7-13-2023

Cyber Plungers: Colonial Pipeline and the Case for an Omnibus Cybersecurity Legislation

Asaf Lubin
Maurer School of Law - Indiana University, lubina@iu.edu

CYBER PLUNGERS: COLONIAL PIPELINE AND THE CASE FOR AN OMNIBUS CYBERSECURITY LEGISLATION

Asaf Lubin[*]

The May 2021 ransomware attack on Colonial Pipeline was a wake-up call for a federal administration slow to realize the dangers that cybersecurity threats pose to our critical national infrastructure. The attack forced hundreds of thousands of Americans along the east coast to stand in endless lines for gas, spiking both prices and public fears. These stressors on our economy and supply chains triggered emergency proclamations in four states, including Georgia. That a single cyberattack could lead to a national emergency of this magnitude was seen by many as proof of even more crippling threats to come. Executive Director of the Cybersecurity and Infrastructure Security Agency (CISA), Brandon Wales, went on to describe the incident as a "galvanizing event for the country."

This Article challenges this characterization, suggesting instead that little has changed in terms of regulation, enforcement, or liability and that, as a result, another cyber incident targeting our critical infrastructure is, quite frankly, a matter of when and not if. The Article explores a set of kneejerk legal processes—litigatory, regulatory, and legislative—which were set in motion in the wake of the Colonial Pipeline incident. For each these processes the Article highlights points of failure in generating positive long-term effects aimed at increasing broader cybersecurity. Relying on insights from Daniel Solove and Woody Hartzog's recent book Breached!*, this Article treats the Colonial Pipeline incident as a microcosm through which to understand our broader*

[*] Dr. Asaf Lubin is an Associate Professor of Law at Indiana University Maurer School of Law, Fellow at IU's Center for Applied Cybersecurity Research, Faculty associate at the Berkman Klein Center for Internet and Society at Harvard University, Affiliated Fellow at the Information Society Project at Yale Law School, and a Visiting Scholar at the Federmann Cyber Security Center at Hebrew University of Jerusalem. I want to thank participants of the Georgia Law Review Symposium: "The Intersection of Law and Emerging Technology." I further want to thank the editors and staff of the Georgia Law Review for their excellent work in organizing this symposium and in editing this paper and the broader publication.

regulatory deficits in critical infrastructure cybersecurity. Against this backdrop, the Article offers the first scholarly examination of a new and innovative blueprint developed by the Biden Administration to promote holistic regulations as part of a National Cybersecurity Strategy. The Article highlights both the promises and pitfalls of this Strategy on future regulation of critical infrastructures.

TABLE OF CONTENTS

I. INTRODUCTION

"*This morning: gas and patience running low at the pump*." This is how one reporter chose to begin a May 2021 news segment on the business-crippling Colonial Pipeline ransomware attack.[1] The attack forced Colonial Pipeline executives to completely shut down the operations of a 5,500 mile pipeline—the largest conduit of refined oil products in the U.S.—triggering both panic and fuel shortages across the southeast.[2] At its peak, the nation's capital, Washington D.C., saw eighty percent of gas stations without fuel with North Carolina as a close second with sixty-three percent of its stations reporting shortages.[3]

---

[1] NBC Today, *Drivers Wait Hours in Long Gas Lines After Pipeline Shutdown*, YOUTUBE (May 12, 2021), https://www.youtube.com/watch?v=dWzjAY6nP-o. The federal government defines a ransomware as a "type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted." *See* U.S. DEP'T OF JUST., RANSOMWARE: WHAT IT IS AND WHAT TO DO ABOUT IT, https://www.justice.gov/criminal-ccips/file/872766/download (last visited Feb. 7, 2023).

[2] *See, e.g.*, Matt Egan, *Gas Stations in the Southeast Run Out of Gas as People Panic Buy Fuel*, CENT. NEWS NETWORK (May 12, 2021, 5:48 PM), https://www.cnn.com/2021/05/12/business/gas-shortage-colonial-pipeline/index.html (noting that a ransomware attack caused a pipeline shutdown and consumer panic); *see also, e.g.*, Joseph Menn & Stephanie Kelly, *Colonial Pipeline Slowly Restarts as Southeast U.S. Scrambles for Fuel*, REUTERS (May 12, 2021, 3:11 AM), https://www.reuters.com/business/energy/top-us-fuel-pipeline-edges-toward-reopening-gasoline-shortages-worsen-2021-05-12/ (documenting that "a ransomware attack shut the [Colonial] line, triggering fuel shortages and panic buying in the southeastern United States"). Colonial Pipeline "carries 45 percent of the fuel supplies for the eastern United States." Kim Lyons, *Colonial Pipeline Says Operations Back to Normal Following Ransomware Attack*, VERGE (May 15, 2021, 1:44 PM), https://www.theverge.com/2021/5/15/22437730/colonial-pipeline-normal-ransomware-attack-fuel. The pipeline also "transports 2.5 million barrels per day of gasoline." Christopher Bing & Stephanie Kelly, *Cyber Attack Shuts Down U.S. Fuel Pipeline "Jugular," Biden Briefed*, REUTERS (May 8, 2021, 12:54 AM), https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/.

[3] *See* Paola Rosa-Aquino & Chas Danner, *What We Know About the Colonial Pipeline Shutdown*, N.Y. MAG.: INTELLIGENCER (May 16, 2021), https://nymag.com/intelligencer/article/what-we-know-about-the-colonial-pipeline-shutdown-updates.html (citing reporting from CNBC on the percentage of gas stations experiencing a fuel shortage).

The attack was attributed to Russian ransomware gang DarkSide.[4] DarkSide ran a "ransomware as a service" (RaaS) business, wherein the profits from extortion were shared between it and its affiliates.[5] The affiliates are those end-users who ran the actual extortion campaigns on DarkSide-managed servers and infrastructure.[6] Each affiliate executed "the computer intrusion and deploy[ed] the ransomware," further choosing the "intrusion method" and the negotiating "ransom demands with the victim."[7] Because DarkSide's RaaS program facilitated the scale up of ransomware attacks, further hindering possible enforcement, the U.S. State Department offered a reward of ten million dollars for information assisting in the identification of key DarkSide leaders.[8]

Internal and external investigations following the Colonial Pipeline incident revealed that the systems that directly run the operation of the pipeline and linked refineries were unaffected.[9] It was the company's billing system that had been compromised, making it impossible for Colonial Pipeline "to track fuel distribution

---

[4] *See* Paul W. Parfomak & Chris Jaikaran, *Colonial Pipeline: The DarkSide Strikes*, CONG. RES. SERV. (May 11, 2021), https://crsreports.congress.gov/product/pdf/IN/IN11667 (attributing the attack to Darkside).

[5] *See id*. ("RaaS is a cybercrime model in which one criminal group develops the ransomware and hosts the infrastructure upon which it operates, then leases that capability to another criminal group to conduct an attack.").

[6] For more on RaaS, see Asaf Lubin, *The Law and Politics of Ransomware*, 55 VAND. J. INT'L. L. 1177, 1200–01 (2022) (explaining RaaS and its extortionate business model).

[7] Transnational Organized Crime Rewards Program, *DarkSide Ransomware as a Service (RaaS)*, U.S. DEP'T OF STATE (Nov. 4, 2021), https://www.state.gov/darkside-ransomware-as-a-service-raas/.

[8] *See id*. (offering a reward of ten million dollars for information about the leaders of DarkSide).

