Journal of Technology Law & Policy

Volume 24 Number 1

ARTICLES

NOTES

REGULATING THE IMPENDING TRANSFORMATION OF THE MEAT INDUSTRY: "CULTURED MEAT"

Jaden Atkins[*]

---

* J.D. Candidate, Class of 2020, University of Arkansas School of Law. The author sincerely thanks the Journal of Technology Law and Policy for their careful editing, Professors Susan Schneider and Ann Killenbeck for their invaluable guidance throughout the writing and publishing process, and her husband and family for their unwavering support.

INTRODUCTION

The year is 2022. You and your friend are hungry, so you go down the street to your friend's favorite new burger joint for lunch. You sit down and tell the waiter that you want a burger with cheese, medium rare. Fifteen minutes later, your food comes out. You take a bite. It tastes just like the burgers your dad used to grill—right down to the ridiculous amount of grease and the red, slightly undercooked center. About halfway through your burger, your friend mentions, "Yeah, I like this place because they serve those new burgers grown in labs. It's good for the environment!" You stop chewing and consider spitting it out, but you decide against it, reluctantly swallowing. Grown in a lab, what does that mean? Is this a joke?

Strange as it may sound, this new meat grown in a lab could soon be a reality.[1] It goes by many names, including: "clean meat," "lab-grown meat," "artificial" or "synthetic meat," "in-vitro meat," "cell-based meat," and even "Franken-meat."[2] The American government seems to prefer "cell-cultured" or "cultured meat," so I will use that terminology in this Article.[3] If the "ick factor" demonstrated in the hypothetical above can be overcome, the benefits of cell-cultured meat could be pretty incredible.[4] However, with those potential benefits come potential risks,

---

1. *See* discussion *infra* Section I.B para. 1.

2. *See, e.g.*, U.S. FOOD & DRUG ADMIN., *Foods Produced Using Animal Cell Culture Technology*, Docket No. FDA-2018-N-2155, at 92, 151 (July 12, 2018), https://www.fda.gov/media/115122/download [hereinafter *FDA Transcript*] (comparing the popularity of these names for cell-cultured meat); Alan Boyle, *It's (Not) Alive! Franken-Meat Lurches from the Lab to the Frying Pan*, NBC NEWS (Aug. 4, 2013, 5:55 PM), https://www.nbcnews.com/technolog/its-not-alive-franken-meat-lurches-lab-frying-pan-6C1083 5458.

3. JOEL L. GREENE & SAHAR ANGADJIVAND, CONG. RESEARCH SERV., IF10947, REGULATION OF CELL-CULTURED MEAT 1 (2018) [hereinafter CRS ON CULTURED MEAT]; s*ee infra* Section IV.B for a discussion on why to prefer "cultured" as a legal matter, as well; s*ee, e.g.*, *FDA Transcript*, *supra* note 2, at 91–92. *See infra* Section IV.B for a discussion on why to prefer "cultured" as a legal matter, as well.

4. *See* Charlotte Hawks, *How Close are We to a Hamburger Grown in a Lab?*, CNN (Mar. 8, 2018, 2:23 PM), https://www.cnn.com/2018/03/01/health/clean-in-vitro-meat-food/index.html (coining the term "ick factor" to describe the obstacle of people's general disgust with the idea of cultured meat); discussion *infra* Section I.B.2.

including unknown health problems, both from foodborne illness and long-term health risks.[5] Due to these potential benefits and risks, it is necessary to determine: (1) how this new technology will be regulated, and (2) who will regulate it.

Although the United States Department of Agriculture (USDA)'s Food Safety and Inspection Service (FSIS) typically regulates "meat," the Federal Drug Administration (FDA) claims that it is better prepared to regulate this new technology given its experience regulating similar biotechnologies.[6] Thus, both the USDA and FDA currently claim to have jurisdiction over cell-cultured meat.[7]

So, why does it matter which agency regulates cell-cultured meat? It matters because each agency has different principles that govern how it regulates food safety.[8] Generally, the USDA regulates the specific procedures used to prepare the food to ensure its safety; the FDA, however, is mainly concerned with the safety of the final product and only considers the processes used to identify potential safety risks when evaluating the final product.[9] Accordingly, meat lobbyists, such as the United States Cattlemen's Association (USCA), generally support the USDA's sole jurisdiction over cell-cultured meat and clear labeling practices, which distinguish cultured meat from "real meat."[10] On the other hand, environmentalists, animal rights activists, and other supporters of cell-cultured meat generally support placing it under the FDA's sole jurisdiction, which would afford more lax labeling requirements.[11]

This issue should not be decided based on a particular interest group's desires, but rather upon a weighing of the potential benefits of a quick deployment of the new technology against the potential risks to human health at each stage of production. Thus, I argue that, because the FDA is better prepared to regulate new technologies, and has some experience in the regulation of meat, it should hold sole jurisdiction of regulation up to the point that cell-cultured meat becomes "meat," in the traditional sense, at harvest. However, because the USDA is better prepared to regulate traditional meat and its vulnerability to foodborne illness, the USDA should regulate cell-cultured meat as it would other forms of meat from that point on. However, the FDA should have sole jurisdiction over cell-

5. *See* discussion *infra* Section I.B.2.
6. *See* discussion *infra* Section I.C.
7. *See* discussion *infra* Section I.C.
8. *See* discussion *infra* Section I.A.1.
9. *See* discussion *infra* Section I.A.1.
10. *See* discussion *infra* Section I.B.3.
11. *See* discussion *infra* Section I.B.3.

cultured meats that already fall under its purview, including wild game and non-catfish seafood.

