South Dakota Law Review

Volume 68 | Issue 3

2023

Something Old, Something New: Devising Legal Solutions for Combating Cybersecurity Risks in the Agribusiness Sector

John G. Browning

SOMETHING OLD, SOMETHING NEW: DEVISING LEGAL SOLUTIONS FOR COMBATING CYBERSECURITY RISKS IN THE AGRIBUSINESS SECTOR

HON. JOHN G. BROWNING†

Agriculture is a key pillar of the American economy, as well as a vital part of our Critical National Infrastructure. Thanks to technological advances, "smart farming" has resulted in higher yields as well as advances in food safety, crop sustainability, and harvest efficiency. Yet these advances have come with a risk: vulnerability to cyberattacks and data privacy concerns. This article discusses that risk and proposes both "old" and "new" legal solutions. The "old" solution is the Cold War-era Defense Production Act, while the "new" solution is drafting and implementing a federal law on cybersecurity and data protection specific to the agribusiness sector, similar to what HIPAA has meant to the healthcare field.

I. INTRODUCTION

In May 2021, management of multinational meatpacking giant JBS revealed that a ransomware attack had hit the company, forcing the company to shut down twenty percent of the beef-packing plants in the United States, as well as numerous pork and poultry processing facilities in states like Texas, Iowa, Nebraska, and Colorado.[1] Ultimately, JBS paid the Russian hackers behind the crippling attack 11,000,000 in cryptocurrency to regain control of their computer systems.[2] This incident and others like it have exposed a grim reality of the vital agribusiness sector: that with the technological advances that have enabled incredible increases in yields and sustainability also come greater cybersecurity vulnerabilities. What legal measures can be taken to address these and similar cybersecurity risks to such an important part of our Critical National Infrastructure ("CNI")? Even more recently, Dole Operations PLC was brought to a crashing halt in February 2023 by a cyberattack.[3] The ransomware attack showed how vulnerable the "just in time" nature of food supply chains can be. The agricultural giant notified its retailers and quickly shut down its cyber-systems, hoping to limit the number of

† Justice (ret.) John G. Browning has been a civil litigator for over thirty-three years, focusing his practice on the defense of civil litigation and appeals in state and federal court. Prior to returning to private practice in 2021, he served as a justice on Texas's Fifth District Court of Appeals. Justice Browning also serves as Distinguished Jurist in Residence at Faulkner University's Thomas Goode Jones School of Law and as Chair of the Institute for Law & Technology at The Center for American and International Law. He is a graduate of Rutgers University and the University of Texas School of Law.

1. *Meat Giant JBS Pays $11M in Ransom to Resolve Cyber-Attack*, BBC (June 10, 2021), https://perma.cc/BQD7-AMTC.

2. *Id.*

3. Sean Lyngaas, *Cyberattack on Food Giant Dole Temporarily Shuts Down North American Production, Company Memo Says*, CNN (Feb. 22, 2023), https://perma.cc/QCS4-GKYM.

grocers who could not stock Dole salads.[4] Dole has four processing plants in the United States and more than 3,000 employees.[5] Although it was not immediately clear how long the company was offline, Senior Vice President Emanuel Lazapolous called the impact "limited" and said "[a]ll our businesses are implementing our Crisis Management Protocol to resume 'business as usual' post haste, inclusive of our Manual Backup Program, if needed."[6]

This article will discuss how, in the absence of self-regulation by the agribusiness industry itself, the answer may very well lie in federal intervention—specifically by implementing legal solutions that are both old and new. The "old" approach consists of invoking the Defense Production Act ("DPA") to mandate industry-wide adoption of heightened cybersecurity measures. As this article shows, although the DPA itself dates back to 1950, ample recent precedent exists for its invocation, including the Biden administration's use of it in 2021 to speed up vaccine production and in 2022 to address the baby formula shortage. The "new" approach consists of adopting a federal data protection/data privacy law that is specific to the unique needs of the agribusiness sector. Here again, precedent exists for such a step. The Gramm-Leach-Bliley Act, for example, regulates data practices in the financial services industry, while the Health Insurance Portability and Accountability Act ("HIPAA") governs data protection and data privacy in the healthcare arena.

This article begins with an introduction to the various types of cybersecurity risks impacting the agribusiness sector in the wake of the technological advances ushered in by the era of "smart farming." This will entail an examination of not only the JBS ransomware attack and other cyber breaches in the agribusiness field, but also the lessons to be learned from such episodes. The article then moves on to discuss what would be involved in invoking an "old" legal solution—the DPA—in order to impose the cybersecurity protections needed to safeguard this critical component of the American economy. Afterward, the article examines what the "new" approach might consist of, including adoption of a national regulatory framework, for cybersecurity in the agribusiness sector. As the article argues, the industry's failure to adopt its own guidelines when the issue was initially broached in 2015, as well as the flaws inherent in a state-by-state "patchwork quilt" of cybersecurity regulation, make a national standard preferable.

Agriculture is a key pillar of the American economy, and protecting those involved in it from cyberthreats is crucial. With the very technology that has increased productivity and sustainability also presenting heightened risks of disruption, legal solutions on the federal level—something old and something new—present the best hope of protecting our nation's farmers and livestock producers.

---

4. *Id.*

5. *Id.*

6. Teri Robinson, *Ransomware Attack Brings Dole Operations to a Temporary Halt*, SECURITY BOULEVARD (Feb. 27, 2023), https://perma.cc/J6SZ-7VR7.

II. THE IMPORTANCE OF TECHNOLOGY TO THE AGRIBUSINESS SECTOR

American agriculture has undergone sweeping changes in the last sixty-plus years, with a wide variety of impacts ranging from changing population dynamics to evolving dietary preferences. But arguably the single most significant factor to impact agribusiness is technology. In 1970, there were about four million farms in the United States, but by 2015, there were only about half that many.[7] The total area of farmed land decreased just slightly in that time, with the average farmer in 2015 farming 444 acres, compared to less than 300 acres per farmer in 1960. Yet despite farming less land, gains in productivity have resulted in an output 2.5 times greater in 2015 than in 1960.[8] Productivity growth in such staple commodities as corn, soy, and wheat have more than doubled over the last fifty years.[9] How have such gains been achieved? Crop yield has become more productive and more efficient thanks to technology, the development of "smart" agricultural systems, and the practice of precision agriculture (sometimes called "smart farming").

