notification	Private right of action
Alabama	Ala. Code § 8-38-1 et seq.	2018	Acquisition	No harm	Yes	Yes	Yes	
Alaska	Alaska Stat. § 45.48.010 et seq.	2009	Acquisition	No harm	Yes	Yes	Yes	Yes
Arizona	Ariz. Rev. Stat. § 18-551 to -552	2006	Risk of misuse	No harm	Yes	Yes		
Arkansas	Ark. Code §§ 4-110-101 et seq.	2005	Acquisition	No harm	Yes	Yes		
California	Cal. Civ. Code §§ 1798.29, 1798.82	2003	Acquisition		Yes	Yes	Yes	Yes
Colorado	Colo. Rev. Stat. § 6-1-716	2006	Acquisition	No harm	Yes	Yes		
Connecticut	Conn. Gen Stat. §§ 36a-701b, 4e-70	2012	Access	No harm	Yes	Yes	Yes	
Delaware	Del. Code tit. 6, § 12B-101 et seq.	2005	Acquisition	No harm	Yes	Yes		
DC	D.C. Code §§ 28–3851 et seq., 2020 B 215	2007	Acquisition		Yes	Yes		Yes
Florida	Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)	2014	Access	No harm	Yes		Yes	
Georgia	Ga. Code §§ 10-1-910 to -912; 46-5-214	2005	Acquisition		Yes			
Hawaii	Haw. Rev. Stat. § 487N-1 et seq.	2007	Misuse or risk of misuse	No harm	Yes	Yes		Yes
Idaho	Idaho Stat. §§ 28-51-104 to -107	2006	Misuse or risk of misuse	No harm	Yes	Yes	Yes	
Illinois	815 ILCS §§ 530/1 to 530/25, 815 ILCS 530/55 (2020 S.B. 1624)	2006	Acquisition		Yes	Yes	Yes	Yes
Indiana	Ind. Code §§ 4-1-11 et seq., 24-4.9 et seq.	2006	Acquisition					
Iowa	Iowa Code §§ 715C.1, 715C.2	2008	Acquisition	No harm	Yes	Yes	Yes	
Kansas	Kan. Stat. § 50-7a01 et seq.	2007	Access		Yes	Yes		

Table 1: (continued)

State	Citation	Year	Trigger for notification	No harm exception	Individual notification	Owner notification	AG notification	Private right of action
Kentucky	KRS § 365.732, KRS §§ 61.931 to 61.934	2014	Acquisition		Yes	Yes		
Louisiana	La. Rev. Stat. §§ 51:3071 et seq.	2006	Access	No harm	Yes	Yes	Yes	Yes
Maine	Me. Rev. Stat. tit. 10 § 1346 et seq.	2006	Misuse or risk of misuse	No harm	Yes	Yes	Yes	
Maryland	Md. Code Com. Law §§ 14-3501 et seq., Md. State Govt. Code §§ 10-1301 to -1308	2008	Acquisition	No harm	Yes	Yes	Yes	Yes
Massachusetts	Mass. Gen. Laws § 93H-1 et seq.	2007	Acquisition		Yes	Yes	Yes	
Michigan	Mich. Comp. Laws §§ 445.63, 445.72	2007	Access	No harm	Yes			
Minnesota	Minn. Stat. §§ 325E.61, 325E.64	2006	Acquisition		Yes	Yes		Yes
Mississippi	Miss. Code § 75-24-29	2011	Acquisition	No harm	Yes	Yes		
Missouri	Mo. Rev. Stat. § 407.1500	2009	Access	No harm	Yes	Yes	Yes	
Montana	Mont. Code §§ 2-6-1501 to -1503, 30-14-1704, 33-19-321	2006	Acquisition		Yes	Yes	Yes	
Nebraska	Neb. Rev. Stat. §§ 87-801 et seq.	2006	Acquisition	No harm	Yes	Yes	Yes	
Nevada	Nev. Rev. Stat. §§ 603A.010 et seq., 242.183	2005	Acquisition		Yes	Yes		Yes
New Hampshire	N.H. Rev. Stat. §§ 359-C:19, 359-C:20, 359-C:21	2007	Acquisition	No harm	Yes	Yes	Yes	Yes
New Jersey	N.J. Stat. § 56:8-161, 163	2005	Access		Yes	Yes		
New Mexico	N.M. Stat. §§ 57-12C-1	2017	Acquisition	No harm	Yes	Yes	Yes	
New York	N.Y. Gen. Bus. Law § 899-AA	2005	Acquisition		Yes	Yes	Yes	
North Carolina	N.C. Gen. Stat §§ 75-61, 75-65, 14-113.20	2005	Access	No harm	Yes	Yes	Yes	Yes
North Dakota	N.D. Cent. Code §§ 51-30-01 et seq.	2005	Acquisition		Yes	Yes	Yes	

Table 1: (continued)

State	Citation	Year	Trigger for notification	No harm exception	Individual notification	Owner notification	AG notification	Private right of action
Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192	2006	Access	No harm	Yes	Yes		
Oklahoma	Okla. Stat. §§ 74-3113.1, 24–161 to —166	2008	Access		Yes	Yes		
Oregon	Oregon Rev. Stat. §§ 646A.600 to .628	2007	Acquisition	No harm	Yes	Yes	Yes	Yes
Pennsylvania	73 Pa. Stat. §§ 2301 et seq.	2006	Access	No harm	Yes	Yes		
Rhode Island	R.I. Gen. Laws §§ 11-49.3-1 et seq.	2006	Acquisition	No harm	Yes	Yes	Yes	Yes
South Carolina	S.C. Code § 39-1-90	2009	Acquisition	No harm	Yes	Yes		Yes
South Dakota	S.D. Cod. Laws §§ 20-40-19 to -26	2018	Acquisition	No harm	Yes		Yes	
Tennessee	Tenn. Code §§ 47-18-2107; 8-4-119	2005	Acquisition		Yes	Yes		Yes
Texas	Tex. Bus. & Com. Code §§ 521.002, 521.053	2009	Acquisition		Yes	Yes		
Utah	Utah Code §§ 13-44-101 et seq.	2007	Acquisition		Yes	Yes		
Vermont	Vt. Stat. tit. 9 §§ 2430, 2435	2012	Acquisition		Yes	Yes	Yes	
Virginia	Va. Code §§ 18.2-186.6, 32.1-127.1:05	2008	Access		Yes	Yes	Yes	Yes
Washington	Wash. Rev. Code §§ 19.255.010, 42.56.590	2005	Acquisition	No harm	Yes	Yes	Yes	
West Virginia	W.V. Code §§ 46A-2A-101 et seq.	2008	Access		Yes	Yes		
Wisconsin	Wis. Stat. § 134.98	2006	Acquisition	No harm	Yes	Yes		
Wyoming	Wyo. Stat. § 6-3-901(b), §§ 40-12-501 to —502	2007	Access	No harm	Yes	Yes		

Table 1 presents summary information on 50 US state and District of Columbia BNLs enacted from 2003 to 2018. Information includes state statute citation, year of enactment, type of data breach triggering notification requirements, whether there is a "no harm" (to breached state residents) exception to that trigger, whether individual state residents suffering data breach are notified, whether data owners separate from breached state residents are notified, whether state attorneys general are notified, and whether state residents and other private individuals with standing have a private right of action to sue firms for untimely notification. Information for Table 1 comes primarily from Solove and Schwartz (2019) supplemented with information from the National Conference of State Legislatures (NCSL 2021). We define "BNL enactment" year as the year the law received legislative and executive approval and then became effective.

make thoughtful choices about which firms to engage with and let markets guide decisions about appropriate sanctions to deter socially undesirable behavior.

Does the evidence support that intuition? There are few published studies empirically analyzing the impact of BNLs on data breaches or the misuse of breached data either locally in individual US states (Kesari 2022a) or nationally across them (Romanosky, Telang, and Acquisti 2011). This is concerning. Data hacking operations are increasingly sophisticated (Gupta 2018). Markets for stolen consumer identities on the dark web have more participants (Steel 2019). And consumers blithely share more personal data online without appreciating professional and personal risks (Acquisti and Fong 2020; Acquisti, Brandimarte, and Loewenstein 2020). As costly data breaches increase, so does the need to understand whether and when BNLs decrease their number and magnitude.

We respond by asking two research questions: (1) Do BNLs decrease the count of data breach events? (2) Do they decrease the magnitude of records compromised in a data breach event? As BNLs differ along various dimensions, our answers to these two questions also compel investigation about whether certain types of BNLs decrease data breach counts and magnitudes more than others – for example, BNLs providing consumers with a private right of action to sue firms for legal damages. As malicious actors may exploit them after the fact, we also investigate whether BNLs decrease follow-on malicious uses like identity theft and fraud.

We generate evidence to answer the two questions about BNLs and data breach trends using novel data from the Privacy Rights Clearinghouse (PRC), a California-based, not-for-profit organization aggregating information on data breaches in firms since 2005 (Collins 2019; Goel and Shawky 2014; Nieuwesteeg 2017; PRC 2022). PRC data include information on breached firms, locations, and numbers of records compromised. PRC data also include information on data breach cause – for example, whether the cause was an error by an employee inside the firm or by an outside hacker. We use PRC data to estimate change in data breach event counts and magnitudes by exploiting the phased nature of BNL enactments from 2003 to 2018. Our estimations utilize a two-way fixed effects design featuring so-called "difference-in-differences" estimations permitting causal inference about the impact of BNL enactments on data breach event counts and magnitudes in different US states from 2005 to 2019. In doing so, we examine various data breach types such as those caused by an external hacker and various BNL types such as those giving affected state residents with private rights of action to sue firms for untimely data breach notification. We use the same two-way fixed effects approach to investigate the impact of BNLs on follow-on counts and magnitudes of identity theft and fraud. For these analyses, we use alternative data from the FTC's Consumer Sentinel Network Data Book (FTC 2021).

Our analyses indicate no significant change either in data breach counts or magnitudes, either generally or for specific BNL types. Consistent with prior work (Romanosky, Telang, and Acquisti 2011), we do find a significant decrease in identity theft incident magnitudes during early years of BNL enactments (2005–2010). Across all 15 years of study (2005–2019), however, we observe no significant change in counts or magnitudes of identity theft and fraud incidents. Our different BNL "non-effects" appear to be precisely estimated nulls. Together, they call into question the principal regulatory policy of state legislatures seeking to decrease data breaches and develop a market for data privacy.

These findings are important for academic research, related industry practice, and public policy. They provide researchers with the first broad-sample statistical evidence of BNL ineffectiveness derived from the long-term study of data breaches and follow-on misuse of breached data by malicious actors. They confirm earlier research skepticism about the efficacy of state-based regulation of data privacy in firms (Park 2019) and empirically challenge the conclusion that such state-based regulation decreases related data misuse in the long term.

Our findings also suggest the need for change in data breach standards and information dissemination. Consistent technological standards defining data breaches, timely notification, and mitigation would guide firms in adopting industry-wide practices across the US. Numerous potential solutions exist, ranging from stronger penalties and liabilities for firms failing to meet timely notification standards to more accessible information so that the public can better understand circumstances of firm data breaches and firm attempts to mitigate harm from those breaches. Market development requires both. To that end, we propose an alternative US federal BNL regime featuring the creation of an expert body and supporting staff. This body would set technological standards and publish data in an accessible format for consumers, public officials, and other stakeholders. This new regime could spur immediate decrease in data breach counts and magnitudes as well as longer-term development of the data privacy market state BNLs apparently failed to develop over 20 years.

2 Background

Brief review of BNLs and related research lays a helpful foundation for our study. BNLs represent the principal regulatory policy approach US state legislatures took to curb data breaches in the 2000s and 2010s. Typically, BNLs compel public agencies and private firms to provide timely notification about breaches of personally identifiable information (PII) to affected state residents such as consumers, data owners, and or attorneys general (Peters 2014; Solove and Schwartz 2019). Failure

to comply typically prompts state civil penalties (Faulkner 2007). More egregious failures to comply might also draw attention, enforcement actions, and penalties from US federal authorities like the FTC. Table 2 shows that, by 2019, certain US federal appellate circuits had established a basis for standing and injury-in-fact for data security-based privacy harm.

Others have analyzed foreign national (*e.g.,* Kemp, Buil-Gil, Mirò-Llinares, and Lord 2023) and supranational (*e.g.*,Karyda and Mitrou 2016) approaches to data privacy and security regulation, but our interest is with the US approach. Federal data privacy and security regulation might best be described as a patchwork of statutes targeting specific industries or groups and defining specific data security standards for the same: the Gramm Leach Bliley Act and the Fair and the Accurate Credit Transactions Act (FACT) cover financial data; the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act cover healthcare data; and the Children's Online Privacy Protection Act (COPPA) covers data on children under the age of 13 (Faulkner 2007; Rode 2006; Stevens 2012). In 2002, the Sarbanes-Oxley Act (SOX) overhauled financial reporting and investor protections in publicly listed firms. Although SOX did not explicitly address data breaches, recent US Securities and Exchange Commission (SEC) releases (SEC 2018) and guidance (SEC 2020) articulated new disclosure requirements for material cybersecurity risks and data security safeguards as part of broader corporate governance oversight mandated by SOX.

Otherwise, regulation governing data breaches has been left to individual states with BNLs as the principal state response (Peters 2014; Stevens 2012; Wolf 2018). A state-by-state approach has intuitive appeal. It permits experimentation by state policy-makers and gives firms some choice in data privacy regime (Needles 2009; Rode 2006). In practice, however, most commentators find the approach wanting (Joerling 2010; Peters 2014; Stevens 2012). BNLs typically apply to the states of residents with breached records rather than to states where breached firms are located. Thus, enactment of a BNL in a large population state like California could implicate any firm with a national customer base. As discussed by Tom (2010), consumer groups have favored the enactment of a federal BNL setting a single set of standards, penalties, and information on data breaches. Firms are similarly disposed. State laws impose inconsistent requirements and increasing costs for firms dealing with up to 51 different state regulatory regimes (Peters 2014). In this context, it is not surprising that many legal commentators advocate for federal legislation pre-empting state BNLs and creating a single federal BNL (Faulkner 2007; Peters 2014; Picanso 2006; Tom 2010).

Most empirical work also reflects skepticism about a state-by-state approach for addressing data breaches. Much of this work is anecdotal and bereft of rigorous statistical methods to identify effects. Still, it largely suggests that civil liability in

Table 2: US circuit court of appeals decisions on standing and injury in fact standards related to data breaches.