In Part I of this Article, I lay a background for the current regulatory framework of safety and labeling applied by the USDA and FDA, the current understandings and hopes concerning cultured meat, and the current debate regarding the future regulation of cultured meat. In Part II, I argue that both the USDA and FDA have statutory authority to claim jurisdiction over cultured meat. In Part III, I argue that the framework proposed by the two agencies properly grants the FDA jurisdiction over pre-harvest safety of cell-cultured meats and grants the USDA jurisdiction over post-harvest safety of meats that would normally fall under its jurisdiction. However, in Part IV, I argue that the agencies should also split jurisdiction of labeling in a way that allows the FDA to determine whether cell-cultured meat fits within a newly defined statement of identity and allows the USDA to regulate its labeling. Finally, I conclude that, although the USDA and FDA's proposed framework for sharing jurisdiction is the best possible framework to ensure food safety and is properly based in the law, it improperly gives sole power over labeling cell-cultured meat to the USDA.

I. BACKGROUND

A. *The Current Framework of Food Regulation*

There are currently two agencies that regulate food safety for human consumption, the USDA and FDA. Generally, the USDA regulates most red meats, poultry, and the processing and grading of eggs, while the FDA regulates non-meat food, dietary supplements, seafood, wild game, and eggs in the shell.[12]

1. Sources of Agency Jurisdiction

The FDA and USDA derive their jurisdiction over particular foods from multiple statutes. The USDA's FSIS implements and enforces the Federal Meat Inspection Act (FMIA), Poultry Products Inspection Act (PPIA), and Egg Products Inspection Act (EPIA), which collectively grant the USDA general jurisdiction over red meat, poultry, and eggs.[13] The USDA bases its operations on the principles of "Hazard Analysis and Critical Control Points" (HACCPs).[14] HACCPs analyze the process of

12. NEAL D. FORTIN, FOOD REGULATION: LAW, SCIENCE, POLICY, AND PRACTICE 14 (2d ed. 2017).

13. 21 U.S.C. §§ 451–72, 601–95, 1031–56 (2018); CRS ON CULTURED MEAT, *supra* note 3.

14. *Id.*

producing various foods and develop methods intended to mitigate the risks to food safety that such products produce.[15]

The FDA, in contrast, implements and enforces the Federal Food, Drug, and Cosmetic Act (FFDCA), Public Health Service Act (PHSA), and Fair Packaging and Labeling Act (FPLA).[16] Together these laws grant the FDA jurisdiction over many different aspects of food production, including the regulation of "food."[17] The FDA evaluates foods based on various principles, including the "Generally Regarded as Safe" (GRAS) Principle, but generally focuses on the safety of the final product rather than the method used to produce it to determine safety.[18] However, the FDA and USDA do share jurisdiction over certain foods, such as catfish.[19] When this occurs, the two agencies create a "Memorandum of Understanding" (MOU) to facilitate regulation.[20]

2. Jurisdiction of "Meat" Regulation

The USDA is generally responsible for the regulation of meat, but this is not always true.[21] For instance, the USDA exclusively regulates "the slaughter and processing of meat animals."[22] However, because the FDA has jurisdiction over "food additives," the agencies share jurisdiction over the food additives contained in meat.[23] The FDA also has jurisdiction over multi-ingredient products containing "3% or less raw meat."[24] Additionally, the FDA exclusively regulates wild game and all seafood, except catfish.[25]

3. Regulation of Statements of Identity in Labeling

Both the USDA and FDA enforce prohibitions on "misbranded" foods.[26] A food is "misbranded" if one of several conditions is met, including, "[i]f it purports to be–or is represented as a food for which a

15. *Id.*

16. 21 U.S.C. §§ 301–99h (2018); 42 U.S.C. §§ 201–300mm-61 (2018).

17. 21 U.S.C. § 393 (b)(2)(A) (2018); FORTIN, *supra* note 12, at 17.

18. FORTIN, *supra* note 12, at 220–24, 313 (discussing the GRAS principle and its application).

19. CRS ON CULTURED MEAT, *supra* note 3.

20. *Id.*

21. FORTIN, *supra* note 12, at 23.

22. *Id.*

23. *Id.*

24. *Id.*

25. CRS ON CULTURED MEAT, *supra* note 3.

26. *See* 21 U.S.C. § 331 (2018) (FDA regulation of misbranded foods); 21 U.S.C. § 458 (2018) (USDA regulation of misbranded poultry); 21 U.S.C. § 610 (2018) (USDA regulation of misbranded meats); 21 U.S.C. § 1037 (2018) (USDA regulation of misbranded eggs).

definition and standard of identity has been prescribed."[27] Foods are required to show in prominent lettering on their labels a "statement of identity" which correctly represents what they are.[28] Such identifying language has been the focus of various court cases in which parties argued that almond, coconut, and soy "milk" are misbranded because they purport to be "milk," which has its own standard of identity, with little success.[29]

4. FDA Regulation of Emerging Biotechnologies

The FDA is largely responsible for the regulation of emerging food technologies, including genetically modified organisms (GMOs), genetically engineered animals, and cloning.[30] The FDA also has some experience in the use of other cell-cultured technologies, including: cell-cultures utilized in medical applications (such as insulin), algae cultured to produce oils, bacteria cultures found in yogurt, cultured yeasts used as additives in bread products, and common protein additives such as mycoproteins.[31]

B. *Cultured Meat*

Cell-cultured meat, or cultured meat, is an emerging technology that may challenge the current regulatory framework. Although the first burger made with cultured meat was sold at the outrageous price of $300,000 in 2013, the technology has been rapidly developing to produce cultured meat more efficiently so that it is readily available, with the price now set around $600 per buyer.[32] Some estimates show that cultured meat will be available by 2021 in niche markets and available on an industrial scale by 2024 for as low as $1 for a typical hamburger patty.[33] In the wake of major companies such as Tyson announcing major investments, "2019 is shaping up to be the year that startups and big businesses invest more

---

27. 21 U.S.C. § 343 (g) (2018).

28. § 343 (f)–(g).