In precision agriculture, use of "smart" technology and management has meant more efficient use of seed, water, crop nutrients, and herbicides and pesticides, all with the overall goal of increasing production efficiency. Such "smart farming" enables more precise and timely allocation of on-farm resources during the growing season and through harvest and off-farm transport of the crop. This "precision agriculture" has been defined as "a management system that is information and technology-based, is site-specific and uses one or more of the following sources of data: soils, crops, nutrients, pests, moisture, or yield, for optimum profitability, sustainability, and protection of the environment."[10]

There are many examples of smart technologies that make up "precision agriculture." There are sensors integrated into agricultural implements that determine the rate of application of water, pesticides, and herbicides. Autonomous robots, such as robotic milkers, relieve labor shortages on dairy farms, while autonomous planters and harvesters have become so advanced that they are rapidly diminishing the need for farmers to actually drive their equipment. GPS receivers, yield monitors, and other technologies, combined with smartphones, computers, and tablets, allow agricultural producers to collect and store a vast amount of data about their farming operations—whether that is weather data, machine data (information about the farm equipment itself), or agronomic data (information about the crop yields and types of products applied).

---

7. *The Number of U.S. Farms Continues to Decline Slowly*, U.S. DEP'T AGRIC. (last updated June 3, 2022), https://perma.cc/ME7T-8VAD (noting that the number of farms has leveled off at about 2.01 million).

8. *Productivity Growth is Still the Major Driver of U.S. Agricultural Growth*, U.S. DEP'T AGRIC. (last updated Jan. 6, 2022), https://perma.cc/532H-FLQW.

9. *Crops and Livestock Products*, FOOD & AGRIC. ORG. U.N. (2016), https://www.fao.org/faostat/en/#data/QCL.

10. *Precision Agriculture: NRCS Support for Emerging Technologies*, U.S. DEP'T AGRIC. 3 (June 2007), https://perma.cc/RG6P-X26Z.

Smart irrigation systems, using sensors tied to subsurface drip irrigation, enable precise field conditions to be closely monitored, thereby allowing water to be applied at the right time and in the right amount to maintain crop health.[11] Smart cultivators identify and eliminate weeds in fields, reducing if not eliminating the practice of broadly applying herbicides across the entire field. Agricultural drones help ensure that farmers have real time crop monitoring data so that crop inputs can be efficiently used.[12] The data this technology generates provides greater insight into a farm's operating efficiency and production capacity. As a result, drone technology has become vital for farm lenders (like the $330 billion American Farm Credit System) seeking to determine the value of the crop and other agricultural collateral that forms the basis of a production loan. Use of such technology, therefore, can reduce lender risk and increase the availability of capital for farmers.

Other technologies used in precision agriculture involve satellites, differential global positioning systems, continuously operating reference stations, and real-time kinematic ("RTK") positioning. These technologies provide information that enables more precise seed planting, row crop alignment, and application of agricultural inputs like nitrogen. A tractor, for example, might have an RTK receiver that communicates with a base station, enabling farmers to auto-steer equipment, perform precision planting and cultivation, and engage in precise land leveling and tillage. Mapping technologies, sometimes in conjunction with soil sensors, can be used to collect data about soil texture, porosity, water-holding and drainage capacity, temperature, and other features that can inform planting rates, fertilization application, and other critical activities.

Just like crops, use of technology is crucial to precision livestock farming. Production can be optimized by allowing ranchers/farmers to collect information that will assist in recognizing disease in animals, increasing feed efficiency, and saving on labor and feed costs. Technology, which can be customized by animal, supports not just automated milking systems but also electronically governed feeding and health monitoring. From feed sensors and radio frequency ID tags to biosensors implanted on animals, ranchers and farmers can gather and manage a dizzying array of data. This includes data on animal feed consumption, weight gain, feedlot movement, lameness, meat composition and quality, antibiotic use, and milk production. Sensors can measure an animal's body temperature, detect stress, analyze sound, and even detect pH and sweat composition. Microphones can monitor cough sounds to localize respiratory infections in pigs, while noise sensors in poultry plants help determine the effect of environment on chick health.

The importance of technology for the agribusiness sector is, of course, not limited to farmers and ranchers themselves and their efforts to increase efficiency and productivity in a notoriously low-margin industry. Precision agriculture is incredibly important for those industries that support agriculture, including

11. *Reducing the Drip of Irrigation Energy Costs*, USAID WATER TEAM (July 18, 2017), https://perma.cc/Z7BH-WM9N.

12. Savaram Ravindra, *IOT Applications in Agriculture*, IOT FOR ALL (June 30, 2020), https://perma.cc/U6H4-2K8T.

fertilizer and pesticide suppliers, seed companies, feed suppliers, equipment manufacturers and providers, and even financial institutions. In addition, precision agriculture is important to the organizations that support agriculture, ranging from local farm organizations and county-level agricultural extension offices to trade associations, vocational schools and university agricultural programs, and governmental agencies. Some of these entities, such as agricultural programs in vocational schools and universities, have begun providing the necessary training in using precision agriculture-related technologies. Another sector impacted by precision agriculture is comprised of those companies that rely on data and final products from the producers themselves. This includes grain dealers, food/meat processors, commodities brokers, crop insurers, and energy companies—all of which depend heavily on accurate data and quality final products in order to ensure the safety of the food products reaching the market. Related to this is yet another group: those charged with maintaining human and animal health and safety, including regulatory agencies like the U.S. Department of Agriculture ("USDA"). And, of course, consumers are the ultimate group affected by precision agriculture's ability to improve not just productivity, but also the health of livestock and the safety of the food that we buy.

III. CYBERTHREATS TO THE AGRIBUSINESS SECTOR

Unfortunately, "smart farms" are also hackable farms. The ever-increasing use of technology in the agribusiness sector has been accompanied by a broad range of cyberthreats. In a survey conducted by the *Farm Journal*, fifty-three percent of farmers reported having concerns about data security.[13] In another study of farmers and agribusiness owners, over half the respondents reported being victims of a computer security incident, demonstrating that those in the agribusiness sector are as vulnerable to cyberthreats as any other industry.[14] And it is not just an American problem. Xing Yang of Nanjing Agricultural University in China has researched the subject of how smart agriculture can increase the global food system's efficiency in an effort to alleviate global malnutrition and hunger. According to Yang, agricultural cybersecurity is not given enough attention, and part of the challenge rests with the fact that agricultural "Internet of Things" ("IoT") "applications usually have unique characteristics that can give rise to security issues."[15] While field agriculture might be facing threats from damage to a facility, greenhouse cultivation is vulnerable to control system intrusions, while poultry and livestock breeding may be hit with sensor failures. Specific agricultural equipment may face unique threats. For example, in looking

13. Margy Eckelkamp, *FJ Pulse: Less Than 20% of Farmers Confident in Their Data Security*, FARM J. (Mar. 9, 2020), https://perma.cc/4GZX-WE2D (revealing that twenty-three percent of respondents reported that they did not think their data was secure, and twenty percent reporting "concerns" with their data security, while only nineteen percent stated that they felt confident in their data security).