Decision	Year	Summary	Circuit
Attias *v. Carefirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017).	2017	Plaintiff consumers have standing under Article III if sensitive information was stolen during a data breach. This is especially true if the stolen data "plausibly" include Social Security numbers (SSNs) and credit card numbers (CCNs).	DC circuit
Katz *v. Pershing, LLC*, 672 F.3d 64 (1st Cir. 2012).	2012	Contrary holding to other circuits. Plaintiffs do ***not*** have standing if they cannot identify actual harm (injury) rather than the mere threat of harm in the future.	1st circuit
Rudolph v. Hudsons Bay Co., No. 18 cv 8472 (PKC) (S.D.N.Y. 2019).	2019	Overturns *Whalen v Michaels Stores*. Plaintiff identified and particularized loss as a result of time spent dealing with the data breach and getting a new CC. This constituted an injury with Article III standing.	2nd circuit
In Re ***Horizon*** *Healthcare Services Inc. Data Breach*, 846 F.3d 625 (3d Cir. 2017).	2017	Laptop stolen from healthcare insurer leads to plaintiff claims under Fair Credit Reporting Act (FCRA). Unlawful disclosure creates a *de facto* injury under FCRA conferring Article III standing.	3rd circuit
Hutton *v. Nat. Bd. of Examiners in Optometry, Inc*, 892 F.3d 613 (4th Cir. 2018).	2018	Database hack led to ID theft and fraudulent CC charges harming plaintiffs. Out-of-pocket costs resulting from and time lost responding to data breach constitute injury with Article III standing.	4th circuit
Galaria *v. Nationwide Mutual Insurance Company*, No. 15–3386 (6th Cir. Sept. 12, 2016).	2016	Hackers breached a computer network and stole plaintiff's data, leading to expenses for plaintiff associated with dealing with the fallout of this hack. This constitutes an injury with Article III standing.	6th circuit
Lewert *v. PF Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016).	2016	Data breach at a Chinese restaurant. CCNs and other data were stolen. Increased risk of fraudulent charges and ID theft constitutes an injury to plaintiff with Article III standing.	7th circuit
Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).	2010	Theft of a laptop with personal data about plaintiffs caused anxiety and threat of future harm. This constitutes an injury with Article III standing.	9th circuit

Table 2: (continued)

Decision	Year	Summary	Circuit
Resnick *v. AvMed, Inc*., 693 F.3d 1317 (11th Cir. 2012).	2012	Theft of a laptop resulted in identity theft and fraud causing financial loss to plaintiff. This constitutes an injury with Article III standing.	11th circuit

Table 2 presents summary information on selected US Circuit Courts of Appeals decisions from 2010 to 2018 defining standing and injury-in-fact standards in data breach cases. Information on these decisions comes primarily from Solove and Schwartz (2019) updated where appropriate by the authors. Decisions listed in the references section of this paper are appear alphabetically based on the first letter of the party in highlighted in ***bold italicized*** type.

the wake of BNL enactment neither prevents company negligence nor adequately compensates victims (Faulkner 2007; Joerling 2010). What statistical work does exist largely corroborates this assessment of impotence. Goel and Shawky (2014) use an event study approach to demonstrate that cumulative abnormal share returns to firms after a data breach are negative, but that these punitive effects diminish over time. Laube and Böhme (2016) analytically demonstrate that, even under optimistic assumptions, mandatory reporting requirements in BNLs are unlikely to generate substantial data breach reductions because optimal audits and sanctions are difficult to formulate and implement, despite legislative histories indicating that lawmakers are aggressively trying to do so.

In what may be the only encouraging pieces of published empirical work, Kesari (2022a) finds that medical identity theft rates, often following data breaches, significantly decreased in California after the state revised its BNL in 2016, while Romanosky and colleagues (2011) find that BNLs enacted in several US states significantly decreased incidences of general identity theft in the 2000s. Neither study evaluates BNL impact on data breach instances themselves. Studies in other working papers also suggest some BNL effect. One such study by Nieuwesteeg (2017) uses PRC data from 2005 to 2012 analyzed with fixed effects regression to detect significantly positive BNL effects on notification counts though the overall rate of notification remains extremely low. Another such study by Kesari (2022b) uses the FTC Consumer Sentinel Network Data Book from 2000 to 2020 analyzed with a staggered synthetic controls approach to detect a wide range of significantly negative *and positive* BNL effects on incidences of identify thefts nationally.

In this context, our study fills important research gaps. We use data of national scope across two decades analyzed with a difference-in-differences approach to generate broad sample statistical evidence permitting causal inference about any significant BNL effects on the count of data breach incidents (counts), the number of breached records no matter the counts (magnitudes), and downstream malicious

use for identity theft and fraud. Our study fills gaps in previous work related to data, time-period, and analytical approach to generate comprehensive evidence about whether BNLs decrease data breach counts and magnitudes.

3 Empirical Methods

3.1 Data and Sampling

We use data from several sources to generate that evidence. We start with the PRC data (2022). Founded in 2005, the PRC aggregates information on data breaches for research and public policy-making purposes (Ayyagari 2012; Goel and Shawky 2014). The PRC grew out of an initiative at the University of California San Diego and the State of California, from which it still sources much of its data breach information. The PRC also collects information from government agencies in other states, from US federal government agencies such as the Department of Health and Human Services Office for Civil Rights, and from non-governmental organizations and individuals such as DataBreaches.net. The PRC also collects its own data from media reports. As of January 2022, PRC data included information on more than 9000 instances of data breaches at firms, government agencies, and other types of organizations across the US. It is the largest publicly accessible database on firm data breaches traceable to specific states, thus making it popular for academic research and related policy analyses on data breaches (see, *e.g.*, Edwards, Hofmeyr, and Forrest 2016).

In addition to sheer quantity, PRC data quality matters for our study. They include information on both data breach incidents and the number of records associated with each incident. This permits analyses of counts and magnitudes. PRC data are also categorized several ways, including whether the data breach was caused by an inside employee handling error or by an outside hacker. This allows us to analyze heterogeneity in the cause of data breach counts and magnitudes.

PRC data also present challenges for researchers to address. One challenge relates to time. The PRC data starts in 2005, 2 years after BNL enactment in California and the same year as BNL enactment in 11 other states.[1] Thus, our analyses may understate the impact of early and potentially quite important BNLs. That said, the concern does not undermine the basic validity of our analyses across the range

1 We define the "BNL enactment" year as the year the law completed all three stages: legislative approval, executive approval, and then became effective. In most US states, the year of approvals and effectiveness is the same. Where they differ, we use the year when a BNL law became effective as the year of BNL enactment.

of BNL enactments from 2003 to 2018. Empirically, it means that observations from these states will not help in identification of BNL enactment effects, but they will still help in identifying broader time trends.

Another challenge relates to attribution of PRC data on breach magnitudes. Some breach incidents in the PRC data may attribute all records breached to a firm's state of domicile rather than to each state where firm customers are located. Such misattribution is more likely for incidents of massive data breaches at large publicly listed companies such as the 2017 Equifax data breach incident (Equifax 2019). Thus, our analyses may skew estimates of BNL enactment effects in states with many large publicly listed companies such as New York. Empirically, it means that we should compare any general analyses of BNL impact on data breach magnitudes with re-analyses using sub-samples including only smaller firms. They are more likely to have greater overlap of state corporate domicile and customer location. The PRC data permit sub-sampling for these and other robustness analyses.[2]

A third challenge relates to the concurrence of trends in BNL enactment and PRC data collection breadth. From 2005 to 2019, 14 states began publicly disclosing information about data breach incidences either when their BNLs were first enacted (*e.g.*, Massachusetts in 2007) or afterwards (*e.g.*, California in 2012).[3] PRC could collect and report data from these states more easily after their BNL enactments. These concurrent trends create the potential for detection of a spuriously positive rather than expected negative correlation between BNL enactment and data breach counts and magnitudes.[4]

Empirically, it means we should include in all estimated models time (year) fixed effects. Their inclusion should ameliorate problems of strict increases in incidents in different years. We should also compare full-sample analyses of BNL impact on breach counts and magnitudes using sub-samples of PRC data less likely to come from these state sources. The PRC data let us identify incidents of

2 We defer for the moment description of FTC data used to test whether BNLs decreased incidents of identity theft and fraud.

3 Fourteen states were publicly disclosing information on data breach incidences sometime from 2005 to 2019: These states (and years of earliest publicly disclosed data breach incidents) include: California (2012), Delaware (2018), Hawaii (2007), Indiana (2014), Iowa (2011), Maine (2010), Montana (2018), New Hampshire (2016), New Jersey (2015), North Dakota (2018), Oregon (2015), Vermont (2016), Washington State (2016), and Wisconsin (2012).

4 Alternatively, and much less likely, increasing data breach reports in the PRC following public disclosure of breach incident information by a state could correlate precisely with breach incident reductions due to BNL enactment in that same state. Analyses might then indicate no significant (net) BNL effects in that state. While possible in concept, this result is highly unlikely in practice, particularly for states with different years for BNL enactment and public disclosure of data breach incidences. In any case, inclusion of year fixed effects in all estimated models as well as the alternative data and sub-sampling strategies described in this section address this potential problem.

healthcare-related breaches largely coming from non-state sources such as the US Department of Health and Human Services. The PRC data also let us identify general breach incidents that come from state attorney general offices. Thus, we can compare full-sample analyses of BNL impact with analyses of BNL impact using (federal) healthcare and non-state attorney general sub-samples of PRC data. Finally, we should compare analyses of BNL impact on breach counts and magnitudes using PRC data with BNL impact on post-breach incidents of identity theft and fraud using the FTC's Consumer Sentinel Network Data Book, another non-state data source.

Our analyses also rely on data about BNLs from Solove and Schwartz (2019) and the National Conference of State Legislatures, cross-checked for accuracy through review of the same data published by the Perkins-Coie law firm (Perkins 2021). Both sources let us identify BNL enactment (treatment) dates and characteristics such as triggers for notification and individuals to be notified. These data sources comprise the empirical foundation for analyses of BNLs and firm data breaches occurring in the US from 2005 to 2019. These data sources yield a sample of 765 state-year observations of data breach counts and magnitudes in 51 "states" including the District of Columbia.

3.2 Variables

3.2.1 Dependent Variables

We define two dependent variables. The first dependent variable is the count of data breach events occurring in each state *j* in year *t*. This allows us to assess changes in the frequency of data breached after BNL enactment. The second is the number of records breached in each state *j* in year *t*. This allows us to assess changes in the magnitude of data breached after BNL enactment. This dependent variable can be nearly zero or in the millions. We take the natural log of this dependent variable, thus interpreting magnitude effects as elasticities.

3.2.2 Primary Independent Variable

The primary independent variable is a 0–1 indicator term equaling one when a BNL has been enacted in state *j* in year *t*. We take two approaches to defining BNL enactment. Our first approach defines BNL enactment with the year *t* when any type of BNL comes into force in state *j*. Our second approach defines BNL enactment with the year *t* when a type of BNL creating a private right of action comes into force in state *j*. Our first approach is broad but may not account for a subset of BNLs using private enforcement to create stronger firm incentives to safeguard against data breaches. Our second approach narrows BNL enactment criteria but

may not account for BNLs that, though they create no private right of action, still create firm incentives to safeguard against data breaches if vigorously enforced by public officials like state attorneys general. We present most results below using both approaches.

3.2.3 Controls

We employ a difference-in-differences estimation strategy, so we also include two-way state (cross-sectional) and year (time-series) fixed effects. Intuitively, state fixed effects should absorb any time invariant heterogeneity between states – for example, California having a much larger population and economy than, say, Rhode Island. Year fixed effects should absorb any universal trends across states changing from year to year – for example, an increasing trend in data breaches across states.

3.3 Model Specification, Estimation, and Hypothesis Tests

We estimate effects using the following equation:

$$Y_{jt} = \beta_1 x_1 + \varrho_j + \tau_t + \varepsilon$$

β_1 captures the key difference in differences, that is, the difference in annual data breach counts and magnitudes in states following BNL enactment. ϱ is a vector of state fixed effects indexed by j. τ is a vector of time (year) fixed effects indexed by t. ε is the error term. When assessing data breach magnitudes, y_{jt} is the natural log of the number of records breached in state j in year t. To estimate variation in that number, we use ordinary least squares (OLS) regression. β_1 is thus interpreted here as the elastic change in the number of breached records in "treated" states when a BNL has been enacted. When assessing data breach counts, y_{jt} is the number of data breach events in state j in year t. To estimate variation in this number, we use quasi-maximum likelihood Poisson regression. β_1 is then interpreted as the marginal change in absolute counts. This estimator avoids complications following from logged OLS and fixed effect negative binomial estimators (Allison and Waterman 2002; Silva and Tenreyro 2006, 2011). We use Stata Version 16.1 (Stata 2019) for all estimations. No matter the dependent variable measure or estimator, our assumption that BNL enactment decreases data breach counts and magnitudes reduces to tests of whether $\beta_1 < 0$.

3.4 Other Methodological Issues and Innovations

Four methodological issues merit brief discussion given our approach to analyzing BNL effects on data breach counts and magnitudes: (1) whether the assumptions of

difference-in-differences analysis hold; (2) whether specific data breach categories might be more responsive; (3) whether, given the expectation of a null result, we can differentiate between the absence of statistical significance and the absence of any effect; and (4) adjustments for multiple comparisons.

Regarding the first issue about difference-in-differences analysis, the primary assumption is that the dependent variable for treatment and control groups is trending in a parallel manner prior to treatment (Angrist and Pischke 2008). The intuition is simple. If treated states are accelerating in data breaches prior to treatment but untreated states are decelerating in data breaches, then estimation of the treatment effect would be biased, and the estimated effect would be incorrectly attributing post-treatment differences to the treatment.

To determine whether treated and untreated states are trending in this parallel manner, we use a variant of the event-study method proposed by Autor and colleagues (2003) and exemplified in previous research (Burtch, Carnahan, and Greenwood 2018; Carnahan 2017; Zamoff, Greenwood, and Burtch 2022). We estimate the effect semi-parametrically by creating 15 0–1 indicators equaling one when data breach magnitudes or counts for state j in year t are a certain number of years before or after state j receives treatment in the form of BNL enactment. These "relative time" indicators let us visualize magnitude and count effects from 4 years before (Rel Time $t-4$) to 10 years after (Rel Time $t + 10$) BNL enactment. Relative time indicators for years t and $t - 1$ are omitted to serve as bases for comparison.[5] Relative time indicators more than 4 years before treatment (Rel Time $t-4$) and 10 years after treatment (Rel Time $t + 10$) are collapsed for interpretability.

Regarding the second issue, data breach category, there are two ways that firms might approach the question of limiting data breaches. First, firms might be more concerned about attacks from outside hackers than inside employees making data handling errors. Such a conclusion is reasonable if firms possess valuable consumer data those hackers could profitably misuse themselves or sell to others. Second, many data breaches stem from poor internal practices. That prospect motivates many firms to institute internal policies intended to prevent unintentional disclosure of protected data – for example, requiring uniform data encryption (Winn 2009). We investigate both possibilities. It is plausible that a change in one is not visible with unaddressed data poisoning the pool. Taking this approach further allows us to avoid the "file-drawer" problem, wherein researchers gravitate towards significant and publishable results rather than insignificant ones often failing to reach

5 We omit two periods rather than one from relative time estimations to account for co-movements between relative time indicators and absolute time dummies eliminating an additional degree of freedom from these estimations.

the public through publication (Dynes and Holbein 2020; Franco, Malhotra, and Simonovits 2014; Goldfarb and King 2015).

Regarding the third issue about differentiating insignificant results from precisely estimated null effects, we turn to research analyzing differentiation in economics, political science, business, medicine, and law (Ahammer, Halla, and Schneeweis 2020; Dynes and Holbein 2020; McNamara, Vaaler, and Devers 2003; Walker and Nowacki 2011). Traditional hypothesis testing relies on rejecting the null hypothesis that two terms are not statistically different. Such testing typically provides an estimate of difference between two groups and the statistically derived confidence in that difference. This approach becomes problematic when making comparisons failing to reject the null. This situation often arises in underpowered empirical studies (Gelman and Carlin 2014). Following Dynes and Holbein (2020), we address this third issue following research on statistical sub-significance. In addition to conventional interpretation of estimated coefficients, we set 36 percent of a standard deviation as a threshold for what constitutes a meaningful difference from zero (Hartman and Hidalgo 2018; McCaskey and Rainey 2015).

The fourth issue addresses corrections to the standard 95 percent confidence interval when analyses include multiple dependent variables. Again, this relates to the file-drawer issue (Franco, Malhotra, and Simonovits 2014). Increasing the number of treatments also increases the likelihood of finding some significant correlation purely by chance. That said, we choose *not* to employ a correction in what follows given our expectation of a null result. A confidence interval correction would widen intervals, thus making it more difficult to observe any significance. But our goal is to make it more difficult *not* to observe significance, thus our non-correction strategy.

4 Results

4.1 OLS and Poisson Regression Results for Data Breaches

We start with Table 3 OLS and Poisson regression results addressing research questions about whether BNLs reduce data breach counts or magnitudes. They indicate no systemic correlation between BNL enactment and change in either data breach magnitudes or counts. Columns 1 and 2 report results regarding data breach magnitudes. Neither enactment of any BNL (Column 1) nor enactment of a BNL with a private right of action (PROA) (Column 2) significantly influences the log number of records breached. Convention also indicates that the effects are a precisely estimated null. The p-values are $p = 0.834$ (Column 1) and $p = 0.456$ (Column 2) respectively. The standard deviation of the log number of records breached is 4.83, 36

Table 3: Effect of BNLs on data breach counts and magnitudes.