29. *See, e.g.*, Ang v. Whitewave Foods Co., No. 13-CV-1953, 2013 WL 6492353, at *4 (N.D. Cal. Dec. 10, 2013) (unreported) (dismissing with prejudice the class action against soy milk, almond milk, and coconut milk producers because the products "clearly convey the basic nature and content of the beverages, while clearly distinguishing them from milk that is derived from dairy cows," and it is "simply implausible that a reasonable consumer would mistake" such a product for cow's milk).

30. FORTIN, *supra* note 12, at 285–86, 291, 315.

31. *FDA Transcript*, *supra* note 2, at 16, 44, 46, 47.

32. *See* G. Owen Schaefer, *Lab-Grown Meat*, SCIENTIFIC AMERICAN (Sept. 14, 2018), https://www.scientificamerican.com/article/lab-grown-meat/.

33. CBS NEWS, *Lab-Grown Meat Could be in Restaurants by 2021* (July 17, 2018, 10:14 PM), https://www.cbsnews.com/news/mosa-meat-lab-grown-meat-could-be-restaurants-by-2021.

in the alternative protein space."[34] With this in mind, regulations must be established quickly to ensure that this promising technology is safely, but quickly implemented.

1. Production of Cell-Cultured Meat

Cell-cultured meat is created by, first, taking a muscle sample from an animal.[35] From that sample, stem cells are taken and placed in a bio-reactor, where they are fed a nutrient medium and allowed to multiply exponentially.[36] This nutrient medium may include water, amino acids, vitamins, sugars, lipids, minerals, protein factors, and hormones, which enable the cells to grow naturally as they would in a living animal.[37] From one original cow's muscle sample, an estimated 80,000 quarter-pound burgers could be created.[38] Meanwhile, the cells' environment is controlled within a unique bioreactor so that the feed supply, temperature, pH, and oxygen levels can be controlled to efficiently form tissue.[39] After the cells have multiplied and formed tissue, the cell medium is drained, and the tissue is harvested, rinsed, and analyzed for quality to ensure that there are no impurities.[40]

2. Potential Impacts of Cultured Meat Development

Cultured meat has been heralded by various groups as a solution to many current problems. Perhaps most notably, environmentalists view cultured meat as a possible solution to the significant environmental impacts associated with meat production.[41] It is well-established that meat production, and especially beef production, has severely harmful effects on our environment due to its exorbitant energy, land, and water usage, as well as CO2 greenhouse gas (GHG) emissions (which

34. Nathan Owens, *Tyson Plans Own Plant-Based Foods*, ARK. DEMOCRAT GAZETTE (Feb. 9, 2019, 4:30 AM), https://www.arkansasonline.com/news/2019/feb/09/tyson-plans-own-plant-based-foods-20190/ (reporting on Tyson's announcement earlier that week that Tyson will be launching their own alternative protein source that could be on shelves by the end of 2019, although Tyson has not yet indicated whether this protein source will be cell-cultured or a plant-based protein product).

35. Schaefer, *supra* note 32.

36. *See FDA Transcript*, *supra* note 2, at 96–97.

37. *Id.* at 96.

38. Schaefer, *supra* note 32.

39. *FDA Transcript*, *supra* note 2, at 97.

40. *Id.*

41. *See, e.g.*, Bahar Gholipour, *Lab-Grown Meat May Save a Lot More than Farm Animals' Lives*, NBC NEWS (Apr. 6, 2017, 1:34 PM), https://www.nbcnews.com/mach/innovation/lab-grown-meat-may-save-lot-more-farm-animals-lives-n743091.

contribute to climate change).[42] In one speculative, independent study, scientists found that cultured meat "involves approximately 7-45% lower energy use . . . , 78-96% lower GHG emissions, 99% lower land use, and 82-96% lower water use depending on the product compared."[43] Although this study produced impressive results, it is widely criticized due to its high degree of speculation.[44] While more studies are likely necessary to confirm the study's results based on new information about what methods producers actually use as the technology develops, if even remotely true, these projections are impressive.

Animal rights activists additionally hope that cultured meat can function as a solution to animal abuse issues commonly found in factory farms.[45] Although, in its current state, the production of cultured meat requires the slaughtering of animals for the gathering of base cells, cultured meat offers a far more efficient process, drastically reducing the number of animals slaughtered for meat by unknown numbers.[46] Some animal rights activists hold out hope that initial tissue samples will eventually be taken from live animals via biopsy, eliminating the need to slaughter animals altogether.[47]

---

42. *See, e.g.*, FAO, TACKLING CLIMATE CHANGE THROUGH LIVESTOCK: A GLOBAL ASSESSMENT OF EMISSIONS AND MITIGATION OPPORTUNITIES (2013), http://www.fao.org/3/a-i3437e.pdf (tracking emissions from worldwide production of various kinds of livestock); Bryan Walsh, *The Triple Whopper Environmental Impact of Global Meat Production*, TIME (Dec. 16, 2013), http://science.time.com/2013/12/16/the-triple-whopper-environmental-impact-of-global-meat-production/ (examining the impact of livestock production on land, water, and emissions); CENTER FOR SUSTAINABLE SYSTEMS, PUB. NO. CSS09-05, CARBON FOOTPRINT FACTSHEET 1 (Aug. 2018), http://css.umich.edu/sites/default/files/Carbon_Footprint_Factsheet_CSS09-05_e2018_0.pdf (comparing the impact of livestock production on emissions against other sources of food and other industries).

43. Hanna L. Tuomisto & M. Joost Teixeira de Mattos, *Environmental Impacts of Cultured Meat Production*, ENVTL. SCI. TECH., 6117, 6117 (2011), https://pubs.acs.org/doi/pdf/10.1021/es200130u.

44. *See, e.g.*, Isha Datar, *Environmental Impacts of Cultured Meat*, NEW HARVEST (July 22, 2014), https://www.new-harvest.org/environmental_impacts_of_cultured_meat (noting criticisms of the study as being based on unproven assumptions about how cultured meat could be grown).