14. Andrew Geil et al., *Cyber Security on the Farm: An Assessment of Cyber Security Practices in the United States Agriculture Industry*, 21 INT'L FOOD & AGRIBUSINESS MGMT. REV., no. 3, 317 (2018).

15. Payal Dhar, *Cybersecurity Report: "Smart Farms" are Hackable Farms*, IEEE SPECTRUM (Mar. 15, 2021), https://perma.cc/6HB3-W7HY.

at solar insecticidal lamps, Yang's study found "that the lamp's high voltage pulse affects the data transmission from Zigbee-based IoT devices and data acquisition sensors."[16] Data acquisition technologies, on the other hand, are vulnerable to everything from unauthorized access and privacy leaks to malicious attacks.

Just what kind of cyberthreats does an entity in the agribusiness sector face? In one possible scenario, a cyber intruder could introduce "rogue data" into the cellular, Bluetooth, or Wi-Fi networks and "tell" an irrigation system to under water or over water crops, thus destroying them.[17] Or, a hacker could identify a vulnerability in the operating system of a piece of harvesting equipment (such as a combine or tractor) and shut down a whole fleet of harvesting vehicles, thus allowing the window of time to harvest crops to expire—resulting in the loss of that year's harvest. If a terrorist wanted to cause a major disruption to the livestock sector, he could exploit cyber weaknesses in livestock health technology and introduce a highly contagious infectious agent into a livestock operation such as foot-and-mouth disease.[18] In fact, actual infection or disease would not even be necessary. All a bad actor would have to do is hack into a livestock producer's data system, manipulate data to make it appear that the herd is infected, and then blast that information out on the internet and watch it go viral. The fallout from such news would take weeks to mitigate, and likely lead to stock market losses, adverse effects on exports, and damage to public trust.[19] And, finally, of course, there is also the "tried and true" attack of employing ransomware—holding a company's data hostage for a ransom payment.

These scenarios are not just hypotheticals. In 2018, the U.S. Council of Economic Advisers reported that the agricultural sector experienced eleven cyber incidents in 2016.[20] While this might seem relatively low compared to other business sectors like manufacturing or transportation, the increasing reliance on technology in "smart" or precision agriculture makes the devastating potential of a crippling cyberattack very real. Consider, for example, the 2017 cyber-infrastructure disaster in the Maersk shipping line. A malware attack resulted in a complete IT shutdown for the company. While the full IT system was restored over a ten-day period, Maersk reverted to manual logistics. The cyberattack caused a twenty percent drop in volume and a reported $300 million in losses for the company.[21]

16. *Id.*

17. *Threats to Precision Agriculture*, 2018 PUBLIC-PRIVATE ANALYTIC EXCH. PROGRAM 1, 5 (2018), https://perma.cc/2B5X-SLRK.

18. *Id.*

19. *Id.*

20. *The Cost of Malicious Cyber Activity to the U.S. Economy*, COUNCIL OF ECON. ADVISERS 1, 19 (Feb. 2018), https://perma.cc/UPM9-WL3F.

21. Jonathan Saul, *Global Shipping Feels Fallout from Maersk Cyber Attack*, REUTERS (June 29, 2017), https://perma.cc/AP2U-AL33. Industry insiders estimated the loss at closer to $500 million; Maersk operations came to a standstill, as ships could not be located at sea and could not be unloaded at port. Michael Mimoso, *Maersk Shipping Reports $300 M Loss Stemming from NotPetya Attack*", THREATPOST (Aug. 16, 2017), https://perma.cc/VW8R-C5XA.

Examples of specific cybersecurity incidents involving the agribusiness sector abound. For example, in a 2021 speech on the U.S. Senate floor, Iowa Senator Chuck Grassley reported several attempted attacks on agricultural systems, including one against an Iowa grain cooperative that a Russian cybercrime ring targeted demanding a $5.9 million ransom. According to a Crowdstrike intelligence report, out of an estimated 160 or so such hacking groups that the security company actively tracks, at least 13 were specifically targeting the agriculture industry.[22] According to the U.S. Federal Bureau of Investigation ("FBI"), at least eight hacks of agriculture companies took place in 2021.[23]

That Iowa grain cooperative mentioned by Senator Grassley was just one of six experiencing ransomware attacks between September 15 and October 6, 2021. The attackers employed a variety of different ransomware agents, including BlackMatter, BlackByte, Suncrypt, and Conti. The results varied as well; while some grain cooperatives lost only certain functions like administrative controls, others had to completely halt production.[24] According to the FBI, these attacks in 2021 and two additional ones in early 2022 were part of a coordinated effort "during critical planting and harvest[ing] seasons, disrupting operations, causing financial loss, and negatively impacting the food supply chain."[25] At least one 2021 ransomware attack was an indirect one. In July of that year, cyber attackers infected the network of a business management software company with the "HelloKitty/FireHands" ransomware variant and demanded a $30,000,000 ransom.[26] A number of that software company's clients experienced secondary ransomware attacks, including several agricultural cooperatives.

According to the same FBI report, in February 2022, "a company providing feed milling and other agricultural services" reported two unsuccessful attacks by a hacker to gain access, possibly for purposes of launching a ransomware assault.[27] And in March 2022, a "multi-state grain company suffered a Lockbit 2.0 ransomware attack,"[28] which had the potential to disrupt the spring planting season—since the company not only performed grain processing, but provided seed, fertilizer, and logistics services as well.[29]

Ransomware attacks on cooperatives are hardly the only threat looming. Individual farms may be targeted in a variety of ways. In August 2021, "white hat" hackers released a video demonstrating the vulnerabilities of self-propelled tractors and farming equipment operated by GPS signal. Just like hacking in to

22. Shane Tews, *Cybersecurity in Agriculture: Don't Forget About Mobile*, AEIDEAS (Nov. 9, 2021), https://perma.cc/H9WL-8NG6.