Dependent variable	**(1)**	**(2)**	**(3)**	**(4)**
Estimator	**ln(Records)**	**ln(Records)**	**numEvents**	**numEvents**
Treatment	**Log-OLS**	**Log-OLS**	**Poisson**	**Poisson**
	Any BNL	**BNL w/Private Right of Action (PROA)**	**Any BNL**	**BNL w/PROA**
Any BNL enacted	0.147		−0.0394	
	(0.699)		(0.117)	
BNL w/PROA enacted		0.727		0.116
		(0.968)		(0.341)
State fixed effects	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes
Observations	765	765	765	765
R-squared	0.543	0.544		
Number of groups	51	51	51	51

Table 3 presents coefficient estimates, standard errors (in parentheses) and asterisked (*) indicators of statistical significance for four panel difference-in-difference regression estimations assessing the impact of BNL enactments on annual data breach counts and magnitudes. We use breach data from the PRC (2022) for these estimations. The dependent variable in Columns 1–2 is the natural log of records breached in state *j* during year *t*. The dependent variable in Columns 3–4 is the count of data breach incidents (no matter the number of records breached) in state *i* during year *t*. The key independent variable in Columns 1 and 3 is a 0–1 indicator term equaling one when state *i* in year *t* has enacted any type of BNL. The key independent variable in Columns 2 and 4 is a 0–1 indicator term equaling one when state *i* in year *t* has enacted a BNL permitting private rights of action. Though not presented in Table 3, all estimations also include state and year fixed effects, that is, 0–1 indicator terms for 50 of 51 states and the District of Columbia as well as 14 of 15 years (2005–2019) studied. These results are available from the authors. All estimations use robust standard errors clustered on states. Levels of statistical significance for coefficient estimates are defined by the number of asterisks: $^{***} = p < 0.01$ (significant at the 1 percent level); $^{**} = p < 0.05$ (significant at the 5 percent level); and $^{*} = p < 0.10$ (significant at the 10 percent level). The absence of asterisks on coefficient estimates means that they are not different from zero at commonly accepted levels of statistical significance. This table suggests that BNLs generally and BNLs with private rights of action significantly decrease neither data breach counts nor magnitudes.

percent of which is 1.74. Both point estimates thus fit well within what Hartman and Hidalgo (2018) argue constitutes a meaningful difference from zero. Moreover, the estimated effects are positive (not negative), contrary to the intended effect of BNLs.

Columns 3 and 4 of Table 3 report results regarding data breach counts. There, we again see no change after Poisson regression estimation, whether BNL enactment is broadly (Column 3) or more narrowly (Column 4) defined. These coefficients

again constitute precisely estimated nulls. The p-values are $p = 0.736$ (Column 3) and $p = 0.735$ (Column 4), nowhere near conventional thresholds of statistical significance or a third of a standard error from zero. An equivalence test using the Hartman and Hidalgo (2018) approach further passes muster – the threshold being 6.75 or 36 percent of 18.75. Results reported in Table 3 generally indicate no significant relationship between BNL enactment and change in either data breach counts or magnitudes.

Turning next to the event study results in Table 4, we observe neither significant and systemic pre-treatment, nor significant and systemic post treatment, effects. This is striking. In the pre-treatment measurements – for example, effects 4 years prior to treatment (Rel Time $t-4$) – there is no systematic trend up or down. This suggests that the parallel pre-treatment trends assumption of the difference-in-differences analysis is not demonstrably violated (Angrist and Pischke 2008; Autor 2003). Post-treatment estimations are also devoid of significance at generally accepted levels. Perhaps most striking is that, of the 57 estimated coefficients estimated, only one is significant – Rel Time $t-4$ in Column 3. This is less than would be predicted by a random draw – 1 in 20 at $p < 0.05$. An equivalency test at the 36 percent level passes for all estimations. Not a single coefficient crosses the threshold. In fact, not a single estimate crosses 10 percent of the Hartman and Hidalgo (2018) levels. Again, these results offer no empirical support for the assumption that BNLs reduce data breach counts or magnitudes.

Table 5 presents results from OLS and Poisson regression analyses of BNL enactment effects on data breach counts and magnitudes related to external causes such as hacks and internal causes such as employee errors. Here, the intuition is that effects might be concentrated in a single type of data breach of greater concern to firms. Once again, we observe no significant effects across the estimations. Most of the coefficients are positive. All equivalency tests at 36 percent easily pass. Again, these results offer no empirical support for the assumption that BNLs reduce data breach counts or magnitudes. Instead, they appear to have no material effect.

4.2 Difference-in-Differences Diagnostic Analyses

One concern with multi-site, phased difference-in-differences analysis is the potential for inverse weighting issues. In short, the estimation of the treatment is the sum of weighted comparisons of treated and untreated observations based on when treatment occurs. Each treatment cohort has its own weight on the estimate and derived coefficients may be biased in a base difference-in-differences analysis. Baker, Larcker, and Wang 2022; Callaway and Sant'Anna 2021; Goodman-Bacon 2021 elaborate on these basic points.

Table 4: Effect of BNLs on data breach counts and magnitudes in relative time.

Dependent Variable **Estimator** **Treatment**	**(1)** **ln(Records)** **Log-OLS** **Any BNL**	**(2)** **numEvents** **Poisson** **Any BNL**	**(3)** **ln(Records)** **Log-OLS** **BNL w/PROA**	**(4)** **numEvents** **Poisson** **BNL w/PROA**
Rel Time $t-4+$	−0.770	−0.152		
	(0.918)	(0.226)		
Rel Time $t-4$	−1.392	−0.081	−5.867***	
	(1.324)	(0.188)	(1.644)	
Rel Time $t-3$	−0.196	−0.229	−1.196	−0.864
	(1.236)	(0.161)	(2.874)	(0.450)
Rel Time $t-2$	−0.892	0.011	−0.697	−0.345
	(0.734)	(0.102)	(1.320)	(0.249)
	Omitted periods to avoid dummy variable trap			
Rel Time $t+1$	0.236	0.120	−0.367	−0.116
	(0.618)	(0.137)	(1.133)	(0.194)
Rel Time $t+2$	0.097	0.000	0.695	−0.114
	(0.751)	(0.139)	(0.957)	(0.164)
Rel Time $t+3$	−0.567	−0.118	−1.104	−0.220
	(0.759)	(0.145)	(1.068)	(0.177)
Rel Time $t+4$	0.440	−0.010	−0.044	−0.015
	(0.833)	(0.168)	(1.013)	(0.198)
Rel Time $t+5$	−0.962	−0.057	−0.933	−0.125
	(0.835)	(0.220)	(0.887)	(0.211)
Rel Time $t+6$	0.058	0.166	−0.627	0.384
	(1.011)	(0.356)	(1.105)	(0.522)
Rel Time $t+7$	−0.012	0.011	0.617	0.017
	(1.118)	(0.225)	(1.218)	(0.207)
Rel Time $t+8$	−0.504	−0.085	−1.581	−0.081
	(1.257)	(0.257)	(1.183)	(0.161)
Rel Time $t+9$	1.565	−0.125	0.949	−0.062
	(1.295)	(0.278)	(1.293)	(0.143)
Rel Time $t+10$	0.381	0.082	0.032	0.160
	(1.389)	(0.291)	(1.472)	(0.249)
Rel Time $t+10+$	−0.164	0.169	−1.258	0.246
	(1.549)	(0.319)	(0.979)	(0.260)
State fixed effects	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes

Table 4: (continued)

Dependent Variable Estimator Treatment	(1) ln(Records) Log-OLS Any BNL	(2) numEvents Poisson Any BNL	(3) ln(Records) Log-OLS BNL w/PROA	(4) numEvents Poisson BNL w/PROA
Observations	765	765	765	763
R-squared	0.555		0.554	

Table 4 presents coefficient estimates, standard errors (in parentheses) and asterisked (*) indicators of statistical significance for four semi-parametric panel regression estimations assessing pre- and post-BNL enactment trends in annual data breach counts and magnitudes. We use breach data from the PRC (2022) for these estimations. The dependent variable in Columns 1 and 3 is the natural log of records breached in state *j* during year *t*. The dependent variable in Columns 2 and 4 is the count of data breach incidents (no matter the number of records breached) in state *i* during year *t*. The key independent variable in Columns 1–2 is a 0–1 indicator term equaling one for state *i* in successive years prior to (*e.g.*, $t-3$) and after (*e.g.*, $t+3$) enactment of any type of BNL in year $t=0$. The key independent variable in Columns 3–4 is a 0–1 indicator term equaling one for state *i* in successive years prior to and after enactment of a BNL permitting a private right of action in year $t=0$. Though not presented in Table 4, all estimations also include state and year fixed effects, that is, 0–1 indicator terms for 50 of 51 states and the District of Columbia as well as 14 of 15 years (2005–2019) studied. These results are available from the authors. All panel estimations use robust standard errors clustered on states. Levels of statistical significance for coefficient estimates are defined by the number of asterisks: $^{***} = p < 0.01$ (significant at the 1 percent level); $^{**} = p < 0.05$ (significant at the 5 percent level); and $^{*} = p < 0.10$ (significant at the 10 percent level). The absence of asterisks on coefficient estimates means that they are not different from zero at commonly accepted levels of statistical significance. This table suggests that there are no persistently significant data breach magnitude or count trends linked to the run-up to or aftermath of BNL enactment.

Consistent with these studies, we implement two diagnostic analyses. First, a Goodman-Bacon (2021) decomposition analysis assesses weightings associated with each individual treatment. Results are in Table 6 and displayed graphically in Figure 1A and B. As can be seen, while there is heterogeneity in the effect across the different comparison groups, no inverse weighting problem emerges. This bolsters the case that the estimated effects are not significantly biased due to the phased treatment. We exclusively model the linear estimations as no Poisson equivalent to the decomposition exists.

Second, we replicate the linear estimations using the group-time average treatment effects estimator created by Callaway and Sant'Anna (2021). As with the decomposition, no Poisson version of this tool exists. The purpose of this estimator is two-fold. First, it recovers the properly weighted difference in differences. Second, it assists in diagnosing the parallel trends assumption. Graphical results of the estimation are presented in Figure 2A and B. As can be seen in both figures,

Table 5: Effect of BNLs on data breach counts and magnitudes partitioned by internal and external causes.

Dependent variable	(1) ln(Records)	(2) ln(Records)	(3) numEvents	(4) numEvents	(5) ln(Records)	(6) ln(Records)	(7) numEvents	(8) numEvents
Sample	**Externally caused data breaches (*e.g.*, hack)**				**Internally caused data breaches (*e.g.*, employee error)**			
Estimator	**Log-OLS**	**Log-OLS**	**Poisson**	**Poisson**	**Log-OLS**	**Log-OLS**	**Poisson**	**Poisson**
Treatment	**Any BNL**	**BNL w/PROA**	**Any BNL**	**BNL w/PROA**	**Any BNL**	**BNL w/PROA**	**Any BNL**	**BNL w/PROA**
Any BNL enacted	0.272		−0.001		1.060		0.101	
	(0.788)		(0.153)		(0.573)		(0.151)	
BNL w/PROA enacted		1.022		0.325		1.679		0.250
		(1.116)		(0.510)		(1.024)		(0.606)
State fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	765	765	765	765	765	765	765	765
R-squared	0.458	0.458			0.492	0.492		
Number of groups	51	51	51	51	51	51	51	51

Table 5 presents coefficient estimates, standard errors (in parentheses) and asterisked (*) indicators of statistical significance for eight panel difference-in-difference regression estimations assessing the impact of BNL enactments on annual data breach counts and magnitudes. We use breach data from the PRC (2022) for these estimations. The dependent variable in Columns 1–2 and 5–6 is the natural log of records breached in state *j* during year *t* due to an external hack (Columns 1–2) or internal employee error (Columns 5–6). The dependent variable in Columns 3–4 and 7–8 is the count of data breach incidents (no matter the number of records breached) in state *i* during year *t* due to an external hack (Columns 3–4) or internal employee error (Columns 7–8). The key independent variable in Columns 1, 3, 5, and 7 is a 0–1 indicator term equaling one when state *i* in year *t* has enacted any type of BNL. The key independent variable in Columns 2, 4, 6, and 8 is a 0–1 indicator term equaling one when state *i* in year *t* has enacted a BNL permitting a private right of action. Though not presented in Table 5, all estimations also include state and year fixed effects, that is, 0–1 indicator terms for 50 of 51 states and the District of Columbia as well as 14 of 15 years (2005–2019) studied. These results are available from the authors. All estimations use robust standard errors clustered on states. Levels of statistical significance for coefficient estimates are defined by the number of asterisks: $^{***} = p < 0.01$ (significant at the 1 percent level); $^{**} = p < 0.05$ (significant at the 5 percent level); and $^{*} = p < 0.10$ (significant at the 10 percent level). The absence of asterisks on coefficient estimates means that they are not different from zero at commonly accepted levels of statistical significance. This table suggests that BNLs generally and BNLs with private rights of action significantly decrease neither data breach counts nor magnitudes linked to external or internal agents.

Table 6: Results from Goodman-Bacon (2021) decomposition analysis.

T = Treatment **C = Control** **Any BNL**	**Weight**	**DD avg**
Earlier T versus later C	0.148	−1.519
Later T versus earlier C	0.474	0.589
T versus already treated	0.378	0.244
BNL w/PROA		
Earlier T versus later C	0.009	−1.519
Later T versus earlier C	0.072	0.699
T versus never treated	0.825	0.665
T versus already treated	0.094	1.522

Table 6 presents average weights and panel difference-in-difference regression (DD) trend estimates for different comparison groups comprising overall DD linear trends in data breach magnitudes. We use breach data from the PRC (2022) for these estimations. This table suggests no weighting issues biasing panel difference-in-difference regression estimates presented in previous tables.

there is little in the way of pre-treatment trend. Further, there is no demonstrable dip in the number of records breached after BNL enactment.

4.3 Equivalency Tests

One concern with traditional econometric approaches to questions like the ones proposed is that hypothesis testing hinges on the rejection of values not equaling zero. Failing to reject the null is not traditionally interpreted as there being zero effect. Hence the adage: The absence of evidence is not evidence of absence. In this context, we seek analyses establishing the similarity of two items. One such analysis used in medical research is equivalency testing (Walker and Nowacki 2011). Intuitively, the idea is to determine if the confidence intervals of two treatments overlap. If they do, or the confidence intervals are not different from a randomly generated estimate, then treatments are deemed to have similar efficacy. Such an approach is appealing here because it allows us to examine whether the treatment effect is outside the bounds of a randomly generated pseudo effect.

To examine if the effects are demonstrably similar to an effect generated at random, we replicate the estimations reported in Table 3. However, instead of using the actual treatment, we randomize the treatment based on an identical portion of the sample. Using this randomization, we then estimate the pseudo effect, that is, the effect that might appear purely by chance. This process is executed 1000 times for each estimation with the coefficient stored each time. Using these pseudo-estimates,

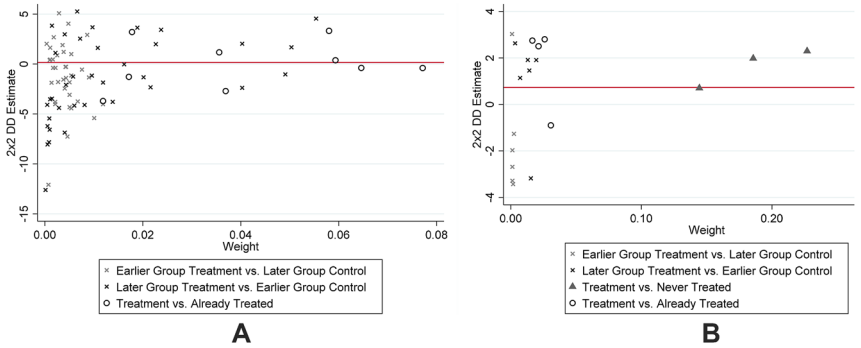

Figure 1: Figure 1A and B plots observations in the comparison groups used to arrive at these weight and DD trend estimates consistent with a Goodman-Bacon (2021) decomposition analysis. The overall two-way fixed effects estimates, 0.3 in Figure 1A and B, equal the average of the *y*-axis values weighted by their *x*-axis value. The lighter exes (x) represent terms where the comparison group is states enacting BNLs earlier (2005–2006) versus a control group of states not having enacted BNLs in later years (2007–2018). The darker exes (x) represent terms where the comparison group is state enacting BNLs later (2007–2018) versus a control group of states not having enacted BNLs in earlier years (2005–2006). The open circles (°) represent terms where the comparison group is states in the initial year of BNL enactment versus states already having enacted BNLs. Figure 1A plots terms for these comparison groups and overall DD trend line for any BNL. Figure 1B does the same for BNLs permitting a private right of action. Figure 1B also plots terms for a fourth comparison group unique to this sub-sample: states that enacted BNLs with a private right of action versus states that never enacted such a BNL. These figures suggest no weighting issues biasing panel difference-in-difference regression estimates presented in previous tables.

we then conduct a mean-equivalence t-test. The appeal of this approach is that we can directly observe if the treatment is superior or inferior to a random draw.