45. *See, e.g.*, Jacy Reese, *Is "Clean Meat" the Solution to Industrial Animal Farming?*, GEO. J. INT'L AFF. (June 25, 2018), https://www.georgetownjournalofinternationalaffairs.org/online-edition/2018/6/24/is-clean-meat-the-solution-to-industrial-animal-farming; *see also* PETA, *PETA's 'In Vitro' Chicken Contest*, https://www.peta.org/features/vitro-meat-contest/ (last updated Mar. 4, 2014) (detailing two contests for the first companies to create cell-cultured beef and chicken, respectively, without slaughtering any animals).

46. *See* Schaefer, *supra* note 32 and accompanying text.

47. *See, e.g.*, *Cultured Meat; Manufacturing of Meat Products Through "Tissue-Engineering" Technology*, FUTURE FOOD, https://www.futurefood.org/in-vitro-meat/index_en.php (last visited Mar. 1, 2019); *see also FDA Transcript*, *supra* note 2, at 167.

Cultured meat has potential positive and negative implications for human health, as well. For instance, cultured meat could be enhanced with beneficial additives, such as vitamin B12.[48] Further, harmful saturated fats could be replaced with healthier omega-3 fatty acids, which have shown promise in treating and preventing various diseases, but the main source of which is disappearing.[49] Cultured meat will most likely be free of the pharmaceutical residues found in some "traditional meat," such as pesticides and growth hormones, but there is some uncertainty as to whether the final product will contain antibiotic residues specifically.[50] Because it is grown in a sterile lab environment, cultured meat may have less of the harmful bacteria responsible for foodborne illness, resulting in considerable health and economic benefits.[51] However, some have cast doubt on the extent to which foodborne illness would actually be reduced, as there is still potential for contamination after harvest.[52] Further, some experts have expressed concerns that the process for creating the cultured meat will create new hazards, some of which may not be discovered until long-term effects have taken hold of consumers.[53]

In addition to the above significant, potential environmental, moral, and health impacts, advancement in cultured meat technology has some less obvious potential consequences. For instance, cultured meat could drastically reduce the cost of kosher meat in the future.[54] As the technology advances, cultured meat could replicate the meats and parts of more exotic animals and flood the markets, expanding our diets and

48. Marta Zaraska, *Is Lab-Grown Meat Good for Us?*, THE ATLANTIC (Aug. 19, 2013), https://www.theatlantic.com/health/archive/2013/08/is-lab-grown-meat-good-for-us/278778/.

49. *Id.*; *see also* Karen Wright & Susan Kruglinski, *I'll Have My Burger Petri-Dish Bred, with Extra Omega-3*, DISCOVER (Sept. 22, 2008), http://discovermagazine.com/2008/oct/22-ill-have-my-burger-petri-dish-bred.

50. Zaraska, *supra* note 48. It should be noted here that the meat industry generally denies that residues from antibiotics and other drugs are in meat; however, a recent study from Consumer Reports found traces of ketamine, phenylbutazone, chloramphenicol (an antibiotic), and other banned or severely restricted drugs in the U.S. meat supply. *See* Rachel Rabkin Peachman, *Are Banned Drugs in Your Meat?*, CONSUMER REPORTS, https://www.consumerreports.org/food-safety/are-banned-drugs-in-your-meat/ (last updated Nov. 27, 2018).

51. *See* Andy Weisbecker, *Food Illness Costs Substantial, Significant*, FOOD SAFETY NEWS (Dec. 8, 2009), https://www.foodsafetynews.com/2009/12/food-illness-costs-substantial-significant/.

52. *See, e.g.*, Zaraska, *supra* note 48.

53. *See, e.g.*, Markham Heid, *You Asked: Should I Be Nervous About Lab-Grown Meat?*, TIME (Sept. 14, 2016), http://time.com/4490128/artificial-meat-protein/.

54. Elaine Watson, *Orthodox Union: Cell Cultured Meat Could Dramatically Lower the Cost of Kosher Meat in the Future*, FOODNAVIGATOR-USA (Aug. 22, 2018), https://www.foodnavigator-usa.com/Article/2018/08/22/Orthodox-Union-Cell-cultured-meat-could-dramatically-lower-the-cost-of-kosher-meat-in-future.

eliminating the incentive of poaching.[55] Eventually, cultured meat may be even more cost efficient than conventional meat, and would therefore constitute one low-cost way to help abate world hunger.[56] The extent of impacts with this technology is unknown, but promising.

3. Competing Interests in Regulation

Although there are many groups that support cultured meat's quick movement to markets, there are also groups that oppose it. The groups interested in quickly moving the technology to market include environmentalists, animal rights activists, and health scientists.[57] These groups typically favor FDA regulation of cultured meat, which would focus more on the safety of the final product rather than its methods.[58]

However, ranchers and the farmers who produce their feed stand to lose a great deal if cultured meat becomes popular. Thus, ranching and farming interest groups argue for stricter regulations that would, as they see it, allow for fair competition.[59] Further, some groups, such as naturalists, are wary of long-term health detriments stemming from cultured meat's "unnaturalness."[60] These groups generally favor USDA regulation of the processes used in the creation of cultured meat as well as clear product labeling, allowing consumers to make an informed choice on potential unknown detriments of cultured meat consumption.[61]

In light of these competing interests, the questions of who will regulate cell-cultured meat and how they will regulate it have quickly become a hot topic.[62]

---

55. JAMIE HOLLYWOOD & MADSEN PIRIE, ADAM SMITH INST., DON'T HAVE A COW, MAN: THE PROSPECTS FOR LAB GROWN MEAT 9 (Aug. 30, 2018), https://static1.squarespace.com/static/56eddde762cd9413e151ac92/t/5b865367575d1f9926d24550/1535529836180/Lab+Grown+Meat+.pdf.

56. *See* CBS NEWS, *supra* note 33.

57. *See supra* Section I.B.2.

58. *See, e.g.*, *FDA Transcript*, *supra* note 2, at 93 (demonstrating that Memphis Meats believes that the current FDA framework should be applied to cultured meats).