[9] *See Colonial Pipeline Hack Prevention*, AGILE ENTERPRISE SERV., https://govaes.com/colonial-pipeline-hack-prevention/ (last visited Feb. 7, 2023) ("The attack targeted Colonial Pipeline's billing system, while the operational technology systems were unaffected. Due to a concern that hackers might have obtained information that could allow them to carry out further attacks on vulnerable pipeline components, the company took this precautionary shutdown measure."); *see also Chevron Says Refineries Unaffected by Colonial Outage but Disruptions Possible*, REUTERS (May 10, 2021, 4:51 PM), https://www.reuters.com/business/energy/chevron-says-refineries-unaffected-by-colonial-outage-disruptions-possible-2021-05-10/ (noting Chevron's statement that their refineries were unaffected by the attack).

and bill customers."[10] Company leaders, prioritizing their bottom line over public interest, refused to distribute fuel without ensuring proper billing first.[11] As such, they chose to shut down operations altogether.[12] CEO Joe Blount's official stance is different, of course. He insists that he ordered the shutdown as a precautionary measure, in service of the public good, because there was no way to determine if more attacks were on the horizon without first pausing all operations.[13] Either way, the hackers knew what they were doing. They chose to target the softer financial underbelly of Colonial Pipeline, and thereby of the broader American gas supply system. Instead of aiming their attacks at the far more secured industrial servers and systems that control and manage the line, they chose to target a mere billing system.[14] In a privatized and highly capitalist environment, like the critical infrastructure ecosystem of the U.S.,[15] even Russian hackers figure out quickly "how to hit [us] where it hurts."[16]

---

[10] Lily Hay Newman, *Colonial Pipeline Paid a $5M Ransom—and Kept a Vicious Cycle Turning*, WIRED (May 14, 2021, 7:00 AM), https://www.wired.com/story/colonial-pipeline-ransomware-payment/.

[11] *See id*. (finding that a factor in Colonial's decision to shut down operations "was that the company's billing system had been infected with ransomware, so it had no way to track fuel distribution and bill customers").

[12] *See id*. (noting that Colonial took down it's network "in an attempt to contain the damage").

[13] *See* Mary Louise Kelly, Jason Fuller & Justine Kenin, *The Colonial Pipeline CEO Explains the Decision to Pay Hackers a $4.4 Million Ransom*, NAT'L PUB. RADIO (June 3, 2021, 6:35 PM), https://www.npr.org/2021/06/03/1003020300/colonial-pipeline-ceo-explains-the-decision-to-pay-hackers-4-4-million-ransom (interviewing the CEO of Colonial Pipeline who explained the decision to pay the ransom as "part of [their] duty to the American people").

[14] For further reading on the protection of industrial control systems in the context of cybersecurity of the underlying U.S. pipeline infrastructure, see Hillary Hellmann, *Acknowledging the Threat: Securing United States Pipeline SCADA Systems*, 36 ENERGY L.J. 157, 157 (2015) (arguing that legislation streamlining and liability and privacy protection for oil and gas pipeline owners could strengthen cybersecurity and incentivize industry participation).

[15] *See* Chris Isidore, *Who Owns the Colonial Pipeline? It's Complicated*, CNN (May 12, 2021, 1:02 PM), https://www.cnn.com/2021/05/12/investing/colonial-pipeline-ownership/index.html (noting that Colonial is privately held).

[16] Rain Noe, *"New Details" Suggest Execs, Not Hackers, Shut Down Colonial Pipeline Due to Inability to Bill Customers*, CORE77 (May 13, 2021), https://www.core77.com/posts/108776/New-Details-Suggest-Execs-Not-Hackers-Shut-Down-Colonial-Pipeline-Due-to-Inability-to-Bill-Customers.

The same set of conflicting financial and public interest considerations stood at the heart of CEO Blount's other controversial decision: to pay a ransom demand of seventy-five bitcoins (worth at the time nearly $4.5 million) to the hackers.[17] On the one hand, paying the ransom increased the likelihood of a speedier recovery and return to "business as usual." At the same time, such payments support an ever-growing criminal enterprise which could risk other pipelines and other critical infrastructure across the country.[18] CEO Blount believes that he made "the right decision," in prioritizing quick recovery over long potential adverse effects.[19] He is perhaps right in this specific incident. After all, the Federal Bureau of Investigation and the Department of Justice ultimately seized back a large portion of the payment by tracking the bitcoin public ledger and employing a private key to access the

---

[17] As Blount explained it, it was the "hardest decision" he ever made in his career. Kelly et al., *supra* note 13.

> The conversation went like this: Do you pay the ransom or not? And of course, the initial thought is: You don't want to pay the ransom. You don't want to encourage [hackers], you don't want to pay these contemptible criminals. But our job and our duty is to the American public. So when you know that you have 100 million gallons of gasoline and diesel fuels and jet fuels that are going to go across the Southeastern and Eastern seaboard of the United States, it's a very critical decision to make. And if owning that de-encryption tool gets you there quicker, then it's the decision that had to be made. And I did make that decision that day. It was the right decision to make for the country.

Id.

[18] For a discussion of the ethical dilemmas around paying the ransom, see Tom Hoffman, *How Organisations Can Ethically Negotiate Ransomware Payments*, 10 NETWORK SEC. 13, 16 (2020) ("[T]he driving factors behind whether to pay a ransom or not are twofold: ethical (if what is at stake is very sensitive personal data, critical infrastructure or people's lives) and financial (if the cost of downtime will exceed the cost of ransom)."). For a discussion on legal and policy issues surrounding the market of private insurance for ransomware victims, see Tom Baker & Anja Shortland, *Insurance and Enterprise: Cyber Insurance for Ransomware*, GENEVA PAPERS ON RISK AND INS. (2022) ("[M]ixed responses to the Colonial ransomware event illustrate a tension between security and enterprise that appears whenever insurance engages with crime."); Kyle D. Logue & Adam B. Shniderman, *The Case for Banning (and Mandating) Ransomware Insurance*, 28 CONN. INS. L.J. 247, 250 (2021) (discussing how "ransom payments are increasingly being covered by insurance").

[19] Kelly et al., *supra* note 13.

relevant proceeds.[20] Not only that, but they also further targeted infrastructural features of the DarkSide RaaS, forcing the gang to go completely offline and shut down their operations, at least temporarily.[21] But while partial success was clearly achieved extraterritorially against the foreign hackers, questions remain as to the success of domestic initiatives for regulatory reform at home.[22]

In the wake of the Colonial Pipeline attack, a number of leading experts and academics put forward excellent scholarship that sought to propose a set of reforms to our gas pipeline cybersecurity problems.[23] The Committee on Homeland Security in the U.S. House of Representatives further ran a series of public hearings, titled "Cyber Threats in the Pipeline," hoping to draw a set of lessons from the Colonial Pipeline ransomware attack on the

---

[20] *Dep't of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside*, DEP'T OF JUST. NEWS (June 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[21] *See* Michael Schwirtz & Nicole Perlroth, *DarkSide, Blamed for Gas Pipeline Attack, Says It Is Shutting Down*, N.Y. TIMES (June 8, 2021), https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html (citing a letter in Russian from the ransomware gang in which they confirm that "[d]ue to the pressure from the U.S., the affiliate program is closed"). *But cf.* Antonia Din, *BlackMatter Ransomware Claims to Be a Successor to DarkSide and REvil*, HEIMDAL SEC. (Aug. 2, 2021), https://heimdalsecurity.com/blog/blackmatter-ransomware-claims-to-be-a-successor-to-darkside-and-revil/ (referring to this new gang as DarkSide's "successor" and noting that they "launched themselves on the dark web, and are actively trying to recruit criminal partners and affiliates to attack large companies in the United States, UK, Canada, and Australia").