Results are reported in Table 7. In Column 1, the test rejects the assertion that the randomly generated pseudo coefficient is either larger ($\Pr(T > t1)$) or smaller ($\Pr(T > t2)$) than the actual coefficient. The same is true for Columns 2 and 4, once again underscoring the precisely estimated nature of the null effects. Results in Column 3 are less clear. On the one hand, they indicate that the random effect is not larger than the estimated effect. On other hand, they also indicate that a random coefficient is smaller than the estimated effect. Indeed, the estimated effect is more than two standard deviations *larger* than the randomly generated pseudo effect. This difference indicates that the estimated data breach count is *not falling* after BNL enactment.

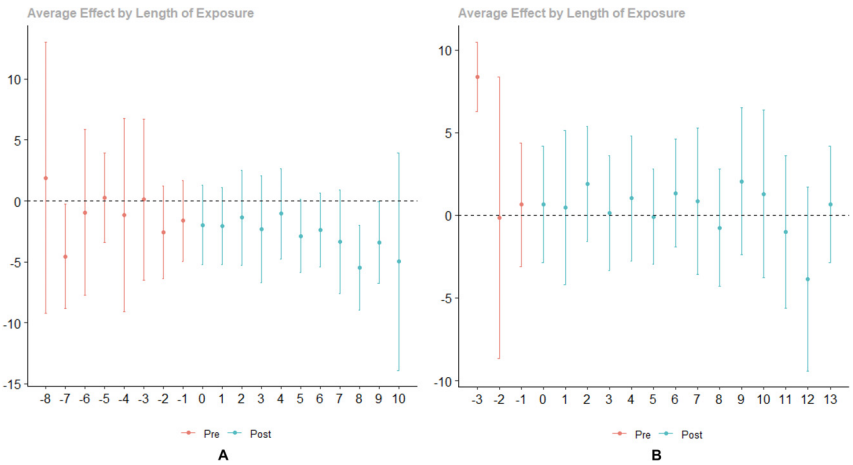

Figure 2: Figure 2A is agraphical representation of Callaway and Sant'Anna (2021) difference-in-difference estimation for any BNL. Figure 2B is a graphical representation of Callaway and Sant'Anna (2021) difference-in-difference estimation for BNLs permitting a private right of action. w/PROA). Figure 2A and B both depict weighted pre- and post-treatment trend estimates derived from panel linear difference-in-difference regression estimation (magnitudes) in Table 3 with five percent ($p < 0.05$) confidence intervals for the log of records breached annually in states j over 19 years pre- and post-enactment of any BNL (Figure 2A) and over 17 years pre- and post-enactment of BNLs permitting a private right of action (Figure 2B). Estimates with confidence interval lines crossing the zero line are not significantly different from zero at the five percent level. We use breach data from the PRC (2022) for these estimations. These figures suggest no persistently significant pre- or post-BNL enactment trends affecting data breach magnitudes.

4.4 OLS and Poisson Regression Results for Alternative PRC Data Sources

Recall our earlier discussion of PRC data limitations tied to the concurrence of BNL enactments and increasing PRC breadth of data sources as certain states begin publicly disclosing information about breach incidents. Again, inclusion of year fixed effects in our model should ameliorate problems of strict increase in incidences in a given year. We should also compare full-sample analyses of BNL impact with analyses of BNL impact using healthcare and non-state attorney general subsamples of PRC data.[6] We do so, and report results in Table 8. Columns 1–4 report results for healthcare-related data breach incidents. Columns 5–8 do the same for

6 For incident type and source, we also consulted PHIPrivacy.net (DataBreaches.net 2021), a private breach data aggregator operating since the late 2000s.

Table 7: Equivalency tests of actual versus randomly generated pseudo coefficient estimates.

Dependent variable	**(1)**	**(2)**	**(3)**	**(4)**
Estimator	**ln(Records)**	**numEvents**	**ln(Records)**	**numEvents**
Treatment	**Log-OLS**	**Poisson**	**Log-OLS**	**Poisson**
	Any BNL	**Any BNL**	**BNL w/PROA**	**BNL w/PROA**
Estimated effect	0.147	−0.039	0.727	0.116
Randomly generated effect	−0.005	−0.107	0.001	−0.002
Standard deviation	0.342	0.277	0.076	0.067
PR($T > T1$) – superior	0.000	0.000	0.000	0.000
Pr($T > t2$) – inferior	0.000	0.000	0.997	0.000

Table 7 presents results from equivalency tests using coefficient estimates derived from panel difference-in-difference regression estimations reported above in Table 3. We use breach data from the PRC (2022) for these estimations. In the row labeled "Estimated Effect," we present actual coefficient estimates from Table 3 panel difference-in-difference regressions assessing the impact of BNL enactments on annual data breach counts and magnitudes. This table also presents in the row labeled "Randomly Generated Effect" pseudo coefficient estimates generated randomly from repeated panel difference-in-difference regression estimations using the same sample. These two coefficient estimates are then compared to test whether randomly generated pseudo coefficient estimates are significantly larger (Pr($T > t1$) or smaller (Pr($T > t2$) than their actual counterparts at commonly accepted levels of statistical significance, that is, at least $p < 0.10$ (10 percent significance). Randomly generated pseudo coefficients in Columns 1–2 and 4 are neither significantly larger nor smaller than their actual counterparts. The randomly generated pseudo coefficient in Column 3 is not significantly larger but is significantly smaller than its actual counterpart. This table suggests that the actual impact of BNL enactment with a private right of action on data breach counts is larger (not smaller) than what might be observed by chance.

non-healthcare-related data breach incidents. Columns 9–12 do the same for data breach incidents not sourced from state attorney general offices.

Results across columns of Table 8 are consistent. There are no significant changes in data breach counts or magnitudes in these sub-samples compared to the full-sample results reported earlier. After implementing these empirical safeguards, we observe no demonstrable change in BNL (non-) effects. None of the 12 estimated coefficients for BNL effects approaches commonly accepted levels of statistical significance. All 12 are well within the Hartman and Hidalgo (2018) 36 percent threshold. Even the omission of results in Column 4 makes this point. There were too few healthcare-related breach incidents to estimate BNL effects for states with BNLs giving individuals a private right of action. These results suggest that increasing breadth in PRC data sources from 2005 to 2018 is quite unlikely to be biasing our core results. More broadly, results in Tables 3–8 and Figures 1 and 2 indicate the following: (1) BNL enactment does not significantly decrease data breaches whether

Table 8: Effect of BNLs on data breach counts and magnitudes with PRC data subsamples.

Dependent variable	**(1) ln(Records)**	**(2) ln(Records)**	**(3) numEvents**	**(4) numEvents**	**(5) ln(Records)**	**(6) ln(Records)**	**(7) numEvents**	**(8) numEvents**	**(9) ln(Records)**	**(10) ln(Records)**	**(11) numEvents**	**(12) numEvents**
Sample	**Health**	**Health**	**Health**	**Health**	**Non-health**	**Non-health**	**Non-health**	**Non-health**	**State AGs excluded**	**State AGs excluded**	**State AGs excluded**	**State AGs excluded**
Estimator	**Log-OLS**	**Log-OLS**	**Poisson**	**Poisson**	**Log-OLS**	**Log-OLS**	**Poisson**	**Poisson**	**Log-OLS**	**Log-OLS**	**Poisson**	**Poisson**
Treatment	**Any BNL**	**BNL w/PROA**	**Any BNL**	**BNL w/PROA**	**Any BNL**	**BNL w/PROA**	**Any BNL**	**BNL w/PROA**	**Any BNL**	**BNL w/PROA**	**Any BNL**	**BNL w/PROA**
Any BNL enacted	−0.449		−0.148		0.157		−0.0320		0.210		0.0482	
	(0.312)		(0.821)		(0.700)		(0.120)		(0.696)		(0.0843)	
BNL w/PROA enacted		−0.536		Omitted		0.733		0.142		0.749		−0.0672
		(0.281)				(0.967)		(0.346)		(0.963)		(0.217)
State fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 8: (continued)

Dependent variable	(1) ln(Records)	(2) ln(Records)	(3) numEvents	(4) numEvents	(5) ln(Records)	(6) ln(Records)	(7) numEvents	(8) numEvents	(9) ln(Records)	(10) ln(Records)	(11) numEvents	(12) numEvents
Sample	Health	Health	Health	Health	Non-health	Non-health	Non-health	Non-health	State AGs excluded	State AGs excluded	State AGs excluded	State AGs excluded
Estimator	Log-OLS	Log-OLS	Poisson	Poisson	Log-OLS	Log-OLS	Poisson	Poisson	Log-OLS	Log-OLS	Poisson	Poisson
Treatment	Any BNL	BNL w/PROA	Any BNL	BNL w/PROA	Any BNL	BNL w/PROA	Any BNL	BNL w/PROA	Any BNL	BNL w/PROA	Any BNL	BNL w/PROA
Observations	765	765	220	220	765	765	765	765	765	765	765	765
R-squared	0.452	0.452			0.542	0.543			0.537	0.538		

Table 8 presents coefficient estimates, standard errors (in parentheses) and asterisked (*) indicators of statistical significance for 12 panel difference-in-difference regression estimations assessing the impact of BNL enactments on annual data breach counts and magnitudes. We use breach data from the PRC (2022) for these estimations. The dependent variable in Columns 1–2 is the natural log of healthcare-related (Health) records breached in state *j* during year *t* from 2005 to 2019. The dependent variable in Columns 3–4 is the count of healthcare-related data breach incidents (no matter the number of records breached) in state *j* during year *t* from 2005 to 2019. The dependent variable in Columns 5–6 is the natural log of non-healthcare-related (Non-Health) records breached in state *j* during year *t* from 2005 to 2019. The dependent variable in Columns 7–8 is the count of non-healthcare-related data breach incidents (no matter the number of records breached) in state *j* during year *t* from 2005 to 2019. The dependent variable in Columns 9–10 is the natural log of records not apparently sourced from state attorney general offices (State AGs Excluded) breached in state *j* during year *t* from 2005 to 2019. The dependent variable in Columns 11–12 is the count of data breach incidents (no matter the number of records breached) not apparently sourced from state attorney general offices in state *j* during year *t* from 2005 to 2019. The key independent variable in Columns 1, 3, 5, 7, 9, and 11 is a 0–1 indicator term equaling one when state *j* in year *t* has enacted any type of BNL. The key independent variable in Columns 2, 4, 6, 8, 10, and 12 is a 0–1 indicator term equaling one when state *j* in year *t* has enacted a BNL permitting a private right of action. Though not presented in Table 8, all estimations also include state and year fixed effects, that is, 0–1 indicator terms for 50 of 51 states and the District of Columbia as well as 14 of 15 years (2005–2019) studied. These results are available from the authors. All estimations use robust standard errors clustered on states. Levels of statistical significance for coefficient estimates are defined by the number of asterisks: $^{***} = p < 0.01$ (significant at the 1 percent level); $^{**} = p < 0.05$ (significant at the 5 percent level); and $^{*} = p < 0.10$ (significant at the 10 percent level). The absence of asterisks on coefficient estimates means that they are not different from zero at commonly accepted levels of statistical significance. This table suggests that BNLs generally and BNLs with private rights of action significantly decrease neither data breach counts nor magnitudes of healthcare-related and other non-state-related data breach incidents.

measured as counts or magnitudes and whether caused internally or externally; and (2) BNL null effects are generally estimated with precision.

4.5 OLS and Poisson Regression Results for Identity Theft and Fraud

These core findings are consistent with the position that BNLs have neither curbed data breaches nor developed a market for data privacy where firms can choose deterrence levels and consumers can observe and respond to those choices. This is distressing as BNLs are the primary tool state legislators have put forward to curb data breaches and legislative histories explicitly belabor the need to resolve this growing problem. Yet, critics might respond that BNLs have a more limited aim. They are supposed to deter related data misuse due to, say, identity theft or fraud. Data breaches are not themselves problematic. It is the combination of data breaches and then misuse of breached data by malicious actors. Thus, the motivation for BNLs is data crime rather than data breach decrease. And timely notice of data breaches is related to whether consumers can take timely reparative actions to avoid victimization by malicious actors. For example, timely notice of breaches in their credit card data would give the credit card holders opportunities to cancel credit cards and freeze credit reports before misuse by malicious actors.

Evidence from prior published studies at state (Kesari 2022a) and national levels (Romanosky, Telang, and Acquisti 2011) suggests that BNLs may decrease incidences of identity theft. The one published national study is based on data from the 2000s when, as Table 1 indicates, the wave of BNL enactments was still building. We can re-evaluate this evidence after BNL enactments across all states. We can also evaluate this evidence after the substantial evolution of identity theft and fraud practices in the 2010s (Gupta 2018; Irshad and Soomro 2018; Steel 2019). That decade saw larger and more sophisticated instances of identity theft and fraud (Gupta 2018). It also saw the development of markets for trading stolen identities through so-called dark web locations such as the Tor network (Steel 2019). Finally, it saw the rise of social media creating new public points where data might fall into the hands of malicious actors (Irshad and Soomro 2018). In this context, we should understand whether the initially suppressive effect of BNLs enacted in the 2000s had longer-term effects.

To do so, we draw on data from the FTC's Consumer Sentinel Network Data Book (FTC 2021) (FTC data). Used widely in prior work (Anderson 2019; Raval 2020; Romanosky, Telang, and Acquisti 2011), the FTC data provide information on incidents of identity theft and fraud in each state. Consistent with our prior approach, we collect information on these incidences for all states from 2005 to 2019. Unlike data from the PRC, we have no information on the underlying cause of such data

misuse. We simply know that a theft or claim of fraud was reported in a given state and year. We therefore estimate the effect using the log of files misused using OLS regression and the count of misuse incidences, no matter the number of files involved, using Poisson regression. These two dependent variable measures parallel the data breach count and magnitude measures.

We first replicate prior work by Romanosky and colleagues (2011) documenting that BNLs enacted from 2005 to 2010 decreased incidents of identity theft. Replication study results are reported in Table 9. OLS regression of logged identity fraud magnitudes following BNL enactment during the same time-period yields the same negative sign (−0.0514) significant at the five percent level ($p < 0.05$). These results suggest a concordance of data and methods, thus increasing confidence in follow-on study of longer-run effects reported in Tables 10 and 11.

Table 9: Replication of Romanosky and Colleagues (2011) restricting FTC data to 2005–2010.