59. *See, e.g.*, Leanna Garfield, *There's a Growing Battle Between Fake Meat Startups and Big Beef, and Neither Side is Backing Down*, BUS. INSIDER (June 10, 2018, 10:06 AM), https://www.businessinsider.com/beef-companies-file-petition-against-lab-grown-meat-startups-2018-2; *FDA Transcript*, *supra* note 2, at 200–01.

60. *See* Christopher Bryant & Julie Barnett, *Consumer Acceptance of Cultured Meat: A Systematic Review*, 143 MEAT SCI. 8, 12 (2018) (observing that cell-cultured meat's perceived "unnaturalness" causes some to claim that it is "dangerous to consume," "inherently unethical," or harmful to the environment).

61. *See, e.g.*, Garfield, *supra* note 59 (describing approaches of the traditional meat producer's interest groups in this issue).

62. *See, e.g.*, Helena Bottemiller Evich, *Welcome to the Turf Battle over Lab-Grown Meat*, POLITICO (June 15, 2018, 6:12 PM), https://www.politico.com/story/2018/06/15/lab-grown-meat-feds-turf-battle-629774.

C. *Shifting Thoughts on the Regulation of Cultured Meat*

Until very recently, legal academics generally believed that the FDA would hold sole jurisdiction over cell-cultured meat because the FDA's current regulatory framework was considered best suited to the task.[63]

This assumption was thrown into chaos in April 2018, when "USDA Secretary Perdue, in response to questions on cell-cultured meat, stated that meat and poultry are under the sole purview of the USDA, and any product labeled as meat would be under USDA purview."[64] However, in June 2018 "FDA Commissioner Gottlieb issued a statement on cell-cultured meat announcing that under the FFDCA, the FDA has oversight for cell-cultured meat" additionally announcing that the FDA would hold a public meeting on the regulation of cell-cultured meat.[65] In response, a USDA spokesperson affirmed the USDA's position that the USDA had sole jurisdiction over cell-cultured meat, but stated that the USDA was open to working with the FDA.[66]

In the absence of central authority, this "turf standoff" created significant confusion and attracted the attention of the House Appropriations Committee, which took the position that the USDA has sole jurisdiction over cell-cultured meat.[67] Despite the involvement of the House Appropriations Committee, the FDA moved forward and held its first public meeting in July 2018; the meeting detailed how cell-cultured technology might fit into its existing regulatory framework by comparing it to technology that the FDA already regulates.[68]

However, in September 2018, the USDA and FDA announced that they would hold a joint public meeting in October "to discuss the potential hazards, oversight considerations, and labeling of cell-cultured food products derived from livestock and poultry tissue."[69] This meeting arose in response to the USCA's publication of a petition requesting: (1) that USDA's FSIS be granted sole jurisdiction over cell-cultured meat, and (2) that companies be prevented from labeling cell-cultured meat as "meat" or "beef."[70] Although neither the USDA nor the FDA ceded

---

63. *See, e.g.*, Zachary Schneider, *In Vitro Meat: Space Travel, Cannibalism, and Federal Regulation*, 50 HOUS. L. REV. 991, 1014–15 (2013).

64. CRS ON CULTURED MEAT, *supra* note 3, at 2.

65. *Id.*

66. *Id.*

67. Evich, *supra* note 62; CRS ON CULTURED MEAT, *supra* note 3, at 2.

68. *FDA Transcript*, *supra* note 2, at 32–52.

69. Joint Public Meeting on the Use of Cell Culture Technology to Develop Products Derived from Livestock and Poultry, 83 Fed. Reg. 46,476, 46,476 (Sept. 13, 2018), https://www.govinfo.gov/content/pkg/FR-2018-09-13/pdf/2018-19907.pdf.

70. *Id.* at 46,477. This petition attracted a great deal of attention, receiving over 6,100 comments to the USDA.

jurisdiction of any particular aspect of regulation during the meeting, the agencies agreed that they both should have a role in the regulation of cell-cultured meat.[71]

Amid speculation of possible legislation, the USDA and the FDA released a joint statement in November 2018 further clarifying their individual roles (2018 joint statement).[72] According to the statement, the FDA will "oversee[] cell collection, cell banks, and cell growth and differentiation," while the USDA will "oversee the production and labeling of food products derived from the cells of livestock and poultry."[73] Under this framework, "[a] transition from FDA to USDA oversight will occur during the cell harvest stage."[74] The agencies made clear with this statement that they did not want Congress to intervene via its Farm Bill or any other legislation: "[b]ecause our agencies have the statutory authority necessary to appropriately regulate cell-cultured food products derived from livestock and poultry the Administration does not believe that legislation on this topic is necessary."[75] Despite this clear message, speculation remains that Congress may intervene and give USDA sole jurisdiction.[76]

Finally, on March 7, 2019, the FDA and USDA released a joint statement announcing their MOU on their joint regulation of cultured meat.[77] This MOU further details how the joint regulation will occur.[78]

---

71. *See, e.g.*, U.S. DEP'T OF AGRIC. & U.S. FOOD & DRUG ADMIN, DOCKET NO. FSIS-2018-0036, USDA AND FDA JOINT PUBLIC MEETING ON THE USE OF CELL CULTURE TECHNOLOGY TO DEVELOP PRODUCTS DERIVED FROM LIVESTOCK AND POULTRY, DAY 2 MORNING SESSION, 7 (Oct. 23–24, 2018) [hereinafter *Joint Transcript*], https://www.fsis.usda.gov/wps/wcm/connect/42c8b917-8c01-459d-8aa3-51e0b67ae84a/transcript-cellular-agriculture-day1-morning-102318.pdf?MOD=AJPERES.