23. *Id.*

24. *Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons*, FED. BUREAU INVESTIGATION (Private Industry Notification) (Apr. 20, 2022), https://perma.cc/NT4F-WF5V. At least two of the cooperatives were later identified as Iowa's NEW Cooperative and Minnesota's Crystal Valley Cooperative.

25. *Id.*

26. *Id.*

27. *Id.*

28. *Id.*

29. *Id.*

remotely "hijack" a car like a Tesla, these "white hats" showed how such farming equipment could be hijacked and interfered with remotely.[30] By hacking signals from sensors, threat actors can tamper with levels of fertilizer, pesticides, or water used for irrigation.

Attacks on a water supply are not merely the subject of conjecture. In February 2021, the west coast of Florida experienced a cyberattack on its water supply when a hacker seized control of Oldsmar, Florida's Industrial Control System and proceeded to raise the level of sodium hydroxide to 100 times the normal level.[31] More commonly known as lye, sodium hydroxide poisoning can cause burns, vomiting, bleeding, and severe pain. Fortunately, the cyberbreach was detected and secured before anyone was injured—but the potential for harm from such an attack is clear. And for anyone who doubts either the capability of a pipeline being hijacked by cybercriminals or the chaos that can ensue, consider the ransomware attack on the Colonial Pipeline in May 2021—the largest attack on an oil infrastructure target in the history of the United States, and one which not only disrupted fuel supplies itself, but also spawned fuel shortages, panic buying, long lines at the pumps, and other chaos.[32]

It is no small wonder, then, why both the U.S. and Canadian governments listed agriculture (and water) as CNI, and why cybersecurity in the agriculture sector has received increased attention and resources in recent years. In March 2021, the Canadian government announced increased funding to enhance the agriculture sector's cybersecurity, noting the "critical and increasingly interconnected" nature of agriculture.[33] In 2017, the U.S. Department of Defense ("DOD") funded the National Strategic Research Institute at the University of Nebraska to begin cyberbiosecurity research, with the goal of creating a list of preventative procedures to reduce vulnerabilities to cyberattacks.[34]

A. THE JBS ATTACK

Perhaps no incident illustrates the vulnerability of the agribusiness sector to cyberattack better than the May 2021 ransomware attack on JBS, the Brazilian-based meatpacking multinational company—an attack which forced the meat processing giant to shut down twenty percent of the beef-packing plants in the United States as well as pork and poultry processing facilities in Texas, Colorado, Nebraska, and Iowa for days. Founded by Brazilian rancher José Batista Sobrinho as a slaughtering operation in 1953, JBS has more than 150 plants in 15 countries,

30. Stephanie Mercier, *Cyber Security Concerns in the U.S. Agricultural Sector*, FARM J. (Oct. 19, 2021), https://perma.cc/DX67-3F34.

31. John Meah, *Food, Farms and Cyber Security: Agriculture Faces a Growing Problem*, TECHOPEDIA.COM (Aug. 12, 2021), https://perma.cc/QL8R-N5S7.

32. Gloria Gonzalez et al., *"Jugular" of the U.S. Fuel Pipeline System Shuts Down After Cyberattack*, POLITICO (May 8, 2021), https://perma.cc/7VRY-HW5J.

33. Meah, *supra* note 31.

34. Tiffany Drape et al., *Assessing the Role of Cyberbiosecurity in Agriculture: A Case Study*, 9 FRONTIERS IN BIOENGINEERING & BIOTECHNOLOGY (Aug. 19, 2021), https://perma.cc/3UVX-38DE.

and is the world's largest beef producer, the world's largest poultry producer, and the world's second-largest pork producer. It has 245,000 employees.[35]

On May 30, 2021, JBS USA's CEO, Andre Nogueria, announced that the company had been forced to halt operations in North America and Australia as a result of being "the target of an organized cybersecurity attack affecting some of the servers supporting its North American and Australian IT systems."[36] JBS reported that it had shut down all affected systems, notified relevant authorities, and retained third-party IT experts to resolve the situation. JBS further announced that "the company's backup servers were not affected" and that it was "actively working with an [i]ncident [r]esponse firm to restore its systems as soon as possible."[37] As a result of the attack, however, JBS was forced to cease operations at thirteen of its meat processing plants in the United States.

JBS did not identify who the attackers were or even explicitly mention a ransomware attack. However, the FBI identified the culprits as REvil, a criminal network of ransomware hackers that first came to prominence in 2019.[38] While the REvil developer team itself purportedly numbers fewer than ten individuals, REvil is known for using RaaS (ransomware as a service), in which most of the attacks "are conducted by the affiliates or adverts who disseminate the payload and navigate the victim's networks"; these "affiliates" infect the targeted systems with the computer virus that encrypts the target's files and dispenses a ransom demand message.[39]

Two days after its initial announcement, JBS made a cheerier follow-up announcement:

> Our systems are coming back online, and we are not sparing any resources to fight this threat. We have cybersecurity plans in place to address these types of issues and are successfully executing those plans. Given the progress our IT professionals and plant teams have made in the last 24 hours, the vast majority of our beef, pork, poultry, and prepared foods plants will be operational tomorrow.[40]

The remarkably quick recovery struck a number of observers as less than realistic, given that many organizations have taken weeks or even months to become fully operational after a ransomware attack; some have even gone bankrupt. On June 9, 2021, JBS announced that it had made an $11,000,000

35. Felipe Zárate, *A Global Attack: JBS Case*, FLUID ATTACKS (June 7, 2021), https://perma.cc/9SNK-T293; Eric Swotinsky, *JBS Attack Shows the Immense Threat Posed by Ransomware*, ACRONIS (June 4, 2021), https://perma.cc/BE5X-CEV2.

36. Press Release, Media Statement: JBS USA Cybersecurity Attack, JBS USA LLC (May 31, 2021), https://perma.cc/6GEK-7KQK.

37. *Id.*

38. Press Release, FBI Statement on JBS Cyberattack, Fed. Bureau Investigation (June 2, 2021), https://perma.cc/3UAZ-EEZP.