[22] Bobby Chesney describes what he calls the "offensive perspective" and the "defensive perspective" to cybersecurity law and policy. 3.1 BOBBY CHESNEY, CHESNEY ON CYBERSECURITY LAW, POLICY, AND INSTITUTIONS 1 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547103. Whereas the former concerns government intrusions abroad to target foreign hackers and intercept their malicious activities, the latter improving cybersecurity defenses domestically with "the policy goal of minimizing unauthorized access to or disruption of computer systems. *Id.*

[23] *See, e.g.*, Ido Kilovaty, *Cybersecuring the Pipeline*, 60 HOUS. L. REV. 101, 106 (2023) (proposing "specific recommendations to address the current shortcomings of the regulatory approach to pipeline cybersecurity"); Joe R. Reeder & Tommy Hall, *Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack*, CYBER DEF. REV. 15 (Summer 2021) (proposing six "lessons learned" that the "Nation must take to heart").

regulation of the industry and beyond.[24] In this brief symposium Article, I wish to build on these studies and examinations. Two years after the largest cyberattack on a U.S. critical infrastructure ever reported, I wish to take advantage of the benefit of time to understand the long-term effects that the incident has had on our national cybersecurity legal environment. In particular, I wish to test the argument that Executive Director of the Cybersecurity and Infrastructure Security Agency (CISA), Brandon Wales, recently made: that the Colonial Pipeline attack was a "galvanizing event for the country."[25]

To determine how "galvanizing" the incident really was, I explore a set of three legal responses to the breach. All three responses are typical when such incidents happen. So common, in fact, that in their recent book *Breached!*, Daniel Solove and Woodrow Hartzog label them with the moniker "triple punch":

> After a data breach, the law will spring into action. Breach notification laws will often be triggered, requiring notification of a breach. Regulatory agencies will launch an investigation and might bring an enforcement action. A blizzard of lawsuits will likely be filed. This combination—a triple punch in the gut—is expensive and demanding of resources. That would be okay if the rules and enforcement fostered a secure data ecosystem. But it's not working.[26]

---

[24] *Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure, Hearing before the H.R. Comm. on Homeland Sec.*, 117th Cong. (June 9, 2021), https://www.govinfo.gov/content/pkg/CHRG-117hhrg45085/pdf/CHRG-117hhrg45085.pdf; *see also United States Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack, Hearing before the H.R. Comm. on Homeland Sec.*, 117th Cong. (June 15, 2021), https://www.congress.gov/117/chrg/CHRG-117hhrg45310/CHRG-117hhrg45310.pdf (hoping to learn about the government's plans to respond to future cyber incidents).

[25] David Jones, *How the Colonial Pipeline Attack Instilled Urgency in Cybersecurity*, CYBERSEC. DIVE (May 17, 2022), https://www.cybersecuritydive.com/news/post-colonial-pipeline-attack/623859/.

[26] DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 60 (2022).

The triple punch of litigation, legislation, and regulatory investigation and enforcement form the holy trinity of cybersecurity incident response in law and policy circles within the United States. In their book, Solove and Hartzog highlight why each of these kneejerk legal reactions repeatedly fails in generating meaningful long-term cybersecurity regulation.[27] Applying their insights to the Colonial Pipeline case study is thus worthwhile to further cement these findings. This is how this Article progresses, with Part II exploring the litigatory response, Part III exploring the regulatory response, and Part IV exploring the legislative response.

But there is another reason why this Article's investigation is well-timed. Solove and Hartzog called in their book for "holistic data security" regulation.[28] This regulation should be informed by the fact that "breaches are the product of the data ecosystem, which is perversely structured in ways that not only [] fail to prevent data breaches but make it easier for them to occur and heighten the damage they cause."[29] The Biden Administration seems to be going in this direction, with the recently released National Cyber Strategy (NCS).[30] In the leadup to its release, the NCS was described as a document "unlike any before it," as it dares to say, "things that others have been afraid to say."[31] The NCS does seem to indicate a move towards "holistic data security" regulation of the kind envisioned by Solove and Hartzog. If the vision presented in the Strategy actually materializes, then Colonial Pipeline will certainly prove to be a "galvanizing event."

The NCS was released shortly before we all gathered together in Athens, Georgia, for the Symposium's proceedings in March. As

---

[27] *See id.* at 67 (emphasizing that contemporary data security law generally does not "look . . . beyond the blast radius of a data breach" and therefore repeatedly fails to achieve its aims).

[28] *See id*. (proposing that improvement in data security "requires seeing it quite differently" as "holistic data security").

[29] *Id.*

[30] THE WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY (Mar. 1, 2023) [hereinafter NCS], https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[31] Tim Starks, *The Biden National Cyber Strategy Is Unlike Any before It,* WASH. POST (Jan. 6, 2023), https://www.washingtonpost.com/politics/2023/01/06/biden-national-cyber-strategy-is-unlike-any-before-it/.

such, I use the conclusion to provide a first scholarly examination of some of the main promises and pitfalls in the NCS.

II. COLONIAL PIPELINE AND THE LITIGATORY RESPONSE

First came the blizzard of lawsuits. Mere days after the ransomware attack, Ramon Dickerson, a North Carolina resident, brought a negligence class action suit against Colonial Pipeline. His complaint reasoned that Colonial Pipeline had a duty of care "to use reasonable means to secure and safeguard its computer systems and gasoline transmission operations" and comply with all relevant "industry standards" for security.[32] Dickerson sought actual and compensatory damages (for the high price of gas that he paid) as well as statutory fines, punitive damages, and attorney's fees.[33]

Another class action began a month later with a complaint from EZ Mart 1, LLC., a North-Carolina gas station and convenience store. Whereas the first action was brought by a class of individual gas purchasers, this second action was brought by "[a]ll gas stations that experienced a fuel shortage, an increase in the price of gasoline, or an inability to sell fuel to their customers as a result of the Ransomware attack."[34] The action brought a similar theory of negligence akin to the one espoused by Dickerson, rooted in the double duties to "implement adequate and reasonable measures to ensure that the pipeline's critical infrastructure was safeguarded" and to "take reasonable steps to safeguard" private and sensitive information regarding suppliers and customers.[35]

Noteworthy is that the first two complaints also relied on the Declaratory Judgment Act to seek even further remedies from the

---

[32] Class Action Complaint ¶¶ 60–62, Dickerson v. CDPQ Colonial Partners, L.P., No. 1:21-cv-02098, 2021 WL 2009109 (N.D. Ga., May 18, 2021) [hereinafter Dickerson Complaint]. Plaintiffs' Second Amended Complaint in *Dickerson* asserted, beyond the negligence claims, additional violations of the North Carolina Unfair and Deceptive Trade Practice Act, breach of public duty pursuant to Title 51 of the Georgia Code, as well as public nuisance and unjust enrichment claims. Second Amended Complaint ¶¶ 62–113, Dickerson v. CDPQ Colonial, L.P., No. 1:21-cv-02098, 2021 WL 7501465 (N.D. Ga. Aug. 4, 2021).

[33] Dickerson Complaint, *supra* note 32, ¶¶ 60–61.

[34] Class Action Complaint ¶ 8, EZ Mart 1, LLC v. Colonial Pipeline Co, No. 1:21-cv-02522, (N.D. Ga., June 21, 2021) [hereinafter EZ Mart Complaint], https://www.classaction.org/media/ez-mart-1-llc-v-colonial-pipeline-company.pdf.