72. U.S. DEP'T OF AGRIC., RELEASE NO. 0248.18, STATEMENT FROM USDA SECRETARY PERDUE AND FDA COMMISSIONER GOTTLIEB ON THE REGULATION OF CELL-CULTURED FOOD PRODUCTS FROM CELL LINES OF LIVESTOCK AND POULTRY (2018), https://www.usda.gov/media/press-releases/2018/11/16/statement-usda-secretary-perdue-and-fda-commissioner-gottlieb [hereinafter USDA AND FDA FIRST STATEMENT ON REGULATION].

73. *Id.*

74. *Id.*

75. *Id.*

76. *See, e.g.*, Liz Crampton, *Cell-Based Meat Issue Could Still be Settled on the Hill*, POLITICO (Nov. 20, 2018, 10:00 AM), https://www.politico.com/newsletters/morning-agriculture/2018/11/20/cell-based-meat-issue-could-still-be-settled-on-the-hill-422882.

77. U.S. DEP'T OF AGRIC., RELEASE NO. 0027.19, USDA AND FDA ANNOUNCE A FORMAL AGREEMENT TO REGULATE CELL-CULTURED FOOD PRODUCTS FROM CELL LINES OF LIVESTOCK AND POULTRY (2019), https://www.usda.gov/media/press-releases/2019/03/07/usda-and-fda-announce-formal-agreement-regulate-cell-cultured-food.

78. *See* U.S. DEP'T OF AGRIC. & U.S. FOOD &. DRUG ADMIN., FORMAL AGREEMENT BETWEEN THE U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES FOOD AND DRUG

Under the MOU, the FDA will "conduct premarket consultation processes," including "oversight of collection, cell lines and banks, and all components and inputs" and, "[a]t harvest, . . . provid[e] information necessary for USDA to determine whether harvested cells are eligible to be processed into meat or poultry products that bear the USDA mark of inspection."[79] The USDA will then "[c]onduct inspection in establishments where cells cultured from livestock and poultry subject to the FMIA and PPIA are harvested, processed, packaged or labeled" and "[r]equire that the labeling of human food products derived from the cultured cells of livestock and poultry be preapproved and then verified through inspection."[80]

II. STATUTORY AUTHORITY FOR REGULATION

Prior to evaluating this proposed framework of joint jurisdiction, we must first ask, is it legal? That is, do both the FDA and USDA have power under current laws to regulate what they propose to regulate? The statutory basis for both the USDA and FDA's authority to regulate cell-cultured meat is debatable, and the lack of clarity of what cell-cultured meat will look like does not help this issue; ultimately, however, both agencies will likely have the authority to regulate cell-cultured meat in at least some fashion.

As an initial matter, the FDA's sole power to regulate specific forms of traditional meat should extend to any cultured meat forms of those meats. Although no such division was explicitly made in the 2018 joint statement, the title of the statement indicates that it is meant to apply only to "Food Products from Cell Lines of Livestock and Poultry."[81] The FDA's sole power to regulate any cultured meat that falls into one of these categories should be clear as the USDA has no basis for regulating these categories under the current statutory and administrative framework. Thus, the FDA will have the sole power to regulate cell-cultured meat derived from wild game and all seafood except catfish, and any multi-ingredient products containing "3% or less raw [cultured] meat."[82] The remainder of this section thus focuses on each agency's authority to regulate cell-cultured meat that does not fall under one of these categories.

ADMINISTRATION AND U.S. DEPARTMENT OF AGRICULTURE OFFICE OF FOOD SAFETY 2–4 (2019) [hereinafter USDA AND FDA CULTURED MEAT MOU], https://www.fsis.usda.gov/wps/wcm/connect/0d2d644a-9a65-43c6-944f-ea598aacdec1/Formal-Agreement-FSIS-FDA.pdf?MOD=AJPERES.

79. *Id.* at 2.

80. *Id.* at 3.

81. *See* USDA AND FDA FIRST STATEMENT ON REGULATION, *supra* note 72.

82. *See* discussion *supra* Section I.A.2.

A. *USDA Statutory Authority*

The USDA's regulation of meat relies on two parallel statutes providing for the regulation of both poultry and traditional red meats.[83] If cell-cultured meat is a "meat food product," it falls under USDA jurisdiction to regulate per the FMIA.[84] Therefore, arguments for USDA's jurisdiction over cell-cultured red meats rely on the definition of "meat food product," which is composed of three elements.

First, a "meat food product" only applies to products "capable of use as human food which [are] made wholly or in part from any meat or other portion of the carcass of any cattle, sheep, swine, or goats."[85] In its current form, cell-cultured meat likely meets this element because the initial sample used in the culture is taken from the legs of once-living cattle, sheep, swine, or goats.[86] However, groups are working to eliminate the need for a living animal to be slaughtered at all by acquiring initial tissue samples via biopsy from live animals.[87] Arguably, if this alternative process is successful, the USDA may lack jurisdiction to regulate any product derived from the process.

Further, even if taken from a dead animal, it is not totally clear that the tissue sample would constitute a "carcass." Interestingly, "carcass" does not seem to have a definition under the statute. Applying the normal meaning of the word, "carcass" would usually imply that the subject is dead, but the tissue sample itself when taken from the animal is very much alive—it must be alive for the cells to propagate. Thus, cultured meat producers could argue that the USDA does not have proper authority to regulate cultured meat on these grounds.

Second, a product that would otherwise be a "meat food product" *may* be "exempted from definition as a meat food product by the Secretary" *if* it "contain[s] meat or other portions of such carcasses only in a relatively small proportion."[88] The portion of the actual animal carcass used in cell-cultured meat is clearly small in proportion to the amount of meat it creates, but the FDA and USDA's 2018 joint statement shows that the

83. *See* 21 U.S.C. §§ 451–72, 601–95, 1031–56 (2018).

84. *See* 21 U.S.C. § 621 (2018) ("The Secretary shall appoint from time to time inspectors to make examination and inspection of all amenable species, inspection of which is hereby provided for, and of all carcasses and parts thereof, and of all meats and meat food products thereof, and of the sanitary conditions of all establishments in which such meat and meat food products hereinbefore described are prepared.").

85. 21 U.S.C. § 601(j) (2018).