39. Zárate, *supra* note 35.

40. Press Release, JBS USA and Pilgrim's Announce Progress in Resolving Cyberattack, JBS USA LLC (June 1, 2021), https://perma.cc/35K2-T4DA.

ransom payment to REvil.[41] According to the company, "this decision had to be made to prevent any potential risk to our customers."[42] Published reports indicated that the initial ransom demand from REvil was $22.5 million.[43]

What was the result, beyond the payment of money? According to at least one source, the cyberattack that paralyzed the world's largest meat production company reduced its revenue by twenty percent.[44] Meat prices, which had already risen five percent over the previous year due to the coronavirus pandemic, rose again. Due to the attack, U.S. plants slaughtered twenty-two percent fewer cattle than they had just the week before the attack.[45] And, of course, JBS became just the latest in a series of cautionary tales about cyberattacks on American companies that the U.S. government would discuss, this time in a March 2022 report to the U.S. Senate by the Senate Committee on Homeland Security and Governmental Affairs.[46] But as the following sections will discuss, the government can do more than talk. There are legal solutions to be explored, one old and one new.

IV. SOMETHING OLD—IS THE DEFENSE PRODUCTION ACT A SOLUTION TO CYBERSECURITY CONCERNS OF THE AGRIBUSINESS SECTOR?

Can a solution to a futuristic problem like the agribusiness sector's cyber breach issues be found in a law from the past? More specifically, can the Defense Production Act of 1950 ("DPA")[47]—a law whose original purpose was to stabilize prices, wages, and salaries during the Korean War[48]—provide a means for the adoption of cybersecurity measures in the agribusiness sector? The DPA confers upon the President the authority to ensure that domestic industry can meet national defense requirements. In the original incarnation of the Act, the President had the power to requisition materials and property, expand government and private defense production, ration consumer goods, and establish a voluntary reserve of private sector executives who the federal government could employ during emergencies.[49] The current version of the DPA permits the President to mandate the prioritization of government contracts over other customers for goods and

41. Jacob Bunge, *JBS Paid $11 Million to Resolve Ransomware Attack*, WALL ST. J. (June 9, 2021), https://perma.cc/Q8DG-NY7Q.

42. *Id.*

43. Lawrence Abrams, *JBS Paid $11 Million to REvil Ransomwar, $22.5 Million First Demanded*, BLEEPINGCOMPUTER (June 10, 2021), https://perma.cc/4HKS-RMWY.

44. Tanya Sabharwal, *Ransomware Cyberattack Case Study: JBS, World's Biggest Meat Supplier*, DIGIAWARE (July 23, 2021), https://perma.cc/6UE3-UCEW.

45. Pieter Arntz, *JBS Says It is Recovering Quickly from a Ransomware Attack*, MALWAREBYTES (June 2, 2021), https://perma.cc/D82D-QSM9.

46. *America's Data Held Hostage: Case Studies in Ransomware Attacks on American Companies*, U.S. SEN. COMM. ON HOMELAND SEC. & GOV. AFF. 23–24 (Mar. 2022), https://perma.cc/DC8U-8LDP.

47. 50 U.S.C.A. § 2061 (1950).

48. Michael H. Cecire & Heidi M. Peters, *The Defense Production Act of 1950: History, Authorities, and Considerations for Congress*, CONG. RSCH. SERV. 1, 4 (Mar. 2, 2020), https://perma.cc/Y4EB-TNR3.

49. Eric C. Surette, Annotation, *Construction and Application of the Defense Production Act of 1950, 50 U.S.C.A. § 2016 et seq. and Its Regulations*, 8 A.L.R. Fed. 3d art. 5, § 1 (2016).

services, as well as to offer incentives to produce critical materials and technologies for national defense purposes.[50] The Act also empowers the President to require anyone capable of meeting the government's needs to accept and perform contracts—even if that company is not already a government contractor.[51] The DPA has a "sunset" provision requiring Congress's periodic renewal. Pursuant to this provision, the Act has been renewed fifty-three times since its initial passage; it is currently set to expire on September 30, 2025.[52]

Before analyzing the DPA itself, the provisions applicable to agriculture and cybersecurity, and how the Act has been interpreted, two recent national crises in which the DPA was invoked illuminate its potential applicability to the agribusiness sector. First, during the COVID-19 pandemic, both President Donald Trump and President Joe Biden invoked the Act. President Trump used it to "prioritize the allocation of medical resources, prevent hording of personal protective equipment and require General Motors to build ventilators."[53] And more directly analogous to the agribusiness sector, President Trump also ordered beef, pork, and poultry processing facilities to stay open during lockdown so that the American population's supply of protein would remain uninterrupted.[54] As for President Biden, he invoked the DPA in March 2021 to speed up vaccine production through expediting the production of raw materials, equipment, supplies, and machinery. Outside of the pandemic, President Biden also used the Act to ramp up the supply of materials for the large-capacity batteries used in civilian electronic vehicles.[55]

The most recent use of the DPA is also instructive. On May 18, 2022, President Biden reacted to a nationwide shortage of baby formula by announcing the first of three DPA authorizations for infant formula.[56] First, the President directed suppliers of baby formula ingredients to prioritize delivery and distribution to formula manufacturers. Next, he authorized manufacturers to add legally binding language to their orders with suppliers to give them priority over other customers.[57] These orders enabled manufacturers like Abbot Nutrition to receive priority on raw materials for infant formula, like sugar and corn syrup. It also enabled manufacturers like Reckitt to obtain priority orders of single-use filters needed to generate oils that go into producing infant formula. President Biden also used the Act to authorize Operation Fly Formula flights, which used DOD aircraft to fly in the equivalent of 1.5 million 8-ounce bottles of infant

50. J. Michael Littlejohn, *Using All the King's Horses for Homeland Security: Implementing the Defense Production Act for Disaster Relief and Critical Infrastructure Protection*, 36 PUB. CONT. L.J. 1, 6 (2006).

51. *Id.*

52. Cecire & Peters, *supra* note 48, at Summary.

53. Erik Gordon, *What You Need to Know About the Defense Production Act—The 1950s Law Biden Invoked to Try to End the Baby Formula Shortage*, THE CONVERSATION (May 19, 2022), https://perma.cc/7R9E-DMP6.