[35] *Id.* ¶¶ 8, 41.

court.[36] Namely, the plaintiffs were concerned that the defendant "may lack the incentives to take all steps necessary to prevent similar cyberintrusions [sic] in the future."[37] The court was therefore called to utilize its vested authority to award equitable and injunctive relief and impose on Colonial Pipeline an obligation to employ reasonable security measures and protocols "consistent with law and industry standards."[38]

Finally, two months after EZ Mart's complaint, Jerry Todd Everhart, Deborah Frazier, and Joseph Frazier brought a third class action against Colonial Pipeline. These plaintiffs raised a different set of concerns than the prior class actions. They all shared personally identifiable information (PII) with Colonial Pipeline. Such information included names, contact information, date of birth, government-issued IDs (including social security numbers), and health insurance information.[39] Their complaint relied on negligence, breach of contract, breach of confidence, and invasion of privacy claims, to seek compensation for injuries suffered and increased risks generated from Colonial Pipeline compromising their PII.[40] Their list of injuries included:

> (1) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, or recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, not limited to lost

---

[36] *See* Declaratory Judgment Act, 28 U.S.C. § 2201 ("[I]n any civil action involving . . . [a] countervailing duty proceeding regarding a class . . . any court of the United States, upon the filing of an appropriate pleading, may declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought. Any such declaration shall have the force and effect of a final judgment or decree and shall be reviewable as such."); *see also* Dickerson Complaint, *supra* note 32, ¶ 71 (arguing that the court possesses broad powers to fashion a remedy); EZ Mart Complaint, *supra* note 34, ¶ 130 (arguing that the court's broad powers allows it enjoin the company and put protective measures in place).

[37] EZ Mart Complaint, *supra* note 34, ¶ 129.

[38] *Id*.

[39] Everhart v. Colonial Pipeline Co., No. 1:21-cv-03559, 2022 WL 3699967, at *1 (N.D. Ga., Aug. 27, 2021).

[40] *Id.*

> time, and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII.[41]

All three class actions came before the U.S. District Court for the Northern District of Georgia, where Colonial Pipeline is headquartered.[42] One after the other, all three cases were dismissed.[43] This is not surprising. Wholesale rejections of privacy and cybersecurity class actions are notoriously common in our judicial system. Bernard Chao summarized this point:

> Huge data breaches fill our headlines. Companies often violate their own privacy policies by selling customer data or by using the information in ways that fall outside their policy. Yet even when there is indisputable misconduct, the law generally does not hold these companies accountable. That is because traditional legal claims are poorly suited for handling privacy losses. Contract claims fail when privacy policies are not considered contractual obligations. Misrepresentation claims cannot succeed when customers never read and rely on those policies. The economic loss rule (which disallows recovery for purely economic injuries) thwarts many negligence claims. But undoubtedly the thorniest obstacle is that privacy harms are often not considered cognizable injuries under conventional legal theories. Tort, contract, and

---

[41] *Id.* at *2.

[42] *Id.*; Dickerson Complaint, *supra* note 32; EZ Mart Complaint, *supra* note 34.

[43] Everhart, 2022 WL 3699967, at *6; Order Granting Motion to Dismiss, EZ Mart 1, LLC v. Colonial Pipeline Co., No. 1:21-cv-03559 (N.D. Ga. July, 8, 2022) [hereinafter EZ Mart Order] (entering an order to dismiss the petition); Order Granting Motion to Dismiss, Dickerson v. CDPQ Colonial Partners, L.P., No. 1:21-cv-02098 (N.D. Ga. June, 17, 2022) [hereinafter Dickerson Order] (same).

> constitutional standing doctrine all demand some form of concrete injury, but privacy injuries are often too intangible or risk-based to qualify. Thus, no matter how blatantly a company violates its privacy obligations or how porous a company's data security, the victims' lawsuit is often perfunctorily dismissed.[44]

Nearly all of these points were brought into full display in the dismissals of the class action complaints against Colonial Pipeline. Note that all three cases were summarily dismissed, thereby denying plaintiffs even the basic ability to engage any of their allegations in a more substantive way. While not surprising, the decisions set a significant and undeniable barrier to collective litigation and actions by victims of security breaches against the companies that manage our critical infrastructure. The legacy of the Colonial Pipeline litigation is thus one of unremitting defiance to liability.[45] Like Cerberus, from Greek mythology, Judge Mark H. Cohen, who presided over all three of the proceedings, acted as a three headed guard dog gatekeeping any private litigator from entering the halls of justice to pursue a claim. While each of the complaints were unique, brought by a different class of litigants, arguing different types of harms and different theories of liability, Judge Cohen was unfazed. His three heads represent a typical dismissal ground.

---

[44] Bernard Chao, *Privacy Losses as Wrongful Gains*, 106 IOWA L. REV. 555, 556 (2021); *see also* John J.A. Lenz, *Privacy Class Actions' Unfulfilled Promise*, *in* CLASS ACTIONS IN PRIVACY LAW 13, 23–29 (Ignacio Cofone ed., 2021) (discussing repeated challenges to privacy class actions).

[45] *See* Kristin L. Bryan, *Federal Court Dismisses Colonial Pipeline Cybersecurity Litigation*, NAT'L L. REV. (July 13, 2022), https://www.natlawreview.com/article/federal-court-dismisses-colonial-pipeline-cybersecurity-litigation ("This case is a significant rejection of a consumer pricing-based theory of liability premised upon a cybersecurity attack that had a widespread impact on the public. As such, this win for Defendants will set the stage for others named in future-filed cases to argue such attenuated claims and theories should be similarly dismissed."); *see also*, Rafael Langer-Osuna, *Colonial Pipeline Data Breach Litigations: Where Are We Now?*, PRIV. WORLD (Nov. 19, 2021), https://www.privacyworld.blog/2021/11/colonial-pipeline-data-breach-litigations-where-are-we-now/ ("The outcome of these cases—specifically the extent to which downstream duties can be implicated by data breaches—could have a major impact on the future of data privacy/cybersecurity litigation.").

A. LACK OF DUTY OF CARE

The plaintiffs in *EZ Mart 1* faced an uphill battle trying to establish a duty and standard of care rooted in common law torts. For the duty to defend personal information, while Judge Cohen acknowledged that such duty might exist in general principles of common law, he found that Colonial Pipeline did not owe the duty to EZ Mart.[46] "EZ Mart does not allege that it had any relationship with Colonial, contractual or otherwise."[47] Indeed, the informational harms were felt by the suppliers and customers that EZ Mart worked with.[48] As a result, any damages that EZ Mart alleges that it and the rest of the class members felt, were not "causally connected to the breach of the alleged duty to safeguard information."[49] As for the other duty, to safeguard the pipeline, Judge Cohen went a step too far. Recall that EZ Mart claimed in its complaint that Colonial Pipeline had a duty to "take and implement adequate and reasonable measures to ensure the Pipeline's critical infrastructure was safeguarded."[50] Yet, Judge Cohen ignored that alleged duty and instead framed it as the "duty to ensure continuous uninterrupted service of the Pipeline."[51] With such a narrow and problematic articulation of the duty asserted, it is no surprise that Judge Cohen was quick to rule that there was no evidence of the existence of such a duty in either "statutory or common law."[52]

---

[46] *See* EZ Mart Order, *supra* note 43, at 11.

[47] *See id.*

[48] *Id.* at 12.

[49] *Id.*

[50] EZ Mart Complaint, *supra* note 34, ¶ 8.

[51] EZ Mart Order, *supra* note 43, at 8.