86. *See supra* text accompanying note 58.

87. *See supra* notes 56–58 and accompanying text.

88. 21 U.S.C. § 601(j).

USDA Secretary has no current plans to except cell-cultured meat on this basis.[89] Therefore, this second element is also met.

Third, a product that would otherwise be a "meat food product" also *may* be "exempted from definition as a meat food product by the Secretary" *if* it has not "historically . . . been considered by consumers as [a] product[] of the meat food industry."[90] Again, there is certainly an argument that cell-cultured meat should be exempted because consumers may not consider cell-cultured meat to be a "meat food product," but the USDA has clearly indicated that they will not exclude cell-cultured meat from its authority in total in the near future, and the element is met.[91]

Thus, the USDA likely holds jurisdiction under the FMIA to regulate cell-cultured meat in its current form when derived from traditional red meats, meaning that derived from cattle, sheep, swine, and goats. Further, in the PPIA, equivalent language is used to give the USDA jurisdiction over "poultry product[s]" under the same circumstances (replacing "cattle, sheep, swine, and goats" in the FMIA with "poultry" and keeping the language otherwise the same).[92] Thus, the same arguments applied above to the regulation of "meat food product[s]" will apply to "poultry product[s]," as well.

Ultimately, the USDA likely holds jurisdiction under the FMIA and PPIA to regulate cell-cultured meats derived from traditional red meats and poultry, although this jurisdiction is subject to a shift to plant-based cell-cultured meats, to the uncertain definition of "carcass," and to exception by the USDA Secretary. Additionally, cell-cultured meats that lie outside the limits of USDA regulation in their traditional form, such as seafood and wild game, must also lie outside the limits of USDA regulation in their cell-cultured form, as the USDA does not have any statutory authority to claim jurisdiction in such cases.

B. *FDA Statutory Authority*

The FDA's source of authority to regulate cell-cultured meat is harder to pin down. The FDA has the broad authority to regulate "food," including "articles used for food or drink for man or other animals . . . [and] articles used for components of any such article."[93]

---

89. *See supra* notes 49, 84–92 and accompanying text.

90. 21 U.S.C. § 601(j).

91. *See supra* note 86 and accompanying text.

92. 21 U.S.C. § 453(f) (2018) ("The term 'poultry product' means any poultry carcass, or part thereof; or any product which is made wholly or in part from any poultry carcass or part thereof, excepting products which contain poultry ingredients only in a relatively small proportion or historically have not been considered by consumers as products of the poultry food industry, and which are exempted by the Secretary.").

93. 21 U.S.C. § 321(f) (2018).

However, the FFDCA expressly exempts those foods which qualify as "[m]eats and meat food products" under the FMIA, and the PPIA further exempts "[p]oultry and poultry products."[94] Therefore, if the USDA has jurisdiction under the FMIA or PPIA to regulate cell-cultured meat, the FDA will not have jurisdiction unless it is established under a separate provision in the future.

While some current laws may seem to provide a basis for FDA authority to regulate cell-cultured meat, most prove inapplicable. The FDA's authority to regulate cannot come from the Cloned Food Labeling Act (CFLA), as the CFLA only applies to products derived from once living, cloned animals and their progeny.[95] Some authorities claim that the FDA's authority also cannot come from New Animal Drug Application (NADA) requirements because scientists have not yet begun altering the DNA of animal tissue samples so as to create a genetically modified meat, though this may be a possibility in the future.[96]

There is significant disagreement, however, on whether the FDA's power to regulate cell-cultured meat could come from its power to regulate "food additives," defined in the FFDCA in its relevant portion as "any substance the intended use of which results or may reasonably be expected to result, directly or indirectly, in its becoming a component or otherwise affecting the characteristics of any food" and not yet be generally recognized as safe, or GRAS.[97] However, courts have further clarified that "in order to qualify as a food additive, a component must be added to a food in order to change that food's properties."[98]

Thus, because "[c]ultured meat is not added to food, it *is* the food," it is wrong to say that the FDA can regulate cultured meat because it *itself* is a food additive, but what is *added* to cells in the culturing process may qualify.[99] Because what qualifies as a "food additive" affects the FDA's

94. 21 U.S.C. §§ 392(a), 467f(a) (2018) ("Poultry and poultry products shall be exempt from the provisions of the Federal Food, Drug, and Cosmetic Act.").

95. B. George Walker, *Double Trouble: Competing Federal and State Approaches to Regulating the New Technology of Cloned Animal Foods, and Suggestions for the Future*, 14 J. TECH. L. & POL'Y 29, 49 (2009) (arguing that the CFLA excludes cell-cultured meat, or "in vitro meat," because it is not a "cloned product").

96. *See* Schneider, *supra* note 63, at 1014–15 (discussing the possible use of NADA contingent on the development of genetically modified meat).

97. 21 U.S.C. § 321(s) (2018); s*ee id.* at 1015 (arguing that cell-cultured meat is a food additive). *But see* Jennifer Penn, "*Cultured Meat": Lab-Grown Beef and Regulating the Future Meat Market*, 36 UCLA J. ENVTL. L. & POL'Y 104, 117 (2018) (arguing that cell-cultured meat is not a food additive).

98. United States v. 29 Cartons of * * * An Article of Food, 987 F.2d 33, 37 (1st Cir. 1993) (citing United States v. Two Plastic Drums, 984 F.2d 814 (7th Cir. 1993)).

99. Penn, *supra* note 97, at 108 (emphasis added).

ability to declare an additive as GRAS, it is important to identify which additives will qualify.