54. *Id.*

55. *Id.*

56. *Id.*

57. *President Biden Announces First Two Infant Formula Defense Production Act Authorizations*, WHITE HOUSE (May 22, 2022), https://perma.cc/5QQ2-V3QQ.

formula to the United States, under the auspices of the Food and Drug Administration, from other countries while domestic production was still being accelerated.[58]

The infant formula shortage, of course, was caused in large part by manufacturing issues that closed production at key plants like Abbott's Sturgis plant. Invoking the DPA to address this issue shows both the power and the limitations of the Act. Yes, the action was a swift, decisive approach to a high-profile crisis. But while it can set priorities for ingredients and increase manufacturing capacity, such authorizations cannot make ingredients magically appear. The DPA's broadened definition of national defense has changed since its original Korean War application. Now, protecting national security also involves supporting "domestic preparedness, response, and recovery from hazards, terrorist attacks, and other national emergencies."[59]

Indeed, the very concept of "national security" has evolved over the course of American history, despite the fact that the term itself is rarely defined in the laws in which it appears. It is clear, however, that national security is no longer limited to armed conflict. The everyday conduct of life and industry depends on a secure cyberspace, and even warfare itself now encompasses the dimensions of the cyber realm.[60] The Cybersecurity Act of 2010 would have given the President authority to establish procedures for the protection of "any information system the infiltration, incapacitation, or disruption of which would have a debilitating impact on national security, including national economic security and natural public health or safety."[61] But because of concerns among observers that this somehow was directed toward the potential limiting or shutdown of the internet in the event of an emergency,[62] Congress eventually passed a bill that called for more private sector involvement, 2015's Cybersecurity Information Sharing Act.[63]

The first part of this Act authorizes companies to monitor and defend against cyberthreats on their own, while the second part provides protections for companies that voluntarily share information about cyberthreats with federal, state, and local governments, as well as with other private companies.[64] Essentially, this law codifies the collaborative "two way street" between public and private entities that protecting cyber systems demand. Among other provisions, the law provides for the Department of Homeland Security to work

58. Press Release, HHS Secretary Becerra Invokes Defense Production Act for Third Time to Further Increase Production of Infant Formula for American Families, DEP'T HEALTH & HUM. SERVS. (May 27, 2022), https://perma.cc/CNY5-THHG.

59. 50 U.S.C.A. § 2061. Indeed, just since 2019, the Department of Homeland Security has invoked the Act roughly 400 times, usually to help in response to natural disasters like hurricanes and floods.

60. Alexander Chanock, *Fixing the War Powers Resolution in the Age of Predator Drones and Cyber-Warfare*, 78 J. AIR L. & COM. 453, 468 (2013) (predicting that future wars will be fought "in the arena of cyberspace").

61. *Summary*, Cybersecurity Act of 2010, S. 773, 111th Cong. § 4 (2009–2010).

62. Major John S. Fredland, *Building a Better Cybersecurity Act: Empowering the Executive Branch Against Cybersecurity Emergencies*, 206 MILITARY L. REV. 1, 34–37 (2010).

63. 6 U.S.C. §§ 1501–1510 (2018); *see also* Brad S. Karp, *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, HARV. L. SCH. FORUM ON CORP. GOVERNANCE (Mar. 3, 2016).

64. 6 U.S.C. §§ 1501–10.

with both federal and non-federal entities to facilitate and promote sharing of cyberthreat indicators, defensive measures, and best practices.[65] This "two way street," however, is a voluntary one. It is fine when an entity in the agribusiness sector voluntarily reaches out to the federal government, as when Monsanto reached out to the FBI to monitor a Chinese national who had worked for the agricultural seed giant from 2008–2017 and was suspected of sharing online farming software with the Chinese government.[66] But what about farmers and others in the agricultural sector who do not seek government help? Or, to put it another way, in the absence of this sector setting its own cyber house in order, what legal authority does the government have to protect against cyberattacks that might disastrously impact U.S. agriculture and this country's food and water supply?

Enter the DPA. In addition to the natural disaster relief and pandemic-related implementation discussed earlier, the Act was used to help resolve California's energy crisis in 2001 by requiring natural gas suppliers to make sales to a nearly bankrupt California power company so that power was not cut off.[67] Its use then led Senator Phil Gramm to describe the DPA as "the most powerful and potentially dangerous American law."[68] The U.S. Supreme Court has even set the stage for sanctioning use of the Act for the taking of private property as far back as 1952, when it held that the DPA empowered the President "to take both personal and real property under certain conditions."[69] Given the recognition that agriculture is a part of America's CNI, and in light of the fact that the Act's scope has been expanded to encompass protecting and restoring critical infrastructure, it stands to reason that the DPA could be invoked in a cybersecurity emergency to protect the agribusiness sector. Moreover, as this article has already pointed out, the agribusiness sector's dependence on technology in this era of precision agriculture and its consequential vulnerability to cyberthreats like the JBS ransomware attack make the scenario of government intervention a realistic one.

Under just what sort of circumstances might the DPA be invoked? The Office of the Director of National Intelligence, the Department of Homeland Security, and a team of public and private sector representatives studied and assembled a number of different hypothetical "threat scenarios" that agribusiness entities might face, ranging from threats to the integrity of data as well as threats to the availability of data.[70] In some of the scenarios discussed, a national security threat is certainly implicated. For example, one hypothetical features a foreign government exploiting access to sensor data generated by agricultural drones, and then exploiting that data to create not only highly accurate assessments of

65. *Id.* § 1502(a)(1)–(5).

66. Christopher Burgess, *Guilty Plea for Monsanto Insider to Economic Espionage Charges*, CLEARANCE JOBS (Jan. 6, 2022), https://perma.cc/ZEV6-8SPV.

67. *The California Energy Crisis and Use of the Defense Production Act*, *Hearing Before the Senate Committee on Banking, Housing, and Urban Affairs*, S. Hrg. 107-215, 107th Cong. 1–2 (2001) (statement of Sen. Phil Gramm, Chairman).

68. *Id.*

69. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 585–86 (1952).

70. *Threats to Precision Agriculture*, *supra* note 17.

American agricultural yields but also to use that ill-gotten intelligence in trade negotiations.[71] Another involves a cyberthreat actor targeting large U.S. cattle operations by manipulating data to falsely imply a major animal disease outbreak[72]—an attack that could take weeks to verify that no such outbreak had occurred, while in the meantime large industry stock losses happen and both exports and public trust plummet.