[52] *Id.* at 10. If the duty examined was a general obligation to secure the pipeline, there is enough statutory language coupled with common law practice, in my opinion, to justify recognizing that duty. For further discussion, see Kilovaty, *supra* note 23, at 106–07; Joseph R. Dancy & Victoria A. Dancy, *Terrorism and Oil & Gas Pipeline Infrastructure: Vulnerability and Potential Liability for Cybersecurity Attacks*, 2 OIL & GAS, NAT. RES., & ENERGY J. 579, 581 (2017). Note that Judge Cohen did consider other possible duty articulations in *Dickerson*, but there too he narrowed and unnecessarily focused the core claim each time. For example, once he tied any analysis of a duty to take "reasonable care in protecting its systems" with an application of "industry standards." Dickerson Order, *supra* note 43, at 11. He then proceeded to apply Georgia law where a violation of industry standards "does not conclusively establish any duty." *Id.* at 12 (citing Kraft Reinsurance Ireland, Ltd. v. Pallets Acquisitions, LLC, 845 F. Supp. 2d 1342, 1353 (N.D. Ga. 2011). A similar analysis was considered and equally

B. LACK OF COGNIZABLE HARM

The plaintiffs in *Everhart* are precisely those that Judge Cohen in *EZ Mart 1* thought might have a plausible duty of care to espouse.[53] Alas, this class struggled to provide evidence of cognizable harm to form part of a prima facie negligence suit.[54] One by one, Judge Cohen rejected each of the theories of harm pertaining to the compromised PII. The "[d]iminished [v]alue" theory was rejected as "conclusory" and unfounded;[55] the "[c]ontinued and [i]ncreased [r]isk" theory was rejected as "hypothetical and speculative";[56] and the "[m]itigation [e]xpenses" theory was rejected since any out-of-pocket expenses were merely self-inflicted "to avoid an insubstantial, non-imminent risk" that was again simply conjectural.[57] To be sure, Judge Cohen is not to be blamed here. As Solove and Hartzog write: "Courts have often struggled to

---

rejected in the context of a duty derived from special relations. Dickerson Order, *supra* note 43, at 14–15. But what stopped Judge Cohen from applying a social policy-focused, multi-pronged assessment to determine the utility of a new duty of care in a changing world? Indeed, California courts, by contrast, have considered these factors: (1) "the foreseeability of harm to the plaintiff"; (2) "the degree of certainty that the plaintiff suffered injury"; (3) "the closeness of the connection between the defendant's conduct and the injury suffered"; (4) "the moral blame attached to the defendant's conduct"; (5) the policy of preventing future harm"; (6) "the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach"; and (7) "the availability, cost, and prevalence of insurance for the risk involved." Rowland v. Christian, 443 P.2d 561, 564 (Cal. 1968); *see also* Bass v. Facebook, Inc., 394 F. Supp. 3d 1024, 1039 (N.D. Cal. 2019) (applying factors); Regents of Univ. of Cal. v. Superior Ct., 413 P.3d 656, 670 (Cal. 2018) (same).

[53] Compare EZ Mart Order, *supra* note 43, at 11 ("EZ Mart does not allege that it had any relationship with Colonial, contractual or otherwise."), with Everhart v. Colonial Pipeline Co., No. 1:21-cv-03559, 2022 WL 3699967, at *1 (N.D. Ga., Aug. 27, 2021) ("These three individuals owned property and resided within the vicinity of Colonial's pipeline, which obligated them to enter into contracts with Colonial in connection with property rights and environmental matters pertaining to Colonial's pipeline.").

[54] *See Everhart*, 2022 WL 3699967, at *2 ("[N]one of these [i.e., allegations] are legally cognizable injuries for which damages may be recoverable for a tort such as negligence under Georgia law.").

[55] *Id.*

[56] *Id.* at *3–4.

[57] *Id.* at *4–5 (quoting Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1345 (11th Cir. 2021)).

understand the harm from data breaches, so data breach cases have often been dismissed."[58]

C. PURE ECONOMIC LOSS

To put the final nail in the coffin, the plaintiffs in both *Dickerson* and *EZ Mart 1* were rejected under the Pure Economic Loss doctrine.[59] Both classes of litigants alleged an interpretation of harm that centers around a pricing-based theory of liability: that their damages were directly tied to the rising price of gas and the shortage which spiked it.[60] As a general rule, under Georgia law and beyond, "[a] plaintiff can recover in tort only those economic losses resulting from injury to his person or damage to his property."[61] Privacy and cybersecurity harms, however, do not usually generate physical, kinetic injury to person or property.[62] As such, the failure to define cognizable harm that the court would appreciate forces litigants to argue pure economic losses which are then summarily dismissed under conventional tort law.[63]

---

[58] *See* SOLOVE & HARTZOG, *supra* note 26, at 55.

[59] EZ Mart Order, *supra* note 43, at 15–18; Dickerson Order, *supra* note 43, at 15–18.

[60] Compare EZ Mart Order, *supra* note 43, at 2 ("EZ Mart allege[d] that Colonial 'elected to shut down the pipeline in whole or in part not because the threat actor has reached operational systems, but because Defendant [i.e., Colonial] was not sure it could continue to accurately bill for the product moving through its Pipeline.'"), with Dickerson Order, *supra* note 43, at 3 ("Plaintiffs are individuals who purchased gasoline at retail and paid higher prices as a result of Colonial's shutdown.").

[61] *See, e.g.*, EZ Mart Order, *supra* note 43, at 16 (quoting Gen. Elec. Co. v. Lowe's Home Ctrs., Inc., 608 S.E.2d 636, 637 (Ga. 2005)) (applying Georgia law); Dickerson Order, *supra* note 43, at 16 (quoting *Gen. Elec. Co.*, 608 S.E.2d at 637) (same).

[62] For more on the categorization of harms generated by privacy and cybersecurity breaches, see generally Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039 (2018); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737 (2018); Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022).

[63] Even where there is a common law exception for the pure economic loss doctrine, that exception is usually tied to certain types of duties and relationships between litigants, which returns one back to the first ground on which Judge Cohen dismissed the claims. *See* EZ Mart Order, *supra* note 43, at 17–18 (rejecting the "independent duty exception" and the "'special relationship' exception"); Dickerson Order, *supra* note 43, at 17–18 (same).

III. COLONIAL PIPELINE AND THE REGULATORY RESPONSE

In *Dickerson*, Colonial Pipeline argued at summary judgement that the consumers' tort claims were preempted by the Federal Energy Regulatory Commission's (FERC) authority over the pipeline.[64] It is an innovative claim that did not receive much attention by Judge Cohen in his orders. Nonetheless, it provides for a good segue into the role that regulatory agencies played in responding to the Colonial Pipeline incident.

One such response came from the U.S. Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA).[65] PHMSA employs a Pipeline Safety Enforcement program "designed to monitor and enforce compliance with pipeline safety regulations [(PSRs)]."[66] These PSRs predominately center around "welding failures, corrosion, excavation damage, incorrect operation, or natural events."[67] On May 5, 2022, PHMSA issued a Notice of Probable Violation (NOPV)

---

[64] Memorandum in Support of Defendant Colonial Pipeline Company's Motion to Dismiss at 9–14, Dickerson v. Colonial Pipeline Co., No. 1:21-CV-02098 (N.D. Ga. Sept. 20, 2021), ECF No. 44–1 ("Plaintiffs seek to circumvent FERC's federal regulatory authority over the operation of the Colonial pipeline through their state law claims. . . . The premise underlying Plaintiffs' claims in this case—that Colonial 'owed a duty to Plaintiffs not to shut down the pipeline'—is violently at odds with well-settled federal pipeline law and would create a state law duty that conflicts with the federal regulatory scheme. As the Supreme Court has held, 'the rights as defined by the tariff cannot be varied or enlarged by either contract or tort of the carrier. And they are not affected by the tort of a third party.' . . . To grant relief on Plaintiffs' state law claims, the Court would have to find Colonial could not do under state law what it is expressly permitted to do under federal law. That is the paradigmatic case for federal preemption." (citations omitted)); *see also* Andrea Vittorio, *Colonial Pipeline Rejects Responsibility for Hack's Gas Pump Hit*, BLOOMBERG L. (Sept. 21, 2021, 12:07 PM), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X6UVEK9O000000?bna_news_filter=privacy-and-data-security#jcite ("Colonial argues the case should be dismissed, in part because the consumers' claims, brought under state law in Georgia, would 'circumvent' the Federal Energy Regulatory Commission's authority over the pipeline's operation.").