Dependent variable	**(1)**
Estimator	**ln(ID theft)**
Sample	**Log-OLS**
Treatment	**2005–2010**
	Any BNL
Any BNL enacted	−0.0524**
	(0.0209)
State fixed effects	Yes
Year fixed effects	Yes
Observations	306
R-squared	0.997
Number of groups	51

Table 9 presents a coefficient estimate, standard error (in parentheses) and an asterisked (*) indicator of statistical significance for a panel difference-in-difference linear regression estimation assessing the impact of BNL enactments on annual identity theft magnitudes. We use data from the FTC's Consumer Sentinel Network Data Book (FTC 2021) for this estimation. The dependent variable in Column 1 is the natural log of identity thefts reported to the FTC from state *j* during year *t*. The key independent variable in Column 1 is a 0–1 indicator term equaling one when state *i* in year *t* has enacted any type of BNL. Though not presented in Table 9, this estimation also includes state and year fixed effects, that is, 0–1 indicator terms for 50 of 51 states and the District of Columbia as well as 5 of 6 years (2005–2010) studied. These results are available from the authors. This estimation uses robust standard errors clustered on states. The level of statistical significance for the coefficient estimate is defined by the number of asterisks: *** = $p < 0.01$ (significant at the 1 percent level); ** = $p < 0.05$ (significant at the 5 percent level); and * = $p < 0.10$ (significant at the 10 percent level). This table suggests that we are using substantially similar data and replicating substantially similar significant negative effects on identity theft magnitudes after BNL enactment as reported in Romanosky, Telang, and Acquisti (2011).

Table 10: Effect of BNLs on identity theft and fraud counts and magnitudes.

Dependent variable	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**
Estimator	**ln(ID theft)**	**ln(Fraud)**	**numTheft**	**numFraud**	**ln(ID theft)**	**ln(Fraud)**	**numTheft**	**numFraud**
Treatment	**Log-OLS**	**Log-OLS**	**Poisson**	**Poisson**	**Log-OLS**	**Log-OLS**	**Poisson**	**Poisson**
	Any BNL	**Any BNL**	**Any BNL**	**Any BNL**	**BNL w/PROA**	**BNL w/PROA**	**BNL w/PROA**	**BNL w/PROA**
Any BNL enacted	−0.031	−0.013	−0.055	0.173*				
	(0.028)	(0.057)	(0.066)	(0.075)				
BNL w/PROA enacted					−0.036	−0.125	0.015	−0.135
					(0.050)	(0.117)	(0.073)	(0.082)
State fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	765	765	765	765	765	765	765	765
R-squared	0.986	0.975			0.986	0.975		
Number of groups	51	51	51	51	51	51	51	51

Table 10 presents coefficient estimates, standard errors (in parentheses) and asterisked (*) indicators of statistical significance for eight panel difference-in-difference regression estimations assessing the impact of BNL enactments on annual identity theft and fraud counts and magnitudes. We use data from the FTC's Consumer Sentinel Network Data Book (FTC 2021) for these estimations. The dependent variable in Columns 1 and 5 is the natural log of identity thefts reported to the FTC from state *i* during year *t*. The dependent variable in Columns 2 and 6 is the natural log of frauds reported to the FTC from state *j* during year *t*. The dependent variable in Columns 3 and 7 is the count of identity theft incidents reported to the FTC (no matter the number of identities stolen) from state *i* during year *t*. The dependent variable in Columns 4 and 8 is the count of fraud incidents reported to the FTC (no matter the number of frauds committed) from state *i* during year *t*. The key independent variable in Columns 1–4 is a 0–1 indicator term equaling one when state *i* in year *t* has enacted any type of BNL. The key independent variable in Columns 5–8 is a 0–1 indicator term equaling one when state *i* in year *t* has enacted a BNL permitting a private right of action. Though not presented in Table 10, all estimations include state and year fixed effects, that is, 0–1 indicator terms for 50 of 51 states and the District of Columbia as well as 14 of 15 years (2005–2019) studied. These results are available from the authors. This estimation uses robust standard errors clustered on states. The level of statistical significance for coefficient estimates is defined by the number of asterisks: *** $= p < 0.01$ (significant at the 1 percent level); ** $= p < 0.05$ (significant at the 5 percent level); and * $= p < 0.10$ (significant at the 10 percent level). The absence of asterisks on coefficient estimates means that they are not different from zero at commonly accepted levels of statistical significance. This table suggests that BNLs generally and BNLs with private rights of action significantly decrease neither counts nor magnitudes of identity theft or fraud over the 15 years studied.

Table 11: Effect of BNLs on identity theft and fraud counts and magnitudes in relative time.

Dependent variable Estimator Treatment	(1) ln(ID theft) Log-OLS Any BNL	(2) ln(Fraud) Log-OLS Any BNL	(3) numTheft Poisson Any BNL	(4) numFraud Poisson Any BNL	(5) ln(ID theft) Log-OLS BNL w/PROA	(6) ln(Fraud) Log-OLS BNL w/PROA	(7) numTheft Poisson BNL w/PROA	(8) numFraud Poisson BNL w/PROA
Rel Time $t-4+$	−0.014	−0.138	−0.109	−0.262*				
	(0.074)	(0.146)	(0.197)	(0.121)				
Rel Time $t-4$	−0.024	−0.023	−0.021	−0.168**	−0.013	0.355*	−0.272**	0.214*
	(0.056)	(0.077)	(0.128)	(0.054)	(0.163)	(0.162)	(0.088)	(0.101)
Rel Time $t-3$	0.003	−0.048	0.075	−0.149*	−0.026	−0.017	−0.112	−0.011
	(0.039)	(0.055)	(0.064)	(0.076)	(0.067)	(0.058)	(0.066)	(0.038)
Rel Time $t-2$	0.025	0.048	0.218	0.020	0.041	0.140	−0.038	0.093
	(0.040)	(0.046)	(0.114)	(0.050)	(0.048)	(0.097)	(0.056)	(0.064)
Rel Time $t+1$	−0.033	−0.008	−0.098*	0.063	−0.007	−0.020	−0.002	0.008
	(0.021)	(0.036)	(0.046)	(0.051)	(0.020)	(0.056)	(0.017)	(0.028)
Rel Time $t+2$	−0.041	−0.028	−0.140*	0.017	0.004	−0.030	0.027	−0.015
	(0.024)	(0.048)	(0.067)	(0.040)	(0.029)	(0.071)	(0.027)	(0.037)
Rel Time $t+3$	−0.042	−0.073	−0.189*	−0.052	−0.008	−0.069	−0.002	−0.023
	(0.040)	(0.054)	(0.086)	(0.084)	(0.035)	(0.102)	(0.041)	(0.042)
Rel Time $t+4$	−0.074	−0.098	−0.249*	−0.074	−0.017	−0.085	−0.067	−0.080
	(0.047)	(0.053)	(0.101)	(0.070)	(0.036)	(0.088)	(0.062)	(0.052)
Rel Time $t+5$	−0.077	−0.071	−0.234*	−0.076	−0.035	−0.023	−0.074	−0.070
	(0.059)	(0.078)	(0.114)	(0.092)	(0.048)	(0.176)	(0.076)	(0.063)
Rel Time $t+6$	−0.082	−0.146*	−0.237	−0.092	−0.049	−0.103	−0.141	−0.175*
	(0.072)	(0.072)	(0.147)	(0.108)	(0.046)	(0.106)	(0.109)	(0.068)
Rel Time $t+7$	−0.083	−0.105	−0.293	−0.098	−0.009	−0.076	−0.122	−0.185
	(0.079)	(0.082)	(0.162)	(0.115)	(0.056)	(0.118)	(0.160)	(0.113)

Table 11: (continued)

Dependent variable	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**
Estimator	**ln(ID theft)**	**ln(Fraud)**	**numTheft**	**numFraud**	**ln(ID theft)**	**ln(Fraud)**	**numTheft**	**numFraud**
Treatment	**Log-OLS**	**Log-OLS**	**Poisson**	**Poisson**	**Log-OLS**	**Log-OLS**	**Poisson**	**Poisson**
	Any BNL	**Any BNL**	**Any BNL**	**Any BNL**	**BNL w/PROA**	**BNL w/PROA**	**BNL w/PROA**	**BNL w/PROA**
Rel Time $t+8$	−0.086	−0.131	−0.279	−0.162	−0.024	−0.057	−0.060	−0.156
	(0.095)	(0.086)	(0.187)	(0.110)	(0.055)	(0.105)	(0.105)	(0.104)
Rel Time $t+9$	−0.065	−0.124	−0.278	−0.184	−0.015	−0.057	−0.085	−0.148
	(0.118)	(0.097)	(0.234)	(0.126)	(0.060)	(0.121)	(0.118)	(0.115)
Rel Time $t+10$	−0.099	−0.131	−0.352	−0.224	−0.012	−0.027	−0.128	−0.152
	(0.132)	(0.105)	(0.280)	(0.155)	(0.077)	(0.099)	(0.135)	(0.120)
Rel Time $t+10+$	−0.096	−0.124	−0.439	−0.203	0.066	−0.044	−0.008	−0.136
	(0.138)	(0.116)	(0.275)	(0.149)	(0.053)	(0.092)	(0.078)	(0.090)
State fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 11: (continued)

Dependent variable	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**
Estimator	**ln(ID theft)**	**ln(Fraud)**	**numTheft**	**numFraud**	**ln(ID theft)**	**ln(Fraud)**	**numTheft**	**numFraud**
Treatment	**Log-OLS**	**Log-OLS**	**Poisson**	**Poisson**	**Log-OLS**	**Log-OLS**	**Poisson**	**Poisson**
	Any BNL	**Any BNL**	**Any BNL**	**Any BNL**	**BNL w/PROA**	**BNL w/PROA**	**BNL w/PROA**	**BNL w/PROA**
Observations	765	765	765	765	765	765	765	765
R-squared	0.986	0.976			0.986	0.976		

Table 11 presents coefficient estimates, standard errors (in parentheses) and asterisked (*) indicators of statistical significance for four semi-parametric panel regression estimations assessing pre- and post-BNL enactment trends in annual data breach identity theft and fraud counts and magnitudes. We use data from the FTC's Consumer Sentinel Network Data Book (FTC 2021) for these estimations. The dependent variable in Columns 1 and 5 is the natural log of identity thefts reported to the FTC from state *j* during year *t*. The dependent variable in Columns 2 and 6 is the natural log of frauds reported to the FTC from state *j* during year *t*. The dependent variable in Columns 3 and 7 is the count of identity theft incidents reported to the FTC (no matter the number of identities stolen) from state *j* during year *t*. The dependent variable in Columns 4 and 8 is the count of fraud incidents reported to the FTC (no matter the number of frauds committed) from state *j* during year *t*. The key independent variable in Columns 1–4 is a 0–1 indicator term equaling one for state *j* in successive years prior to (*e.g.*, $t-3$) and after (*e.g.*, $t+3$) enactment of any type of BNL in year $t=0$. The key independent variable in Columns 5–8 is a 0–1 indicator term equaling one for state *j* in successive years prior to and after enactment of a BNL permitting a private right of action in year $t=0$. Though not presented in Table 11, all estimations also include state and year fixed effects, that is, 0–1 indicator terms for 50 of 51 states and the District of Columbia as well as 14 of 15 years (2005–2019) studied. These results are available from the authors. All panel estimations use robust standard errors clustered on states. Levels of statistical significance for coefficient estimates are defined by the number of asterisks: *** $= p < 0.01$ (significant at the 1 percent level); ** $= p < 0.05$ (significant at the 5 percent level); and * $= p < 0.10$ (significant at the 10 percent level). The absence of asterisks on coefficient estimates means that they are not different from zero at commonly accepted levels of statistical significance. This table suggests that there are no persistently significant identity theft or fraud trends linked to the run-up to or aftermath of BNL enactment.

Table 10 reports results from OLS and Poisson regression of identity theft and fraud incident counts and magnitudes following BNL enactment from 2005 to 2019. Results indicate no significant negative BNL enactment effects. Indeed, we observe in Column 4 a positive (not negative) effect of BNL enactment coefficient (0.174) significant at the 10 percent level ($p < 0.10$). The count of fraud incidents in a state *increased* after enactment of a BNL. Comparison of the estimated coefficients to the Hartman and Hidalgo (2018) thresholds also suggest precisely estimated nulls except in the case of the Column 4 coefficient. Excepting the Column 4 coefficient, *p*-values for others are nowhere near conventional thresholds of significance (averaging at $p = 0.4551$).

Table 11 reports on pre-treatment and post-treatment trends. We observe some initial declines (Column 3) in the number of thefts when the effect is estimated semi-parametrically, but these effects do not appear to persist in the long term. Moreover, there do not appear to be any persistent pre-treatment trends across the estimations, suggesting no substantial violation of the parallel trends assumption.

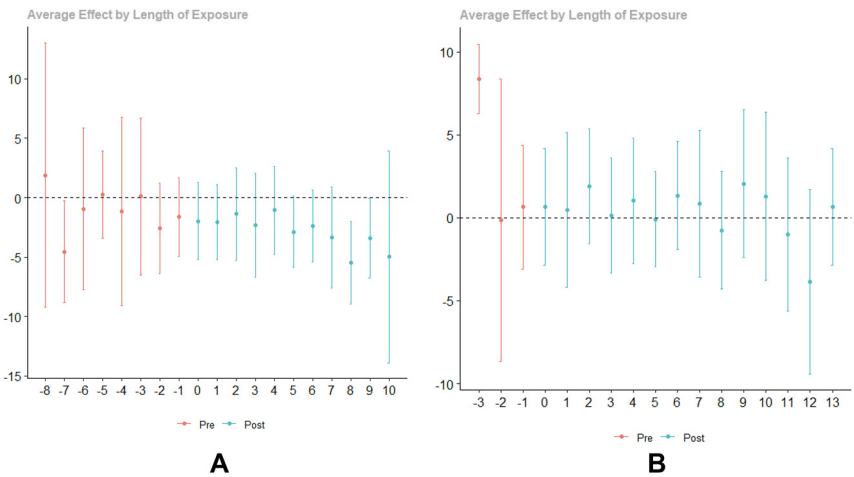

Figure 3: Figure 3A is graphical output of Callaway and Sant'Anna (2021) difference-in-difference estimation for any BNL. Figure 3B is graphical output of Callaway and Sant'Anna (2021) difference-in-difference estimation for BNLs permitting a private right of action. Figure 3A and B both depict weighted pre- and post-treatment trend estimates derived from panel linear difference-in-difference regression estimation (magnitudes) in Table 10, Column 1 (Figure 3A) and Column 5 (Figure 3B) with five percent ($p < 0.05$) confidence intervals for the log of annual identity thefts reported to the FTC from states *i* over 19 years pre- and post-enactment of any BNL (Figure 3A) and over 17 years pre- and post-enactment of BNLs permitting a private right of action (Figure 3B). Estimates with confidence interval lines crossing the zero line are not significantly different from zero at the five percent level. We use breach data from the PRC (2022) for these estimations. These figures suggest no persistently significant pre- or post-BNL enactment trends affecting identity thefts.

We replicate the effect over time for identity theft magnitudes using the Callaway and Sant'Anna (2021) approach. Results in Figure 3A and B corroborate both the lack of persistent significant effect and the absence of significant pre-treatment trends. Finally, we note that none of the estimated coefficients – even those that are significant at commonly-accepted levels – cross the effect size threshold suggested by Hartman and Hidalgo (2018). Taken together, these results indicate that BNLs have done little in the longer term to reduce data misuse.

4.6 Evaluating Alternative Explanations

While the above analyses constitute a broad basis for concluding that BNLs have had no meaningful effect on either data breaches or the follow-on misuse of breached data, our evidence is vulnerable to various rebuttals. Here are four: (1) BNLs may have had temporary early deterrence effects in the same way they had on incidences of identity theft; (2) BNLs may be effective in deterring data breaches in smaller firms operating across fewer, if any, state lines and less able to insulate top managers from liabilities imposed by BNLs; (3) BNLs may be effective in decreasing data breaches in firms when enacted with other state data security laws; and (4) BNLs with certain characteristics other than private rights of action may be effective in decreasing data breaches. We briefly discuss and then investigate evidence related to each.

4.6.1 Early BNL Effects

As with identity theft, it may be that early BNL enactments decreased data breach counts and magnitudes, but later BNL enactments were meaningless as firms had already conformed to earlier BNL enactments, including the initial BNL enactment in California in 2003. While we see no evidence of this trend in our relative time estimations, it may still be observable across time in panel difference-in-differences regression estimations.