Such scenarios may represent just the tip of the iceberg. Imagine a large U.S. agricultural concern that that refines corn, produces ethanol, and uses the ethanol byproducts to produce animal feed that feeds hundreds of thousands of meat-producing animals in feedlots throughout the country. The company is obviously part of our CNI, as not only a significant player in the agribusiness sector but an energy producer as well. Let us assume that like most companies, this entity has its own IT and cybersecurity staff. Now, take it a step further and assume that the FBI or some other government intelligence agency alerts the company's senior leadership to credible intelligence of a cyberthreat actor targeting a specific vulnerability in the company's systems with plans to attack in the imminent future. If the company responds with an overconfident "it's nothing we can't handle" type of reply, what are the federal government's options to prevent an attack with the potential to cut off a large supply of ethanol fuel and animal feed, thus disrupting American energy and food supplies?

Since the DPA's expanded definition of national defense includes "critical infrastructure protection and restoration," and since agriculture is a part of this critical infrastructure with an important role in national security, it seems clear that this company fits within the framework of what the DPA is intended to protect. Moreover, the Act's own wording also encompasses the cybersecurity aspects of the company, not just merely the ethanol or the animal feed. The DPA defines "materials" to include not just raw materials like, say, the ingredients of baby formula, but *also* the technical information "ancillary to the use of such materials."[73] The Act also defines "services" as efforts "needed for or incidental to (A) the development, production, processing, distribution, delivery, or use of an industrial resource or a critical technology item; (B) the construction of facilities; (C) the movement of individuals and property by all modes of civil transportation; or (D) other national defense programs and activities."[74] As for how "materials" has been interpreted by the courts, no cases to date have examined whether cyber systems might fall within the DPA's purview of materials or services. Nevertheless, one early case called for giving "materials" the "broadest kind of definition."[75] Meanwhile, a more recent federal court decision declared

71. *Id.* at 17.

72. *Id.* at 18.

73. *See* 50 U.S.C. § 4552(13) (defining "materials").

74. *Id.* § 4552(16)(A)–(D).

75. Safeway Stores v. Arnall, 196 F.2d 510, 513 (Emer. Ct. App. 1952), *judgment vacated on other grounds*, 344 U.S. 803 (1952).

that the DPA "addresses goods and the *services necessary to produce those goods*, not pure services."[76]

Since cybersecurity tools are incidental to production, as well as technical information "ancillary to the use of . . . materials" necessary for any entity in the agribusiness sector, it seems clear that they fall under the DPA's umbrella.[77] Cybersecurity is both a "material" and a "service" necessary for producing what the agribusiness sector does for national security. If maintaining the safety and integrity of the nation's food supply is critical to our national infrastructure, and if the DPA was intended to ensure a steady flow of materials for the national defense, *and* if cybersecurity is a service incidental to creating such materials, then the DPA authorizes the federal government to take necessary cybersecurity measures. If "something old" like this Act can ensure an uninterrupted supply of infant formula, it can certainly be invoked to protect our food supply from being hacked.

V. SOMETHING NEW—CAN THE FEDERAL GOVERNMENT MAKE THE AGRIBUSINESS SECTOR ADOPT CYBERSECURITY MEASURES?

If the "something old" approach to combating cybersecurity risk in the agribusiness sector is not taken, is there a "something new" alternative? Clearly, the threat exists; according to one 2021 report, the cost of ransomware damages alone ballooned to nearly $20,000,000,000 in 2020.[78] Yet, despite these numbers and the continuing variants of attacks (such as RaaS), the level of readiness is appalling. According to a survey of 582 information security professionals, fifty percent did not believe their organization was prepared for a ransomware attack.[79] With the dizzying variety and value of data in the agribusiness sector—agronomic data about crop selection and yields, land/soil data, weather data, machine data, production data, and livestock data—one would think that the industry would have adopted its own voluntary set of cybersecurity and data protection/privacy standards already.

It is not that the agribusiness sector did not have the chance. On October 22, 2015, the House Agriculture Committee held a hearing on data practices for companies in the agricultural field.[80] Unfortunately, although the Committee heard concerns regarding data practices and security, "most panelists agreed that little to no governmental intervention was desired."[81] The agribusiness sector, even before this hearing, considered the respective merits of private adoption of

76. Fisher v. Halliburton, 696 F. Supp. 2d 710, 718–19 (S.D. Tex. 2010), *order vacated and appeal dismissed*, 667 F.3d 602 (5th Cir. 2012) (emphasis added).

77. 50 U.S.C. § 4552(13)(B).

78. Jason Firch, *10 Cyber Security Trends You Can't Ignore in 2021*, PURPLESEC (Apr. 29, 2021), https://perma.cc/ND5W-NHU8.

79. *Id.*

80. Megan Stubbs, *Big Data in U.S. Agriculture*, CONG. RES. SERV. 3 (2016), https://perma.cc/EBD5-EJ5T.

81. *Id.*

industry standards for data security vs. public regulation. In 2014, the American Farm Bureau Federation developed its Privacy and Security Principles for Farm Data ("Principles"), with thirty-nine organizations from across the agriculture industry signing on by 2016.[82] But while the program has noble goals, it also has serious drawbacks. For one, it is purely voluntary, and there is no penalty if an entity fails to adhere to the Principles. The program also fails to address concerns over how data could be used in ways that might harm a producer. In addition, there is no consistency between the Principles' policies and terminology and the actual contracts that signatory entities might have with farmers; as a result, the Principles do not bind companies in any way that might provide real reassurance to farmers.

As a result of the agribusiness sector's failure to govern itself insofar as cybersecurity and data protection/privacy is concerned, what is left are voluntary standards that lack teeth. Currently, legal requirements for agricultural technology providers and others in this space are limited to the current patchwork quilt of federal and state data protection/data privacy law. Some states have enacted their own data protection and data privacy laws, such as California.[83] However, these state laws may not even be applicable to the specific types of data collected by companies in the agribusiness section, nor do they enact a regime of cybersecurity standards.

In the absence of any uniform state regulations covering agricultural data and with only voluntary industry standards, and with the current cyberthreats facing the agribusiness sector, is it time to enact a federal regulatory scheme? First of all, a previous legislative attempt to empower the USDA to create a secure data warehouse for agricultural data—the Agriculture Data Act of 2018—never made it out of Committee.[84] Second, precedent exists for federal, industry-specific regulations governing data practices. The Gramm-Leach-Bliley Act ("GLBA"), for example, governs institutions in the financial services industry.[85] Another example, the more widely known Health Insurance Portability and Accountability Act ("HIPAA"), governs healthcare entities.[86] With such precedent for the federal government to step in and impose a regulatory framework for the necessity of protecting data security and privacy, and with the need to protect a vital part of our nation's CNI like the agricultural sphere looming larger than ever, the table is set for federal intervention.