[65] *See* Dancy & Dancy, *supra* note 52, at 591 ("The Department of Transportation's . . . Pipeline and Hazardous Materials Safety Administration . . . regulates and enforces the safety standards involved in pipeline construction and operation.").

[66] *Pipeline Enforcement Overview*, U.S. DEP'T TRANSP., (Jan. 25, 2023), https://www.phmsa.dot.gov/pipeline/enforcement/enforcement-overview.

[67] Dancy & Dancy, *supra* note 52, at 591.

and Proposed Compliance Order to Colonial Pipeline.[68] The NOPV noted a number of probable violations of PSRs with proposed civil penalties at the amount of $986,400.[69] In a public statement, PHMSA noted:

> From January through November 2020, PHMSA conducted an inspection of Colonial Pipeline Company's procedures and records for Control Room Management (CRM) in Linden, NJ, Hebert, LA, Greensboro, NC, and Alpharetta, GA. PHMSA made preliminary determinations that Colonial Pipeline Company was in probable violation of several PSRs, including a probable failure to adequately plan and prepare for manual shutdown and restart of its pipeline system. PHMSA informed Colonial Pipeline of the alleged non-compliance items shortly after the 2020 inspections concluded. The NOPV alleges that failures to adequately plan and prepare for a manual restart and shutdown operation contributed to the national impacts when the pipeline remained out of service after the May 2021 cyber-attack.[70]

At first glance, a speedy regulatory investigation and enforcement action would seem to represent a step in the right direction. There are, however, two reasons to be concerned. First, and most obviously, Colonial Pipeline is challenging these findings. In December 2022, lawyers from Colonial appeared at an enforcement hearing at the DOT's regional office in Kansas City,

---

[68] *See* U.S. DEP'T TRANSP., PIPELINE & HAZARDOUS MATERIALS SAFETY ADMIN., NOTICE OF PROBABLE VIOLATION, PROPOSED CIVIL PENALTY, & PROPOSED COMPLIANCE ORDER, (May 5, 2022), https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/2022-05/32022026_Colonial_Pipeline_NOPV_PCP_PCO_05052022.pdf (alleging violations of the Pipeline Safety Regulations).

[69] *See id.* (listing the penalties for each violation)

[70] *PHMSA Issues Proposed Civil Penalty of Nearly $1 Million to Colonial Pipeline Company for Control Room Management Failures*, U.S. DEP'T TRANSP. (May 5, 2022), https://www.phmsa.dot.gov/news/phmsa-issues-proposed-civil-penalty-nearly-1-million-colonial-pipeline-company-control-room.

Missouri.[71] There, the lawyers challenged the allegations that they were unprepared, calling them "inappropriate and incorrect."[72] They further argued that PHMSA stepped outside its authority in issuing the NOPV by expansively interpreting its own guidelines.[73] Moreover, they suggested that the fine was disproportionate ("37 times the size of the only other penalty" ever sought for a violation of the Control Room PSR).[74] PHMSA admitted in the hearing that it "miscalculated prior violations in determining the penalty," thereby signaling that the number will go down.[75] The proceedings are still ongoing, with Larry White, a presiding official at DOT's Pipeline Safety Law Division, scheduled to make a decision sometime this year.[76]

Second, and more importantly, this regulatory process is the only one that could potentially generate some financial liability attributable to the Colonial Pipeline. Colonial Pipeline's revenue is $500 million annually, as of 2021.[77] Even if the fine remains at close to one million dollars, it is still a drop in the ocean for a company of Colonial Pipeline's size.[78] Moreover, the fine has very little to do

---

[71] *See* Mike Soraghan, *Colonial Fights Charges of "Ad Hoc" Response to Pipeline Hack*, E&E NEWS (Dec. 1, 2022), https://www.eenews.net/articles/colonial-fights-charges-of-ad-hoc-response-to-pipeline-hack/ ("The company's representatives spoke at an enforcement hearing held here at the regional office of the Department of Transportation.").

[72] *Id.*

[73] *See id.* (noting that Colonial Pipeline's lead attorney claimed that PHMSA "had misinterpreted the rules and misunderstood Colonial's operations").

[74] *Id.*

[75] *Id.*

[76] *See id.* ("White will make a recommendation sometime next year on Colonial's protest of the enforcement actions and fine."). It should be noted that four years ago, we would not have even known about these proceedings. "PHMSA held such enforcement hearings behind closed doors" until March 2018. *Id.* "In March 2018, E&E News, with help from the Reporters Committee for Freedom of the Press, challenged the convening of a private hearing about leaks at Cheniere Energy Inc.'s Sabine Pass liquefied natural gas export terminal . . . . PHMSA officials agreed to allow an E&E News reporter to attend the 2018 session in Houston. The agency subsequently agreed to post online notices about when enforcement hearings get scheduled." *Id.*

[77] *See Colonial Pipeline Revenue*, ZIPPIA (Sept. 30, 2022), https://www.zippia.com/colonial-pipeline-careers-19622/revenue/ (noting that Colonial Pipeline's "peak revenue" was $500 million in 2021).

[78] *See* Christopher Helman, *Cyber-Ransom of $5m "Nothing" to Colonial Pipeline, Which Has Paid Hundreds of Millions in Dividends to Billionaire Koch Family*, FORBES (May 14, 2021, 2:17 PM), https://www.forbes.com/sites/christopherhelman/2021/05/14/cyber-ransom-

with the actual cybersecurity practices that Colonial Pipeline employed.[79] Those are currently not subject to any regulatory review with an eye towards fines or liability.[80] What deterrence effects does this reality generate for other companies in the pipeline infrastructure supply chain?

Alongside PHMSA, the other regulatory agency of importance is the Transportation Security Administration (TSA). Under the Aviation and Transportation Security Act, TSA holds "security responsibilities over . . . modes of transportation that are exercised by the Department of Transportation," which has been interpreted to include pipelines.[81] "Up until the Colonial Pipeline ransomware in May 2021, there has been little to no regulation of the U.S. pipeline."[82] All that TSA had issued was voluntary guidance.[83] It is for this reason that while "TSA urged Colonial Pipeline to participate in physical and cyber pipeline security assessments prior to the ransomware attack,"[84] none were actually executed, and TSA had no way to force Colonial to do so.

Following the attack, TSA sprang into action and introduced two mandatory directives. Those directives have been mostly criticized by pipeline operators who "have voiced concerns about aggressive timelines and impacts on safety if major equipment changes become necessary."[85] Kilovaty discusses in great length the risks of

---

of-5m-nothing-to-colonial-pipeline-which-has-paid-hundreds-of-millions-in-dividends-to-billionaire-koch-family/?sh=6710f6dc2e6e (reporting that the Colonial Pipeline Company has $3.1 billion in assets).

[79] *See* Soraghan, *supra* note 71 ("DOT's Pipeline and Hazardous Materials Safety Administration is seeking to fine Colonial nearly $1 million for control room failures.").

[80] *See id.* (pointing out that the PMHSA hearing focused on the federal minimum requirements for pipeline control rooms).

[81] 49 U.S.C. § 114(d); *see* Kilovaty, *supra* note 23, at 119 (stating that the Aviation and Transportation Security Act extends the TSA's security responsibilities to pipelines).

[82] Kilovaty, *supra* note 23, at 119.

[83] *See* Ari Natter & Jennifer A. Dlouhy, *U.S. to Step Up Pipeline Cyber Rules in Wake of April Attack*, BLOOMBERG L. (July 19, 2021, 12:23 PM), https://www.bloomberglaw.com/bloomberglawnews/environment-and-energy/X3GB3J48000000?bna_news_filter=environment-and-energy#jcite (characterizing the TSA system as one that has relied on "self-reporting" and "voluntary measures").

[84] Kilovaty, *supra* note 23, at 105.