Along these lines, Table 12 replicates our OLS and Poisson estimations using two data sub-samples. The first is 2005–2015 (Columns 1–4), the second is 2005–2010 (Columns 5–8). The intuition behind this sub-sampling strategy is straightforward. By shaving years off the end of the sample we are better able to capture effects from earlier BNL enactments. Results across all columns of Table 12 indicate no significant decrease in data breach counts or magnitudes following BNL enactment. Though not reported here, we also find no pre-treatment trends.[7] This absence of

7 These results are available from the authors.

Table 12: Effect of BNLs on data breach counts and magnitudes based on alternative time-periods.

Dependent variable	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**
Sample	**ln(Records)**	**ln(Records)**	**numEvents**	**numEvents**	**ln(Records)**	**ln(Records)**	**numEvents**	**numEvents**
Estimator	**2005–2015**	**2005–2015**	**2005–2015**	**2005–2015**	**2005–2010**	**2005–2010**	**2005–2010**	**2005–2010**
Treatment	**Log-OLS**	**Log-OLS**	**Poisson**	**Poisson**	**Log-OLS**	**Log-OLS**	**Poisson**	**Poisson**
	Any BNL	**BNL w/PROA**	**Any BNL**	**BNL w/PROA**	**Any BNL**	**BNL w/PROA**	**Any BNL**	**BNL w/PROA**
Any BNL enacted	0.151		−0.016		0.154		0.081	
	(0.684)		(0.127)		(0.797)		(0.127)	
BNL w/PROA enacted		0.945		0.226		0.551		−0.053
		(0.971)		(0.366)		(0.997)		(0.219)
State fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	561	561	561	561	306	306	306	306
R-squared	0.535	0.537			0.593	0.594		

Table 12 presents coefficient estimates, standard errors (in parentheses) and asterisked (*) indicators of statistical significance for eight panel difference-in-difference regression estimations assessing the impact of BNL enactments on annual data breach counts and magnitudes. We use breach data from the PRC (2022) for these estimations. The dependent variable in Columns 1–2 and 5–6 is the natural log of records breached in state *j* during year *t* over the first 11 years (2005–2015) of our study (Columns 1–2) or over the first 6 years (2005–2010) of our study (Columns 5–6). The dependent variable in Columns 3–4 and 7–8 is the count of data breach incidents (no matter the number of records breached) in state *j* during year *t* over the first 11 years (2005–2015) of our study (Columns 3–4) or over the first 6 years (2005–2010) of our study (Columns 7–8). The key independent variable in Columns 1, 3, 5, and 7 is a 0–1 indicator term equaling one when state *j* in year *t* has enacted any type of BNL. The key independent variable in Columns 2, 4, 6, and 8 is a 0–1 indicator term equaling one when state *j* in year *t* has enacted a BNL permitting a private right of action. Though not presented in Table 12, all estimations also include state and year fixed effects, that is, 0–1 indicator terms for 50 of 51 states and the District of Columbia as well as 14 of 15 years (2005–2019) studied. These results are available from the authors. All estimations use robust standard errors clustered on states. Levels of statistical significance for coefficient estimates are defined by the number of asterisks: $^{***} = p < 0.01$ (significant at the 1 percent level); $^{**} = p < 0.05$ (significant at the 5 percent level); and $^{*} = p < 0.10$ (significant at the 10 percent level). The absence of asterisks on coefficient estimates means that they are not different from zero at commonly accepted levels of statistical significance. This table suggests that BNLs generally and BNLs with private rights of action significantly decrease neither data breach counts nor magnitudes in the earlier years of BNL enactment.

an effect is especially interesting given previous evidence that follow-on incidents of identity theft did decrease temporarily after enactment of BNLs in early moving states. Taken together, these results suggest that early BNL enactments did not deter firms from data breaches even if they did temporarily deter data misuse by malicious actors after those breaches.

4.6.2 Smaller Firm BNL Effects

Another possibility is that successive BNL enactments decrease data breaches only in smaller firms operating in one or a few states rather than in larger firms operating nationally. Larger firms typically have broader geographic operational scope. Social media giants like Google or manufacturing firms like 3M have customers in all 50 states. BNL enactment in any state will implicate their customers. In contrast, a smaller firm operating in one or only a few states may have customers and data records only in those states. Until BNLs are enacted there, incentives to reduce data breaches may be insufficient.[8]

We investigate this empirically by creating a sub-sample of firms that are not part of the S&P 500, the 500 largest companies listed on public exchanges in the US. Our assumption is that these firms are smaller and more likely to be operating in only one or a few surrounding states. Thus, they are less likely to respond to early BNL enactment in any state and more likely to respond only when BNLs are enacted in their state of domicile or in surrounding ones. We then replicate our OLS and Poisson estimations. Results in Table 13 again indicate no significant decrease in data breach counts or magnitudes. Though not reported here, we also find no pre-treatment trends.[9] This evidence suggests that smaller firms are no more likely to deter data breaches following BNL enactment than larger firms.[10]

---

8 A related justification for re-estimating with smaller firms may relate to incentives and insurance. Baker and Griffith (2007) opine that senior executives and board members may be slow to address legal miscues in their firms if they are insulated from those miscues by often overly generous levels of coverage in their Directors & Officers (D&O) insurance policies. Larger firms may have higher D&O policy limits and enjoy great bargaining power to cajole or coerce coverage in the event of a data breach, thus lessening incentives to decrease data breaches after BNL enactments. On the other hand, larger firms are more likely to have brand name capital at stake, be publicly traded, and have in place different governance mechanisms to punish senior executives and board members for BNL violations.

9 These results are available from the authors.

10 This evidence is also responsive to earlier discussion of PRC data and their potential for misattribution large data breach magnitudes. Consistent BNL (non-) effects on data breach magnitudes for smaller firms suggests that any misattribution of data breach magnitudes in the PRC data is not biasing our core results.

Table 13: Effect of BNLs on data breach counts and magnitudes for non-S&P 500 firms.

Dependent variable **Estimator** **Treatment**	**(1)** **ln(Records)** **Log-OLS** **Any BNL**	**(2)** **ln(Records)** **Log-OLS** **BNL w/PROA**	**(3)** **numEvents** **Poisson** **Any BNL**	**(4)** **numEvents** **Poisson** **BNL w/PROA**
Any BNL enacted	0.067		−0.052	
	(0.702)		(0.114)	
BNL w/PROA enacted		0.678		0.104
		(0.939)		(0.340)
State fixed effects	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes
Observations	765	765	765	765
R-squared	0.535	0.535		

Table 13 presents coefficient estimates, standard errors (in parentheses) and asterisked (*) indicators of statistical significance for four panel difference-in-difference regression estimations assessing the impact of BNL enactments on annual data breach counts and magnitudes. We use a sub-sample of breach data from the PRC (2022) for these estimations. We exclude any observations involving firms ever listed in the S&P 500. The dependent variable in Columns 1–2 is the natural log of records breached in state *j* during year *t*. The dependent variable in Columns 3–4 is the count of data breach incidents (no matter the number of records breached) in state *j* during year *t*. The key independent variable in Columns 1 and 3 is a 0–1 indicator term equaling one when state *j* in year *t* has enacted any type of BNL. The key independent variable in Columns 2 and 4 is a 0–1 indicator term equaling one when state *j* in year *t* has enacted a BNL permitting private rights of action. Though not presented in Table 13, all estimations also include state and year fixed effects, that is, 0–1 indicator terms for 50 of 51 states and the District of Columbia as well as 14 of 15 years (2005–2019) studied. These results are available from the authors. All estimations use robust standard errors clustered on states. Levels of statistical significance for coefficient estimates are defined by the number of asterisks: $^{***} = p <$ 0.01 (significant at the 1 percent level); $^{**} = p < 0.05$ (significant at the 5 percent level); and $^{*} = p <$ 0.10 (significant at the 10 percent level). The absence of asterisks on coefficient estimates means that they are not different from zero at commonly accepted levels of statistical significance. This table suggests that BNLs generally and BNLs with private rights of action significantly decrease neither data breach counts nor magnitudes even after we exclude the largest publicly listed firms.

4.6.3 BNL Effects After Enactment of Other State Data Security Laws

BNLs are not the only type of data security law that states have been enacting, albeit the most popular. Others enacted in many states during this same time-period regulate security arrangements for personal data held by firms and state agencies, and regulate data disposal by firms and public agencies. These other security laws were not necessarily enacted in the same years that BNLs were enacted. In this context, it could be that BNLs alone have little or no data breach deterrence effect until

combined with other data security laws defining standards for data security and disposal. Such a possibility is not unreasonable, notably as it is often challenging to demonstrate negligence absent an explicit set of statutory requirements for data handling.

To investigate such a possibility, we collect information on enactment dates for three other US state data security laws from the National Conference of State Legislatures (NCSL 2021). We then replicate our OLS and Poisson estimations with three additional 0–1 indicator terms equaling one in years *t* when these other data security laws have been enacted in states *j*: (1) Firm Data Security Law Enacted; (2) Agency Data Security Law Enacted; and (3) Data Disposal Law Enacted. Results in Table 14 suggest that enactment of BNLs and these other data security laws did not significantly decrease data breach counts or magnitudes. These findings extend our criticism of BNLs to the broader regime of state data security laws. The broader state-based data security legal regime appears to be as toothless as BNLs appear to be.

4.6.4 BNL Effects and Other BNL Characteristics

Table 1 shows that BNLs like Connecticut's require notification when data are accessed without authorization. Others like Delaware's require notification when data is acquired by someone lacking authorization. All BNLs require firms to notify individuals when their data has been breached, but some like Hawaii's require notification of data "owners" that might also have rights to the use of these data. Others like Idaho's require the same notification to the state's attorney general. Still others like Maryland's require individual, owner, and attorney general notification, and give private rights of action to individuals and owners. Our earlier OLS and Poisson regression results did not account for these other differences. We only accounted for BNLs with any type of private right of action.

Our fourth investigation goes further. We assess the impact of BNLs with other coverage dimensions including notification triggers based on unauthorized data access, notification triggers based on unauthorized data acquisition, post-breach individual notification requirements, post-breach owner notification requirements, and post-breach attorney general notification requirements. To do so, we deem BNLs enacted in state *j* in year *t* only when they include terms for: Access Protocol (Columns 1, 6); Acquisition Protocol (Columns 2, 7); Individual Notification (Columns 3, 8); Owner Notification (Columns 4, 9); and AG Notification (Columns 5, 10). Results across all 10 columns of Table 15 again reveal no significant negative effects on data breach counts or magnitudes when BNL enactment is based on any of these different coverage dimensions. Though not reported here,

Table 14: Effect of BNLs on data breach counts and magnitudes given other state data laws.

Dependent variable **Estimator** **Treatment**	**(1)** **ln(Records)** **Log-OLS** **Any BNL**	**(2)** **ln(Records)** **Log-OLS** **BNL w/PROA**	**(3)** **numEvents** **Poisson** **Any BNL**	**(4)** **numEvents** **Poisson** **BNL w/PROA**
Any BNL enacted	0.301		−0.073	
	(0.815)		(0.132)	
BNL w/PROA enacted		0.941		0.142
		(0.934)		(0.317)
Firm data security law enacted	−0.232	−0.128	0.050	0.014
	(0.749)	(0.677)	(0.101)	(0.084)
Agency data security law enacted	0.728	0.752	0.284	0.290
	(0.577)	(0.586)	(0.218)	(0.217)
Data disposal law enacted	−0.287	−0.384	0.027	−0.010
	(0.771)	(0.701)	(0.120)	(0.100)
State fixed effects	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes
Observations	765	765	765	765
R-squared	0.544	0.545		

Table 14 presents coefficient estimates, standard errors (in parentheses) and asterisked (*) indicators of statistical significance for four panel difference-in-difference regression estimations assessing the impact of BNL enactments on annual data breach counts and magnitudes after controlling specifically for three other US state data security laws enacted in many states during the same time-period: (1) a law regulating data security for firms and other non-state governmental agencies; (2) a law doing the same for state governmental agencies; and (3) a law regulating the disposal of data for firms and other non-state governmental agencies and state governmental agencies. We use breach data from the PRC (2022) for these estimations. We exclude any observations involving firms ever listed in the S&P 500. The dependent variable in Columns 1–2 is the natural log of records breached in state *j* during year *t*. The dependent variable in Columns 3–4 is the count of data breach incidents (no matter the number of records breached) in state *j* during year *t*. The key independent variable in Columns 1 and 3 is a 0–1 indicator term equaling one when state *j* in year *t* has enacted any type of BNL. The key independent variable in Columns 2 and 4 is a 0–1 indicator term equaling one when state *j* in year *t* has enacted a BNL permitting private rights of action. We include similar 0–1 indicator terms equaling one when state *i* in year *t* has enacted laws (1) (Firm Data Security Law Enacted), (2) (Agency Data Security Law Enacted), and or (3) (Data Disposal Law Enacted) during the same time-period. Though not presented in Table 14, all estimations also include state and year fixed effects, that is, 0–1 indicator terms for 50 of 51 states and the District of Columbia as well as 14 of 15 years (2005–2019) studied. These results are available from the authors. All estimations use robust standard errors clustered on states. Levels of statistical significance for coefficient estimates are defined by the number of asterisks: $^{***} = p < 0.01$ (significant at the 1 percent level); $^{**} = p < 0.05$ (significant at the 5 percent level); and $^{*} = p < 0.10$ (significant at the 10 percent level). The absence of asterisks on coefficient estimates means that they are not different from zero at commonly accepted levels of statistical significance. This table suggests that BNLs generally and BNLs with private rights of action significantly decrease neither data breach counts nor magnitudes even after other state data security laws are enacted. This table also suggests that the other state data security laws were themselves ineffective at decreasing data breach counts or magnitudes.

Table 15: Effect of BNLs on data breach counts and magnitudes based on alternative definitions of treatment.

Dependent variable	**(1) ln(Records)**	**(2) ln(Records)**	**(3) ln(Records)**	**(4) ln(Records)**	**(5) ln(Records)**	**(6) numEvents**	**(7) numEvents**	**(8) numEvents**	**(9) numEvents**	**(10) numEvents**
Estimator	**Log-OLS**	**Log-OLS**	**Log-OLS**	**Log-OLS**	**Log-OLS**	**Poisson**	**Poisson**	**Poisson**	**Poisson**	**Poisson**
Treatment	**BNL w/access protocol**	**BNL w/acquisition protocol**	**BNL w/individual notification**	**BNL w/owner notification**	**BNL w/AG notification**	**BNL w/access protocol**	**BNL w/acquisition protocol**	**BNL w/individual notification**	**BNL w/owner notification**	**BNL w/AG notification**
Access protocol	1.292					−0.144				
	(1.199)					(0.112)				
Acquisition protocol		0.147					−0.039			
		(0.699)					(0.117)			
Individual notification			0.166					−0.041		
			(0.697)					(0.117)		
Owner notification				0.442					0.021	
				(0.762)					(0.136)	
AG notification					0.246					0.023
					(0.966)					(0.157)
State fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 15: (continued)

Dependent variable Estimator Treatment	(1) ln(Records) Log-OLS BNL w/access protocol	(2) ln(Records) Log-OLS BNL w/acquisition protocol	(3) ln(Records) Log-OLS BNL w/individual notification	(4) ln(Records) Log-OLS BNL w/owner notification	(5) ln(Records) Log-OLS BNL w/AG notification	(6) numEvents Poisson BNL w/access protocol	(7) numEvents Poisson BNL w/acquisition protocol	(8) numEvents Poisson BNL w/individual notification	(9) numEvents Poisson BNL w/owner notification	(10) numEvents Poisson BNL w/AG notification
Observations	765	765	765	765	765	765	765	765	765	765
R-squared	0.545	0.543	0.543	0.543	0.544					
Number of groups	51	51	51	51	51	51	51	51	51	51

Table 15 presents coefficient estimates, standard errors (in parentheses) and asterisked (*) indicators of statistical significance for 10 panel difference-in-difference regression estimations assessing the impact of BNL enactments on annual data breach counts and magnitudes. We use breach data from the PRC (2022) for these estimations. The dependent variable in Columns 1–5 is the natural log of records breached in state *j* during year *t*. The dependent variable in Columns 5–8 is the count of data breach incidents (no matter the number of records breached) in state *j* during year *t*. The key independent variable in Columns 1 and 6 is a 0–1 indicator term equaling one when state *j* in year *t* has enacted a BNL with notification requirements triggered by unauthorized access to data. The key independent variable in Columns 2 and 7 is a 0–1 indicator term equaling one when state *j* in year *t* has enacted a BNL with notification requirements triggered by unauthorized acquisition of (not mere access to) data. The key independent variable in Columns 3 and 8 is a 0–1 indicator term equaling one when state *j* in year *t* has enacted a BNL requiring notification of individuals – often state resident individuals – whose data has been breached. The key independent variable in Columns 4 and 9 is a 0–1 indicator term equaling one when state *j* in year *t* has enacted a BNL requiring notification of breached data "owners" – often state resident firms with rights to use the data for business purposes and to sell those rights to others. The key independent variable in Columns 5 and 10 is a 0–1 indicator term equaling one when state *j* in year *t* has enacted a BNL requiring notification of state attorney general. Though not presented in Table 15, all estimations also include state and year fixed effects, that is, 0–1 indicator terms for 50 of 51 states and the District of Columbia as well as 14 of 15 years (2005–2019) studied. These results are available from the authors. All estimations use robust standard errors clustered on states. Levels of statistical significance for coefficient estimates are defined by the number of asterisks: $^{***} = p < 0.01$ (significant at the 1 percent level); $^{**} = p < 0.05$ (significant at the 5 percent level); and $^{*} = p < 0.10$ (significant at the 10 percent level). The absence of asterisks on coefficient estimates means that they are not different from zero at commonly accepted levels of statistical significance. This table suggests that BNLs with these different characteristics significantly decrease neither data breach counts nor magnitudes.

we also find no pre-treatment trends.[11] No matter how we define BNL enactment, it fails to decrease data breach counts or magnitudes.