While the GLBA had a well-publicized goal of improving the perceived lack of competitive practices in the finance industry, it was also intended to improve

82. *Privacy and Security Principles for Farm Data*, AM. FARM BUREAU FED'N (Nov. 13, 2014), https://perma.cc/2N2B-JHRE.

83. California has a variety of data protection/data privacy laws, including its Electronic Communications Privacy Act, CAL. PENAL CODE §§1546.1–46.4 (2015); its Online Privacy Protection Act, CAL. BUS & PROF. CODE §§ 22575–79 (2003); the "Shine the Light" Law on consumer data privacy, CAL. CIV. CODE §§1738–3273.55 (1988); and the Data Security Law, CAL. CIV. CODE §§1798.100–1798.199.100 (2018).

84. Agriculture Data Act of 2018, S. 2487, 115th Cong. (2018).

85. 15 U.S.C. § 6801 (2012).

86. Health Insurance Portability and Accountability Act, Pub. L. No. 104-91, 110 Stat. 1936 (1996).

the privacy and security of consumer information.[87] This law was the first at the federal level to establish "a minimum federal standard of privacy for financial information."[88] Among the law's provisions, of particular interest is how the GLBA instructs federal agencies to develop standards for financial institutions to maintain in order to have adequate

> administrative, technical, and physical safeguards—(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[89]

The GLBA requires covered financial institutions to adhere to a number of data privacy and protection standards. In addition to requiring these institutions to "develop, implement, and maintain a comprehensive information security program",[90] such programs must contain safeguards that are appropriate to each institution, taking into consideration such factors as "size and complexity," "nature and scope of [the] activities," and "the sensitivity of any customer information at issue."[91] Some of the safeguards specifically mentioned are "regular test[ing] or otherwise monitor[ing of] the effectiveness of the safeguards' key controls, systems, and procedures," as well as the evaluation and updating of a security program following any changes to a company's structure or performance of the security program.[92]

HIPAA is another example of the federal government stepping in to regulate data practices in a particular industry. While the original legislation was intended to improve the ability of Americans to transfer health insurance more easily, reduce fraud, and improve how sensitive patient information is handled and secured, it also required institutions to set security standards for protecting such information and to provide penalties for breaches of these standards.[93] Under HIPAA, institutions must draft and follow their own set of privacy policies and procedures,[94] appoint a designated privacy official to oversee these policies,[95] and follow a set of technical standards to protect the transmission of patient health information being transferred over their networks from being intercepted.[96]

Like the regulatory schemes implemented in the financial services and healthcare industries, a federal legislative framework for protection of data and

87. Jolina C. Cuaresma, *The Gramm-Leach-Bliley Act*, 17 BERKELEY TECH. L.J. 497, 497 (2002).
88. *Id.* at 502.
89. 15 U.S.C. § 6801(b).
90. 16 C.F.R. § 314.3(a) (2016).
91. *Id.*
92. *Id.* § 314.4(a)–(d).
93. *See, e.g.*, Young B. Choi et al., *Challenges Associated with Privacy in Health Care Industry: Implementation of HIPAA and the Security Rules*, 30 J. MED. SYS. 57 (2006) (exploring this further).
94. 45 C.F.R. § 164.530 (2009).
95. *Id.* § 164.530(a)(1)(i).
96. *Id.* § 164.312(e).

adoption of cybersecurity standards in the agribusiness sector would be preferable to the feeble attempts to date at self-governance. A federal approach also would be superior to the piecemeal, state-by-state regulatory environment, since it would permit larger agribusiness entities operating nationally to develop one set of policies and practice in compliance with the proposed federal law, rather than being at the mercy and uncertainty of each individual state's differing requirements.[97] Such an industry-specific law would be more likely to be effective, especially if the rules were promulgated by an agency that deals with agricultural issues on a regular basis and which has expertise that would prove helpful in designing data protection and cybersecurity rules for the agribusiness sector.

VI. CONCLUSION

Of course, an industry-specific federal law is only one federal option. Another route might be through an Executive Order by the President, more narrowly tailored than President Biden's 2022 Executive Order on Improving the Nation's Cybersecurity (EO 14028),[98] which establishes a set of information sharing requirements across multiple industries. But executive orders tend to be drawn in broad strokes and lack the granular detail and the vetting that results from legislative debate.

Like most industries, technological innovation and the spread of "big data" has had a tremendous impact on the agribusiness sector. The higher yields and advances in food safety, crop sustainability, and harvest efficiency that are a hallmark of precision agriculture have addressed a panoply of world hunger concerns, but the technology that makes them possible presents its own risks. Cyberthreats, such as ransomware attacks, loom larger than ever on the national and international landscapes. Current data protection/data privacy and cybersecurity regulations in the United States are woefully ill-equipped to protect as vital a component of our CNI as the agribusiness sector. We need to look no further than the JBS ransomware incident to see how such an important segment of the economy can be—even temporarily—brought to its knees. We are witnesses to the fallout of food shortages, declining stock values, higher prices, and erosion of public confidence.

There are, however, solutions on deck both old and new. A time-tested option, invoking the DPA, has already been used to mobilize vaccine production during the COVID-19 pandemic and to address last year's infant formula shortage. A "new" solution, drafting and implementing a federal law on data protection and cybersecurity specific to the agribusiness sector, has legislative predecessors like the GLBA for the financial services industry and HIPAA governing the healthcare

97. CAL. CODE REGS. tit. 3, §§ 1320–26 (2023). In addition to the patchwork quilt of state data privacy laws, entities in the agribusiness realm may also find federal regulation preferable to the potential for contradictory obligations imposed by state animal welfare laws, along the lines of California's referenda like the "cage free" Proposition 12.

98. Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021).

field. Neither federal law is perfect or without its share of vocal critics, but in the absence of any law, the agribusiness sector's current data security and cybersecurity posture might best be characterized as the Wild West.

Which solution is better—the "old" or the "new"? Invoking the DPA may be speedier and offer greater certainty than embarking upon the road of legislative horse trading, but it should be thought of as a legal tourniquet rather than a longer-term surgical solution. Developing an industry-specific cybersecurity and data protection law, analogous to what has been achieved with the GLBA and HIPAA, promises to be the most viable and lasting route to providing the protection and guidance that the agribusiness sector needs and deserves.