[85] Samantha Schwartz, *Pipeline Operators Raise Concerns over Aggressive TSA Cybersecurity Directives*, CYBERSEC. DIVE (July 28, 2021),

embracing TSA as a cybersecurity tzar for the pipeline sector: "The TSA has been criticized for lacking the expertise and tools to effectively regulate cybersecurity in the pipeline context."[86] Kilovaty thus supports calls made by the Biden Administration to move the entire area of cybersecurity regulation for pipelines from TSA to FREC, which currently is only responsible for the regulation of cybersecurity for the electric sector.[87]

IV. COLONIAL PIPELINE AND THE LEGISLATIVE RESPONSE

With limited regulatory enforcement and clear tension around authorities, expertise, and the scope of mandatory guidelines, it is clear why regulatory responses to the Colonial Pipeline incident are best understood as weak and ineffective. They reflect the complexity of our federal government and the distributed and decentralized governance frameworks surrounding critical infrastructure. Combined with the exceeding privatization of these sectors, it is not surprising that regulatory agencies have been slow to generate meaningful results.

In the vacuum generated by both judges and regulators, legislators might find an opportunity to develop policy and promote

---

https://www.cybersecuritydive.com/news/pipeline-cyber-security-tsa-requirements/604001/. For a detailed discussion of both directives see Kilovaty, *supra*, note 23, at 119–25.

[86] Kilovaty, *supra* note 23, at 126. For further analysis, see *id.* at 126–28.

[87] *See id.* at 128 ("Currently, there are some tensions between the TSA and the Federal Energy Regulatory Commission (FERC), an entity within the Department of Energy (DOE) responsible for the electric sector's cybersecurity regulation. Two FERC Commissioners have expressed their concern as to the adequacy of the TSA as a pipeline cybersecurity regulator. Their observation included a call for a different agency to regulate pipeline cybersecurity, one that 'fully comprehends the energy sector and has sufficient resources to address this growing threat.' In the same vein, the Biden Administration announced its support to move pipeline cybersecurity from the TSA to the FERC. Certain House representatives even proposed the Energy Product Reliability Act, to allow the FERC to regulate the pipeline's cybersecurity."). In fact, "[t]he Pipeline Security Act" (H.R. 3243) was introduced by Congressman Emanuel Cleaver (D-MO)." MICHAEL W. GRAY, OIL & GAS E-REPORT, COLONIAL PIPELINE 2021 RANSOMWARE INCIDENT AND RESPONSES 7 (Dec. 2022), https://www.cailaw.org/media/files/IEL/Publications/ereport/2022/issue-4.pdf. The Act was intended to "enhance the ability of TSA . . . to guard pipeline systems against cyberattacks, terrorist attacks, and other threats. This measure codifies TSA's Pipeline Security Section and clarifies TSA's statutory mandate to protect pipeline infrastructure." *Id.* The Act did not pass. *Id.*

reform. Indeed, in March 2022, the Strengthening American Cybersecurity Act of 2022 (SACA) passed the U.S. Senate.[88] Created in the wake of the Russian war of aggression on Ukraine and U.S. sanctions regime, the Act was hailed as an important tool necessary to deter and disrupt retaliatory cyberattacks against our critical infrastructure.[89] Some celebrated the legislation by arguing that it would "significantly bolster and modernize federal cybersecurity."[90] I'm afraid that SACA will achieve none of that.

For starters, SACA packaged together several pieces of legislation and therefore was mistakenly called by certain media outlets and civil society an "omnibus cybersecurity bill."[91] However, SACA is far from omnibus in that it does not offer a meaningfully omnibus solution to core cybersecurity problems. While combining a few bills,[92] it is still unbelievably narrow, focusing almost entirely on reporting duties for critical infrastructure companies associated with certain types of cyberattacks and ransomware payments.[93]

---

[88] Strengthening American Cybersecurity Act of 2022, S. 3600, 17th Cong. (2022). SACA's reporting and info-sharing obligations were ultimately repackaged and adopted by Congress and signed into law by President Biden on March 15, 2022, as part of the Consolidated Appropriations Act of 2022.

[89] *See, e.g.*, *Portman, Peters Introduce Landmark Legislative Package to Strengthen Public and Private Sector Cybersecurity*, COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFAIRS (Feb. 8, 2022), https://www.hsgac.senate.gov/media/minority-media/portman-peters-introduce-landmark-legislative-package-to-strengthen-public-and-private-sector-cybersecurity_/ (calling the Act a "landmark legislative package that would significantly enhance [the United States'] ability to combat ongoing cybersecurity threats").

[90] *Id*.

[91] *See e.g.*, *US Senate Passes Omnibus Cybersecurity Bill*, INT'L ASS'N OF PRIV. PROS. (Mar. 2, 2022), https://iapp.org/news/a/senate-passes-omnibus-cybersecurity-bill/ ("The U.S. Senate passed . . . a package of bills . . . to enhance U.S. cybersecurity.").

[92] The Act combines the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Pub. L. No. 117-103, 136 Stat 49, the Federal Information Security Modernization Act of 2022, H.R. 6497, 117th Cong. (2d Sess. 2022), and the Federal Secure Cloud Improvement and Jobs Act of 2021, S. 3099, 117th Cong. (1st Sess. 2021).

[93] For a summary of the Act, see Meredith Sherman & Greenbaum, Rowe, Smith & Davis LLP, *An Overview of the Strengthening American Cybersecurity Act*, JDSUPRA (Apr. 1, 2022), https://www.jdsupra.com/legalnews/an-overview-of-the-strengthening-2869067/; *see also* GRAY, *supra* note 87, at 8–9. (summarizing SACA). Namely, the Act establishes that a "covered entity" shall report a "covered cyber incident" to CISA not later than seventy-two hours after the covered entity reasonably believes that the covered cyber incident has occurred. GRAY, *supra* note 87, at 8. Further, a "covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity shall report the payment to [CISA] not later than 24 hours after the ransom payment has been made." *Id*. The Act defined

SACA's focus on reporting and information sharing, while obviously important, cannot replace the need to address other areas of cybersecurity law and policy. The Act offers no new analytical frameworks to be employed by courts or regulators, it generates few, if any, new enforcement tools, and it fails to respond to the need for generating liability standards that could substantively impact pervasive incentive structures on the market.

Moreover, it is currently unclear which entities will be affected by SACA. The Act requires the CISA director "to publish a notice of proposed rulemaking no later than 24 months after the date of enactment of the Act. Then, no later than 18 months after the proposed rulemaking, the Director shall issue a final rule for final implementation."[94] In other words, we have a couple more years until it is clear which critical infrastructure companies are even subject to the new Act.[95]

V. CONCLUSION: THE HOLISTIC APPROACH TO CYBERSECURITY LAW AND THE FUTURE OF CRITICAL INFRASTRUCTURE

At this point we may wish to return to the question that launched this investigation. Was CISA Director Wales statement—that the

---

"covered entities" as "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 2242(b)." *Id.* For more on this rule, see *infra* note 94 and accompanying text.

[94] Taft Stettinius & Hollister LLP, *Strengthening American Cybersecurity Act of 2022*, LEXOLOGY: PRIV. & DATA SEC. INSIGHT (Apr. 8, 2022), https://www.lexology.com/library/detail.aspx?g=cdc5fdd0-6968-4d70-b0b7-d96278c4cbe0.