5 Discussion

5.1 Key Research Questions and Findings

Recall the motivation for this study. Fifty one different BNLs comprise the main public deterrent to data breaches affecting millions of consumers each year. And notification requirements under state BNLs disclose information that could help develop a market for data privacy firms could then use to signal consumers about data security quality and cost. We asked whether BNLs actually deter data breaches and promote development of that market for data privacy.

Our analyses consistently suggest not. From 2005 to 2019, BNLs significantly reduced neither data breach counts nor magnitudes, neither generally nor for specific types of BNLs. BNL enactments from 2005 to 2019 also failed in the longer-term to significantly reduce follow-on data misuse by malicious actors. Our null findings followed from well-calibrated empirical methods designed to detect causal effects from BNLs. Our null findings appear to have been precisely estimated.

5.2 Implications for Research, Practice, and Public Policy

5.2.1 Implications for Research

Our null findings matter for many groups, starting with researchers studying BNLs. We provide the first evidence of apparent BNL ineffectiveness in reducing data breach counts and magnitudes based on broad-sample statistical analysis across all states over nearly the entire period of BNL enactments. This constitutes a substantial advance on anecdotal or single state-based (*e.g.*, Park 2019) evidence. We reinforce skepticism about BNL effectiveness (Joerling 2010; Nieuwesteeg 2017; Peters 2014) and push back on other evidence suggesting some BNL effectiveness in reducing the malicious use of breached data (Kesari 2022a,b; Romanosky, Telang, and Acquisti 2011).

5.2.2 Implications for Practice and Public Policy

Our null findings also matter for various policymakers writing and enforcing current BNLs as well as executives and professionals in law, business, and

11 These results are available from the authors.

information technology coping with them. The apparent ineffectiveness of BNLs at curbing data breaches begs the question: Why? Cybersecurity consultants and insurers tout multimillion-dollar costs and months-long timelines to identify and contain instances of substantial data breach at US-based firms. In 2021, cybersecurity service providers at IBM set the average data breach incident cost at $9.05 million and average timeline for data breach incident identification and containment at 287 days (IBM 2021). But details regarding costs and inconveniences mention neither BNLs nor their related triggers, notification requirements, prospective state investigations, penalties, civil suits, or publication mandates.

It could be that BNLs add little to other much stronger business and legal deterrents to data breaches. A notorious hack of credit card files in late 2013 at the Minneapolis-based retailer Target led to data breaches affecting an estimated 70 million customers. Target incurred multimillion-dollar liabilities to those credit card customers. But a substantial share of the estimated $248 million to $2.2 billion in business and legal costs Target paid also went to other credit card industry businesses victimized by the hack: banks and financing companies, and payments network providers. BNL provisions likely made little difference to notification speed for those businesses (Weiss and Miller 2015).

On the other hand, there is little doubt that BNL notification requirements have led to more notices to consumers of smaller scale data breaches sooner than they would otherwise receive. And there is some evidence that consumers have responded with, for example, greater willingness to pay for credit monitoring services to guard against malicious data use after breaches (Peters 2014). But such measures indicate a shift in the cost of data breaches to consumers rather than internalization by firms or their insurers to encourage fewer data breaches.[12] We noted earlier that 2003–2019 saw development of differing standards for standing to bring data breach lawsuits in federal courts. Even where those standards were more permissive, consumers still face significant challenges in civil tort cases requiring the establishment of causation between breach events and individual damages. Credit monitoring service purchases may be less costly and more immediate non-judicial remedies. Some combination of BNL-prompted cost-shifting to affected consumers and superfluousness to affected businesses may explain the failure of BNLs to prompt more data security vigilance among firm executives and professionals.

12 Even if insurers sought to give data security practices of insured firms closer scrutiny after breach notification, their efforts may be undermined by insured firm breach response teams including outside law firm personnel able to shield important data security practices from insurers and others using attorney-client privilege protections. Schwarcz, Wolff, and Woods 2023 discuss such practices and legal reforms to curb them.

What about the policy makers who are writing and enforcing BNLs? Recall again their aims. BNLs were supposed to decrease data breaches and promote the creation of a market for data privacy where firms could position themselves based on quality and cost. We just noted two reasons why BNL deterrents may have been insufficient to prompt a significant reduction in data breach counts and magnitudes. The market motivation for BNLs might still be effective if standards defined product quality and cost consistently, and if consumers had accessible information to understand where firms positioned themselves regarding those standards. The current set of BNLs seem to be doing neither. Tom (2010: 1570) describes BNL variations as "so numerous that it is virtually impossible to convert these state laws into the more manageable format . . . " Even basic standards about notification are inconsistent. For firms doing business with customers in three different states, a given data breach could easily prompt review of three different notification triggers for three different potential recipients mandating three different types of notification information.

Even if there were consistent standards, the current set of BNLs seem inadequate to the task of providing consumers with accessible information regarding where firms have positioned themselves on data security quality and cost dimensions. By mid-2021, only 19 of the 51 BNL regimes published an archive of data breach incidents accessible to consumers (IAPP 2021). These archives provide little information on any given incident and then with substantial variation in information across archives. A data breach at Volkswagen America and Audi America (VWA) discovered in March 2021 exposed the PII of more than three million customers located throughout the US. Malicious actors likely put some of these data up for sale on the dark web. VWA started filing notifications under various state BNLs in June 2021. Aside from affected actual and potential VWA car owners, millions of consumers in 32 states without any BNL publication archives had little reason to know of the data breach incident, let alone understand how to assess VWA's response.

Consumers in 19 states with published archives in 2021 likely fared no better. Archives with no information about the VWA incident included Hawaii, Maryland, Montana, Oklahoma, Oregon, Texas, Washington State, and Wisconsin. Archives in California, Delaware, Iowa, Indiana, Maine, Maryland, Massachusetts, New Hampshire, North Dakota, New Jersey, and Vermont did note the VWA incident, but with varying information quality: Indiana's archive comprised a single line item listing the date notification was sent (June 11, 2021), the number of state residents affected (875), and the "total" number of individuals affected (90,184); North Dakota's archive provided samples of data breach notification forms sent by VWA to affected consumers as well as a cover letter from VWA's lawyers to the state attorney general describing the incident and mitigating actions VWA was taking; New Jersey's

archive summarized data breach details in a short paragraph with a hyperlink directing viewers to the *Maine* archive for additional detail.

There is little consistency in the presentation of firm breach event information. There is little guidance about how to assess firm breach event response.[13] This troubling combination strikes us as yet another example of an inadequate, perhaps even counter-productive mandated disclosure regime (Ben-Shahar and Schneider 2011). Here, the problem relates to mandated data collection often costly to businesses and data presentation often overly detailed to consumers. Businesses typically respond with selective compliance to contain costs, while consumers respond with selective review given limited time and evaluative expertise. With more than 50 different BNLs and 19 different public archives, businesses have strong incentives to limit the extent of data collection and submission to so many different recipients and outlets. With so many different forms of publicly available data presentation, consumers have strong incentives to, at best, browse or simply ignore disclosed breach event information. Both incentives undermine intended disclosure regime goals.

Obvious public policy responses include a revamp of state BNLs to provide consistent data collection and presentation standards, or single federal-level BNL to provide uniform standards and more resources to enforce them. Along with many other research and public policy commentators (Peters 2014; Stevens 2015; Tom 2010), we prefer the federal response. Along with standards setting, Congress could authorize the creation of an expert body drawn from information technology, legal services, business management, and consumer protection communities to propose, review, and regularly update data security and breach notification standards and best practices. That same body could also recommend sanctions for noncompliance creating substantially stronger deterrents – for example, strict liability with statutory where actual damages are difficult to prove, as well as court costs and attorneys' fees awards for consumers harmed by tardy notification.

At least two existing federal agencies have experience, expertise, and resources to implement such reforms. One is the FTC. It already plays an important role tracking and policing downstream misuse of breached data through its Consumer Sentinel Network Data program. Vesting oversight and enforcement of a federal BNL regime in the FTC would be a natural extension given this expertise and experience. As Cooper and Kobayashi (2022) point out, however, current FTC liability standards of "unreasonableness" in firm cybersecurity practices would likely merit change to the strict liability standard we advocate. Similarly, FTC enforcement power currently barring equitable monetary relief in the first instance of violation would also

13 The International Association of Privacy Professionals (IAPP 2021) publishes links to most online state archives we noted.

need reform so that the agency could impose monetary sanctions on first time as well as "nth time" violators proportionate to the harm those violations caused.

A second agency to consider is the SEC. We have already noted this agency's role in assuring adequate cybersecurity for publicly listed firms under SOX. The agency took yet another step towards such assurance in July 2023 with adoption of rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance (SEC 2023).[14] Vesting oversight and enforcement of a federal BNL regime for publicly listed firms in the SEC would be also a natural extension given its expertise, experience, and growing interest in these issues. With a broad range of oversight and enforcement mechanisms already at hand, the SEC might be able to implement most aspects of the federal BNL regime we have in mind for publicly listed firms far before the FTC could do the same for firms more generally. In due course, both agencies could administer a federal BNL regime with specialization tailored to firms and issues fitting broader agency goals.

Whether state or federal, mandated disclosure regimes often prove ineffective when consumers are overwhelmed with information for which they lack time and expertise to review and interpret (Ben-Shahar and Schneider 2011). One response to that concern is to engage consumer-oriented agencies and experts able to review, distill, and present mandated information in simplified forms permitting easier final consumer review and assessment. To that end, Congress could create a breach event publication system akin to the US Federal Aviation Administration's Airline Service Quality Performance System assessing on-time departure and arrival of airlines operating in the US (FAA 2021). A "Data Breach Deterrence and Security Assurance System" could publish and archive standard information on firm data breaches and mitigation efforts. Perhaps more importantly for consumers trying to assess firm performance, the system could also publish and publicize criteria for ordinally grading firm mitigation efforts, for example, on 1–10 or A–F bases. Agency staff might generate grades or outside organizations could be enlisted for that purpose. The SEC designates certain credit rating agencies (*e.g.*, Moody's Investor Services) as Nationally Recognized Statistical Rating Organizations to ordinally assess the ability and willingness of borrowers to meet their financial obligations (SEC 2021). Expert outside organizations like the American National Standards Institute might provide similar ordinal assessments as Nationally Recognized Data Breach Response Rating Organizations.[15] Policy responses of both types have ample

14 The SEC also adopted rules requiring foreign private issuers to make comparable disclosures.

15 An alternative model to consider is the HIPAA Reporting Tool maintained by the US Department of Homeland Security's Office of Civil Rights (HIPAA 2021). Also known as the "Wall of Shame," the

precedent (Freeman 2000) and could spur near-term development of a data privacy market that the state BNLs apparently failed to develop over nearly 20 years.

5.3 Limitations and Future Research Directions

Like any study, ours has limitations. We emphasize innovations in data and methods permitting causal inference about the (in)effectiveness of BNLs, but those data and methods are not bullet-proof. We have already noted limitations of PRC data for some of the largest and notorious firms and data breach events in recent history. Methodologically, it is evident from the legislative history of BNLs and other state data security laws that enactments are not random. They tend to occur earlier in states with more intense consumer use of electronic data, stronger general consumer protection regulation, and greater awareness of consumer data breaches and misuse – California, for example.

These challenges are familiar to researchers doing macro policy work with archival data. We address them through PRC data sub-sampling of smaller firms and their smaller data breach events, as well as through diagnostic studies suggesting little, if any, difference in pre- and post-enactment data breach trends in earlier versus later enacting states. Future work could include other sub-sampling strategies of industries where all firms tend to be smaller and local – restaurant and entertainment venues, for example. Future methodological work might re-examine pre- and post-enactment trends with a different periodicity such as months of quarters to detect changes in data breach trends that may be tied to seasonal business cycles.

We noted several benefits and challenges in using PRC data. Recall again that one challenge relates to the concurrence of BNL enactments and increased scope in PRC coverage because certain states enacting BNLs also started sharing breach incident data via public archives. Again, we included fixed year effects in our difference-in-differences models to adjust for such strict increases in reporting. We also used various PRC sub-sampling strategies to filter out effects on breach incident counts and magnitudes tied to BNL enactment *and* archive publication in those states. After imposing those safeguards, we find the same pattern of BNL non-effects observed more generally. That is remarkable on its own. Given the concurrence of both events we could well have predicted *positive* (not negative) BNL effects on data

Reporting Tool website archive is similar to many state BNL website archives we reviewed. While a good start, the Reporting Tool lacks other important information on current data security and data breach response standards. Both strike us as important for the development of a data privacy market.

breach counts and magnitudes in the PRC data. In any case, our modeling and subsampling strategies demonstrate how future researchers can anticipate PRC data challenges to take advantage of PRC data benefits.

We think our two-way difference-in-differences analytical approach is sensible for a study of BNL effects on data breaches and follow-on data misuse after 20 years since the first BNL was enacted. Various methodological strategies and diagnostic analyses presented in our study suggest that our analytical approach does not suffer from shortcomings other researchers might use as a justification for some alternative, such as the synthetic controls approach Kesari (2022b) takes in a working paper documenting both significant decrease and increase in identity thefts after BNL enactments and revisions across the US. That said, there may well be value in evaluating BNL effects on data breaches and follow-on data misuse not only when first enacted, but also when revised by state legislatures or enforced differently by state executives.

A perennial concern in any study where "non-effects" matter prominently is estimation power. Our results indicate no decrease in either breach event counts or magnitudes. Those results also appear to be precisely estimated. But those non-effects may yet be underpowered. Our own preliminary study suggests that OLS-based magnitude estimations may be slightly under-powered generally but adequately powered when evaluating pre- and post-treatment breach event magnitudes for BNLs with private rights of action. We note that the observed signs on treated (BNL-enacted) breach magnitudes are positive, not negative. If estimates of general BNL breach magnitude effects are underpowered, then they underpower a trend running contrary to intended BNL effects.

Similar power studies for pre- and post-treatment breach counts are more difficult to implement with a Poisson estimator. We can and do re-estimate breach count effects using OLS albeit with less precision. Here follow-on power studies suggest improved estimates for samples from 2.6 to 5.5 times larger than we use here. These results prompt caution in concluding definitively that BNLs are ineffective in decreasing breach event counts and prompt calls for follow-on research as more data on breach counts becomes available.[16]

Yet another limitation relates to the potential for "bleeding" effects across states. BNL enactment in California may affect firm behavior in neighboring states like Nevada or Arizona. A firm headquartered in California but with operations in those neighboring states might react to BNL enactment in California by changing behavior there and in those neighboring states. This is potentially problematic as it would mean the counterfactual is incorrectly specified. The fraud and identity

16 Details on these power studies are available from the authors.

theft analyses make us less concerned about this potential problem. Recall that we did detect short-term decreases in such data misuse across states as each enacted their BNLs. We think it unlikely that bleeding effects would obscure immediate post-enactment data breach trends but not immediate downstream data misuse trends. That said, future work might investigate BNL effectiveness on, say, a regional basis.

There is also the possibility of measurement error with dependent variables. As hacking operations become more sophisticated, it is plausible that firms will fail to detect data breach incidents and consumers will fail to detect downstream misuse of their data. These developments should be unrelated to BNL enactments, instead being a general trend captured by time fixed effects. Even so, the prospect merits closer investigation. Future work might account for the changing sophistication of hacking practices with, say, expert assessments of hacking practices across different types of data and industries.

Finally, there is the possibility of firm "migratory" behavior following BNL enactments. Firms could flee emerging BNL regimes as they come into force. While this is theoretically possible, we think it unlikely given substantial costs associated with such moves and, as we suggested earlier, the less substantial (than initially projected) BNL compliance costs. This possibility also prompts greater interest in replicating our results with BNLs and data breaches in state agencies and enterprises with little or no capacity to migrate elsewhere. These and other follow-on areas of research should help us understand more broadly and deeply whether and how BNLs meant to reduce data breaches and create a market for data privacy can achieve that aim to the benefit of firms, consumers, and broader society.

References

Acquisti, Alessandro, and Christina Fong. 2020. "An Experiment in Hiring Discrimination via Online Social Networks." *Management Science* 66 (3): 1005—24.

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. 2020. "Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving it in the Digital Age." *Journal of Consumer Psychology* 30 (4): 736—58.

Ahammer, Alexander, Martin Halla, and Nicole Schneeweis. 2020. "The Effect of Prenatal Maternity Leave on Short- and Long-Term Child Outcomes." *Journal of Health Economics* 70: 102250.

Allison, Paul D., and Richard P. Waterman. 2002. "Fixed—Effects Negative Binomial Regression Models." *Sociological Methodology* 32 (1): 247—65.

Anderson, Keith B. 2019. "Mass-Market Consumer Fraud in the United States: A 2017 Update." Washington: US Federal Trade Commission (accessed August 1, 2023).

Angrist, Joushua D., and Jörn-Steffen Pischke. 2008. *Mostly Harmless Econometrics: An Empiricist's Companion*. Princeton: Princeton University Press.

Attias. 2017. *Attias v. Carefirst, Inc*., 865 F.3d 620.

Autor, David H. 2003. "Outsourcing at Will: The Contribution of Unjust Dismissal Doctrine to the Growth of Employment Outsourcing." *Journal of Labor Economics* 21 (1): 1—42.
Autor, D., Frank Levy, and Richard J. Murnane. 2003. "The Skill Content of Recent Technological Change: An Empirical Exploration." *Quarterly Journal of Economics* 118 (4): 1279—333.
Ayyagari, Ramakrishna. 2012. "An Exploratory Analysis of Data Breaches from 2005—2011: Trends and Insights." *Journal of Information Privacy and Security* 8 (2): 33—56.
Baker, Tom, and Sean J. Griffith. 2007. "The Missing Monitor in Corporate Governance: The Directors' & Officers' Liability Insurer." *The Georgetown Law Journal* 95: 1795—842.
Baker, Andrew C., David F. Larcker, and Charles C. Y. Wang. 2022. "How Much Should We Trust Staggered Difference-in-Differences Estimates." *Journal of Financial Economics* 144 (2): 370—95.
Becker, Gary. 1968. "Crime and Punishment: An Economic Approach." *Journal of Political Economy* 76 (2): 169—217.
Ben-Shahar, Omri, and Carl E. Schneider. 2011. "The Failure of Mandated Disclosure." *University of Pennsylvania Law Review* 159 (3): 647—749.
Burtch, Gordon, Seth Carnahan, and Brad N. Greenwood. 2018. "Can You Gig It? An Empirical Examination of the Gig-Economy and Entrepreneurial Activity." *Management Science* 64 (12): 5497—520.
Callaway, Brantly, and Pedro H. C. Sant'Anna. 2021. "Difference-in-Differences With Multiple Time Periods." *Journal of Econometrics* 225 (2): 200—30.
Carnahan, Seth. 2017. "Blocked But Not Tackled: Who Founds New Firms When Rivals Dissolve?" *Strategic Management Journal* 38 (11): 2189—212.
Chesney, Robert. 2021. "Cybersecurity Law, Policy, and Institutions (version 3.1)." In *University of Texas Law, Public Law Research Paper No. 716*. University of Texas Law School: Austin.
Collins, J. Carlton. 2019. "Check on Data Breaches at the Privacy Rights Clearinghouse." *Journal of Accountancy* 228 (3): 67.
Computer World. 2016. "Biggest Hack of 2016: 412 Million Friendfinder Networks Accounts Exposed." November 14. Needham: Computer World (accessed August 1, 2023).
Cooper, James C., and Bruce H. Kobayashi. 2022. "Unreasonable: A Strict Liability Solution to the FTC's Data Security Problem." *Michigan Technology Law Review* 28 (2): 257—304.
DataBreaches.net. 2021. "Annotated Data Breach Incidents Archive." DataBreaches.net (Formerly PHIPrivacy.net). https://www.databreaches.net/category/breach-reports/ (accessed August 1, 2023).
Dynes, Adam M., and John B. Holbein. 2020. "Noisy Retrospection: The Effect of Party Control on Policy Outcomes." *American Political Science Review* 114 (1): 237—57.
Edwards, Benjamin, Steven Hofmeyr, and Stephanie Forrest. 2016. "Hype and Heavy Tails: A Closer Look at Data Breaches." *Journal of Cybersecurity* 2 (1): 3—14.
Equifax. 2019. *In re Equifax*. 362 F. Supp. 3d 1295.
FAA. 2021. "Airline Service Quality Performance System." Washington: US Federal Aviation Aministration (accessed February 1, 2023).
Faulkner, Brandon. 2007. "Hacking Into Data Breach Notification Laws." *Florida Law Review* 59: 1097.
Franco, Annie, Neil Malhotra, and Gabor Simonovits. 2014. "Publication Bias in the Social Sciences: Unlocking the File Drawer." *Science* 345 (6203): 1502—5.
Freeman, Jody. 2000. "The Private Role in the Public Governance." *NYU Law Review* 75: 543.
FTC. 2021. "Consumer Sentinel Network Data Book 2021." Washington: US Federal Trade Commission (accessed August 1, 2023).
Galaria. 2016. *Galaria v. Nationwide Mutual Insurance Company*, No. 15-3386.

Gelman, Andrew, and John Carlin. 2014. “Beyond Power Calculations: Assessing Type S (Sign) and Type M (Magnitude) Errors.” *Perspectives on Psychological Science* 9 (6): 641—51.

Goel, Sanjay, and Hany A. Shawky. 2014. “The Impact of Federal and State Notification Laws on Security Breach Announcements.” *Communications of the Association for Information Systems* 34 (1): 3.

Goldfarb, Brent, and Andrew A. King. 2015. “Scientific Apophenia in Strategic Management Research: Significance Tests & Mistaken Inference.” *Strategic Management Journal* 37 (1): 167—76.

Goodman-Bacon, A. 2021. “Difference-in-Differences With Variation in Treatment Timing.” *Journal of Econometrics* 225 (2): 254—77.

Guardian. 2013. “Did Your Adobe Password Leak? Now You and 150m Others Can Check.” November 7. London: *The Guardian* (accessed August 1, 2023).

Gupta, Abhishek. 2018. “The Evolution of Fraud: Ethical Implications in the Age of Largescale Data Breaches and Widespread Artificial Intelligence Solutions Deployment.” *International Telecommunication Union Journal (ITC Discoveries)* (1): 1—7.

Hartman, Erin, and F. Daniel Hidalgo. 2018. “An Equivalence Approach to Balance and Placebo Tests.” *American Journal of Political Science* 62 (4): 1000—13.

HIPAA. 2021. “Breach Reporting Tool.” Washington: US Department of Health and Human Services Office of Civil Rights (accessed February 1, 2023).

Horizon. 2017. *In re Horizon Healthcare Services Inc. Data Breach*, 846 F.3d 625.

Hutton. 2018. *Hutton v. Nat. Bd. of Examiners in Optometry, Inc.* 2018. 892 F. 3d 613, No. 17-1506.

IAPP. 2021. “U.S. State Data Breach Lists (Listing States With Breach Publication Websites).” Portsmouth: International Association of Privacy Professionals (accessed August 1, 2023).

IBM. 2021. “Cost of a Data Breach Report 2021.” https://www.ibm.com/security/data-breach (accessed August 1, 2023).

Irshad, Shareen, and Tariq Rahim Soomro. 2018. “Identity Theft and Social Media.” *International Journal of Computer Science and Network Security* 18 (1): 43—55.

ITech. 2021. “Facebook Data Breach 2021 Exposes Personal Info of 1.5 Billion Users: 2 Tools to Check if Your Data Have Been Leaked.” October 7. New York: ITech Post. Tech Times LLC (accessed August 1, 2023).

Joerling, Jill. 2010. “Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data.” *Washington University Journal of Law & Policy* 32: 467—88.

Karyda, Maria, and Lilian Mitrou. 2016. “Data Breach Notification: Issues and Challenges for Security Management.” In *MCIS Proceedings*. Paphos, Cyrus: Mediterranean Conference on Information Systems (accessed August 1, 2023).

Katz. 2012. *Katz v. Pershing, LLC*, 672 F.3d 64.

Kemp, Steven, David Buil-Gil, Fernando Mirò-Llinares, and Nicholas Lord. 2023. “When Do Businesses Report Cybercrime? Findings From a UK Study.” *Ciminology & Criminal Justice* 23 (3): 468—89.

Kesari, Aniket. 2022a. “Do Data Breach Notification Laws Reduce Medical Identity Theft? Evidence From Consumer Complaints Data.” *Journal of Empirical Legal Studies* 19 (4): 1222—52.

Kesari, Aniket. 2022b. “Do Data Breach Notifications Work?” Working Paper. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4164674 (accessed August 1, 2023).

Kosseff, Jeff. 2017. “Defining Cybersecurity Law.” *Iowa Law Review* 103: 985—1031.

Krottner. 2010. *Krottner v. Starbucks Corp*, 628 F. 3d 1139, No. 09-35823.

Laube, Stefan, and Rainer Böhme. 2016. “The Economics of Mandatory Security Breach Reporting to Authorities.” *Journal of Cybersecurity* 2 (1): 29—41.

Lewert. 2016. *Lewert v. PF Chang’s China bistro, Inc.*, 819 F.3d 963.

McCaskey, Kelly, and Carlisle Rainey. 2015. "Substantive Importance and the Veil of Statistical Significance." *Statistics, Politics, and Policy* 6 (1—2): 77—96.
McNamara, Gerry, Paul M. Vaaler, and Cynthia Devers. 2003. "Same as it Ever Was: The Search for Evidence of Increasing Hypercompetition." *Strategic Management Journal* 24 (3): 261—78.
Nieuwesteeg, Bernold. 2017. "To Notify or Not to Notify? Do Organizations Comply With U.S. Data Breach Notification Laws? An Empirical Study." Working Paper. https://papers.ssrn.com/sol3/papers.cfm?abstract_id&tnqx3d;2431174 (accessed August 1, 2023).
Needles, Sara A. 2009. "The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law." *North Carolina Law Review* 88: 267—310.
NCSL. 2021. "Security Breach Notification Laws." Washington: National Conference of State Legislatures (accessed August 1, 2023).
Park, Sangchul. 2019. "Why Information Security Law Has Been Ineffective in Addressing Security Vulnerabilities: Evidence From California Data Breach Notifications and Relevant Court and Government Records." *International Review of Law and Economics* 58: 132—45.
Perkins. 2021. "Security Breach Notification Chart." Seattle: Perkins-Coie Law Firm (accessed August 1, 2023).
Peters, Rachel. 2014. "So You've Been Notified, Now What: The Problem With Current Data-Breach Notification Laws." *Arizona Law Review* 56 (4): 1171—202.
Picanso, Kathryn E. 2006. "Protecting Information Security Under a Uniform Data Breach Notification Law." *Fordham Law Review* 75 (1): 355—90.
PRC. 2022. "Privacy Rights Clearinghouse." San Diego (accessed August 1, 2023).
Raval, Devesh. 2020. "Which Communities Complain to Policymakers? Evidence From Consumer Sentinel." *Economic Inquiry* 58 (4): 1628—42.
Resnick. 2012. *Resnick v. Avmed, Inc*, 693 F. 3d 1317.
Rode, Lilia. 2006. "Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security." *Houston Law Review* 43 (5): 1597—634.
Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. 2011. "Do Data Breach Disclosure Laws Reduce Identity Theft?" *Journal of Policy Analysis and Management* 30 (2): 256—86.
Rudolph. 2019. *Rudolph v. Hudsons Bay Co.*, No. 18 cv 8472.
Schwarcz, Daniel, Josephine Wolff, and Daniel W. Woods. 2023. "How Privilege Undermines Cybersecurity." *36 Harvard Journal of Law & Technology* (2): 421—485.
SEC. 2018. "Commission Statement and Guidance on Public Company Cybersecurity Disclosures." Release Nos. 33-10459; 34-82746. February 26. Washington: US Securities and Exchange Commission.
SEC. 2020. *Cybersecurity and Resiliency Observations. Guidance From the Office of Compliance Inspections and Enforcement*. Washington: US Securities and Exchange Commission.
SEC. 2021. "Office of Credit Ratings." Washington: US Securities and Exchange Commission.
SEC. 2023. "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies." Washington: US Securities and Exchange Commission (accessed August 1, 2023).
Silva, J. M. C. Santos, and Silvana Tenreyro. 2006. "The Log of Gravity." *The Review of Economics and Statistics* 88 (4): 641—58.
Silva, J. M. C. Santos, and Silvana Tenreyro. 2011. "Further Simulation Evidence on the Performance of the Poisson Pseudo-Maximum Likelihood Estimator." *Economics Letters* 112 (2): 220—2.
Solove, Daniel J., and Paul M. Schwartz. 2019. *Privacy Law Fundamentals*, 6th ed. Portsmouth: International Association of Privacy Professionals.
Stata. 2019. *Stata Version 16.1*. College Station: StataCorp.

Steel, Chad M. S. 2019. “Stolen Identity Valuation and Market Evolution on the Dark Web.” *International Journal of Cyber Criminology* 13 (1): 70—83.
Stevens, Gina. 2012. *Data Security Breach Notification Laws*. Washington: Congressional Research Service.
Stevens, Tim. 2015. *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press.
Tom, Jacqueline May. 2010. “A Simple Compromise: The Need for a Federal Data Breach Notification Law.” *St. John’s University Law Review* 84 (4): 1569—603.
Walker, Estaban, and Amy S. Nowacki. 2011. “Understanding Equivalence and Noninferiority Testing.” *Journal of General Internal Medicine* 26 (2): 192—6.
Weiss, N. Eric, and Rena S. Miller. 2015. *The Target and Other Financial Data Breaches: Frequently Asked Questions*. Washington: Congressional Research Service.
Winn, Jane K. 2009. “Are ‘Better’ Security Breach Notification Laws Possible?” *Berkeley Technology Law Journal* 24: 1133.
Wolf, Josephine. 2018. “Why It’s So Hard to Punish Companies for Data Breaches.” October 16. *New York Times*.
Zamoff, Mitchell, Brad N. Greenwood, and Gordon Burtch. 2022. “Who Watches the Watchmen: Evidence of the Effect of Body-Worn Cameras on New York City Policing.” *Journal of Law, Economics, and Organization* 38 (1): 161—95.