[95] It is important to acknowledge that while SACA is the primary legislation that the Senate passed in response to the Colonial Pipeline incident, it is by no means the only legislation that was passed. Some legislation was enacted on December 27, 2021, as part of the National Defense Authorization Act for Fiscal Year 2022, S. 1605, 117th Cong. (1st Sess. 2021). They include: the CISA Cyber Exercise Act, which "establishes a National Cyber Exercise program within CISA to promote more regular testing and systemic assessments of preparedness and resilience to cyber attacks against critical infrastructure"; the Domains Critical to Homeland Security Act, which "authorizes DHS to conduct research and development into supply chain risks for critical domains of the United States economy and transmit the results to Congress"; and the Cybersecurity Vulnerability Remediation Act, which "authorize[s] CISA to assist critical infrastructure owners and operators with mitigation strategies against the most critical, known vulnerabilities." GRAY, *supra* note 87, at 6–7.

Colonial Pipeline attack was a "galvanizing event"—an accurate statement?[96] Based on all we surveyed so far, the answer is a resounding no. The kneejerk litigatory, regulatory, and legislative responses that the Colonial Pipeline ransomware generated were casebook examples of all that is wrong with our existing cybersecurity law and policy ecosystem. It simply affirms all that Solove and Hartzog have already identified:

> With a few exceptions, data security law generally doesn't look too far beyond the blast radius of a data breach. The law often fails to hold the right actors responsible, often worsening the damage that data breaches cause. Obsessed with data breaches, the law fails to take the right preventative steps and fails to assign responsibility on the actors who can prevent and mitigate the harm . . . .[97]

My original intention was to stop my Article here with a set of general recommendations. I planned to suggest that what is needed at this moment in time is a real and omnibus regulatory shakeup within the federal government, the kind that is truly rooted in a whole-of-government reform. But before I could put ink on paper, reports have begun to surface about a new Biden Administration National Cyber Strategy (NCS).[98]

The NCS follows an intensive study conducted by the White House National Security Council under the direction of Deputy National Security Adviser Anne Neuberger.[99] The study included an "analysis of the state of regulation for all 16 critical infrastructure sectors."[100]

---

[96] *See* Jones, *supra* note 25 (detailing that Director Wales stated that "Colonial Pipeline was a galvanizing event for the country").

[97] SOLOVE & HARTZOG, *supra* note 26, at 68.

[98] *See* David Jones, *National Cybersecurity Strategy to Debut Within Months, White House Official Says*, CYBERSEC. DIVE (Oct. 19, 2022), https://www.cybersecuritydive.com/news/us-cyber-strategy-chris-inglis/634585/ (reporting that Director Inglis, while speaking at a conference in October of 2022, "previewed the security strategy").

[99] *See* Starks, *supra* note 31 (detailing the reason for initiating the study completed under Anne Neuberger).

[100] *Id.*

The thirty-five-page document is broken down into five main pillars, each broken down into further set of strategic objectives.[101] The pillars include: (1) defending critical infrastructure; (2) disrupting and dismantling threat actors; (3) shaping market forces to drive security and resilience; (4) investing in resilient future; and (5) forging international partnerships to pursue shared goals.[102] The regulations that NCS proposes under each of the strategic objectives are responsive to the gaps identified and to market failures generated by the current state of our critical infrastructure ecosystem.[103]

The Strategy puts significant focus on regulation. It notes that "Regulation can level the playing field, enabling healthy competition without scarifying cybersecurity or operational resilience."[104] The NCS further addresses the issue of liability. It calls "to shift liability onto those entities that fail to take reasonable precautions to secure their software while recognizing that even the most advanced software security programs cannot prevent all vulnerabilities."[105]

Finally, the NCS under the second pillar of disrupting and dismantling, "authorizes U.S. defense, intelligence, and law enforcement agencies to go on the offensive, hacking into the computer networks of criminals and foreign governments, in retaliation to—or preempting—their attacks on American networks."[106]

The NCS is extremely promising. The Strategy is responsive to the kind of "holistic approach" to data security law that Solove and Hartzog have been promoting.[107] Among other things the NCS

---

[101] NCS, *supra* note 30.

[102] *Id.*

[103] *See* Starks, *supra* note 31 (stating that the NCS is in response to the gaps found in regulation, regulatory authority of agencies, and the failures found in voluntary adherence to cybersecurity in critical infrastructure sectors).

[104] NCS, *supra* note 30, at 8.

[105] *Id.* at 20–21.

[106] Fred Kaplan, *When It Comes to Cybersecurity, the Biden Administration Is Getting Much More Aggressive*, SLATE (Jan. 17, 2023, 5:35 AM), https://slate.com/news-and-politics/2023/01/biden-cybersecurity-inglis-neuberger.html.

[107] *See* SOLOVE & HARTZOG, *supra* note 26, at 192 (calling for a broad approach established around foundational concepts to better equip the law to handle this evolving issue of data security).

seems to be "more proactive and less reactive"[108] and aims to "impose responsibility on all the actors in the data ecosystem that play a contributory role in data breaches."[109] These are core tenants of the holistic approach.

That said, the devil is in the details. There is more to learn and understand about the Strategy, and how it will be implemented, before we can assess how big of a tectonic shift it really represents. I also have some concerns about the parts of the program that have already been revealed. Most importantly, the NCS suffers from certain limitations inherent in the nature of our federal democracy and the privatized features of our critical infrastructures. For example, it is unclear how the Federal government intends to set out liability regimes currently subject to state law and common law. Another concern is Congress. The NCS promises that the Federal Government will "use existing authorities to set necessary cybersecurity requirements in critical sectors."[110] The NCS, however, admits that where there are "gaps in statutory authorities to implement minimum cybersecurity requirements or mitigate related market failures" all that the Administration can do is "work with Congress to close them."[111] It is unclear how a dysfunctional partisan Congress could secure the dramatic goals that the NCS sets out to achieve.[112] Finally, the commitment to engage in more aggressive cyber offensive operations abroad generates real risks for destabilization of the datasphere and puts into question America's

---

[108] *Id.*

[109] *Id.* at 194–95.

[110] NCS, *supra* note 30, at 8.

[111] *Id.*

[112] *See* Edward G. Carmines & Matthew Fowler, *The Temptation of Executive Authority: How Increased Polarization and the Decline in Legislative Capacity Have Contributed to the Expansion of Presidential Power*, 24 IND. J. GLOB. LEGAL STUD. 369, 376–84 (2017) (detailing the increasing polarization and diverging ideological viewpoints in Congress over time has resulted in a far less productive modern Congress with fewer legislation passed and is "underperforming as a problem-solving institution"). Indeed, republican congressmen on the Hill were resistant to the NCS, "arguing that most of what they have seen from the strategy 'is a push for more red tape.'" Jonathan Greig, *In Mixed Response to White House Cyber Strategy, House Republicans Focus on Regulations*, THE REC. (Mar. 3, 2023), https://therecord.media/national-cybersecurity-strategy-republican-reaction-green-garbarino.

leadership in norm-setting for responsible behavior in cyberspace.[113]

At the time of writing, we can only guess whether and to what extent the NCS will be implemented, and what its effects will be. There is reason for hope but also reason for doubt. Future work will be necessary to determine whether the NCS represents the kind of shakeup that our government surely needs to prevent another Colonial Pipeline.[114]

---

[113] Yuchong Li & Qinghui Liu, *A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments*, 7 ENERGY REPS. 8176, 8177 (2021) (detailing the potential consequences of engaging in aggressive cyber tactics on the world stage such as destruction of public confidence, escalation of physical conflicts, and "catastrophic destruction . . . to the country's image at the international level").

[114] In June 2023, a massive ransomware attack successfully targeted major U.S. universities, state governments, and federal agencies, including the Department of Energy. The incident demonstrates that we have good reason to remain concerned about critical infrastructure cybersecurity, even post-NCS. *See* Sean Lyngaas, *Exclusive: US Government Agencies Hit in Global Cyberattack*, CNN (June 15, 2023), https://www.cnn.com/2023/06/15/politics/us-government-hit-cybeattack/index.html.