Arguably, the nutrient medium that is added to tissue samples to cause it to expand into what we would recognize as meat would qualify as a "food additive" because it is added to a food, namely a tissue sample, to cause that sample to change as the cells propagate. Whether this is a change in property is unclear, however. Does a change in property require some chemical change in the substance of the food, or is the extreme visual property change between a small clump of cells and a hunk of beef sufficient? Because the court does not define "properties," the law is unclear, but the FDA seems to think that it is sufficient.[100]

Clearer, however, is that other *possible* additives may qualify. Anticipated additives include gases, particularly oxygen and carbon dioxide, and "growth factors," such as cytokines, hormones, and signaling molecules.[101] Any one of these substances is sure to affect the chemical structure of the food, namely the clump of cells, that it is added to, and, thus, should qualify as a "food additive." There is a whole world of possible future developments, such as modifications to nutritional content or the development of blood vessels, that may require artificial additives that would qualify, as well.[102]

Thus, though it is not clear that the FDA has a source of authority to regulate cell-cultured meat *per se* in its *current* form, the FDA likely has authority to regulate most, if not all, of what is *added* to cells in the cell-culturing process, effectively giving it the power to regulate the cell-culturing process. However, this authority does not negate the USDA's authority, or vice versa, as the agencies share joint jurisdiction over food additives in meat.[103]

C. *The Best Authority is a New Authority*

It is worth noting that this jurisdictional murkiness is likely due to the inability of Congress, when drafting the statutes discussed above, to predict that cell-cultured meat would exist and how it would come about. The current statutes were not made to address these questions. Thus, the

---

100. *See FDA Transcript*, *supra* note 2, at 39 ("[Y]ou could have the same chemical identity of a substance and yet the properties could change a great deal depending on the actual size of the particles of the substance in the food."); Penn, *supra* note 97 (emphasis added).

101. U.S. DEP'T OF AGRIC. & U.S. FOOD &. DRUG ADMIN., USDA/FDA JOINT PUBLIC MEETING: THE USE OF CELL CULTURE TECHNOLOGY TO DEVELOP PRODUCTS DERIVED FROM LIVESTOCK AND POULTRY 10, https://www.fsis.usda.gov/wps/wcm/connect/ccb77304-98ad-40c9-a05a-1e22bcf68c70/Day-1A-Morning_USDA-FDA-Joint-Meeting.pdf?MOD=AJPERES (last visited Nov. 7, 2019).

102. Schneider, *supra* note 63, at 1015.

103. *See* FORTIN, *supra* note 12, at 29.

clearest way for Congress to indicate its intentions would be to set a new framework for jurisdiction which clarifies how the agencies should approach these emerging technologies.[104] Given recent announcements however, the USDA and FDA have indicated that they have no intention of sitting on their thumbs waiting for Congress to tell them what to do.[105]

III. EVALUATING THE PROPOSED SHARED JURISDICTION OF SAFETY REGULATION OF CULTURED MEAT

The USDA and FDA's decision to transition from FDA to USDA oversight at point of harvest is the best framework possible for safety regulation of cell-cultured meat. The FDA's extensive experience with regulating cell-cultured technologies and other emerging biotechnologies make it the agency best prepared to ensure the safety of the cell-culturing process.[106] On the other hand, the USDA's extensive experience with ensuring that meats are not contaminated post-harvest make it the best agency to ensure the safety of cell-cultured meat after it is harvested, when it will likely be just as vulnerable to contaminants as traditional meats.[107] Under the newly announced framework, the agencies would share jurisdiction in a way that best ensures the safety of the final product. That said, a deeper look at arguments on each side is helpful to understanding both the reasoning for this division and how such regulation may be implemented.

A. *What Would FDA Regulation of Cultured Meat Look Like?*

The argument for sole FDA regulation relies heavily on the FDA's experience regulating similar emerging technologies. Because the FDA has worked with GMOs, cloning, and cell-culture technologies in other contexts, the FDA would likely more easily adapt its current processes for evaluating the safety of those technologies into evaluations of cell-cultured meat production. This argument is simple, but compelling. However, it is not immediately apparent how the FDA would adapt those processes.

1. Evaluate each Individual Ingredient as GRAS?

One possibility is that the FDA apply its GRAS principle. Applying the GRAS principle, if the FDA has recognized each ingredient in cell-

104. Although this paper will not explore potential statutory frameworks given that the FDA and USDA have announced intentions to share jurisdiction, several previous articles have suggested potential frameworks. *See, e.g.*, Penn, *supra* note 97, at 126; *see also* Schneider, *supra* note 63, at 1025; Walker, *supra* note 95, at 47–50.

105. *See generally supra* notes 84–92 and accompanying text.

106. *See* discussion supra Section I.A.4.

107. *See* discussion *supra* Section I.A.2.

cultured meat as safe, the FDA would consider the final product safe.[108] To some degree, this approach makes sense, as all or most of the components added during the process are likely to be common materials that are generally safe and likely already recognized under GRAS. Those ingredients that are not already addressed by GRAS would be subject to FDA investigations, which would look into the scientific processes that create them to determine their safety.

The FDA used a similar approach to declare a form of rennet (which is created using a bacteria that was genetically engineered to produce rennet and is itself another form of animal cell-culture) to be safe.[109] Rennet is an "enzyme that goes into a product that is later inspected and certified," and is thus rightly treated as a food additive.[110] Cell-culture meat, however, is certainly not a food additive itself, but a collection of possible food additives.[111] Thus, unlike rennet, cell-cultured meat will need to be composed completely of food additives that are GRAS to be GRAS itself. While the FDA's experience with rennet will likely aid in its determination of potential risks, the FDA will have to use a different process to approve cultured meat.

Further, such an approach, when applied to cell-cultured meat, fails to account for the potential, unique risks that could arise due to the cell-culture process. One concern is that, if a pathogen makes its way into the bioreactor due to improper sanitary procedures, it could feed on the nutrient medium and propagate along with the cells, infecting an entire batch of the meat.[112] Notably, a similar concern applies to traditional meats as the contaminated meat of one cow, chicken, etc., may contaminate an entire batch of ground beef, chicken nugget mixture, etc., when mixed together.[113] While such a contaminant will ideally be caught

---

108. Determination of whether a new ingredient is GRAS is "based only on the views of experts qualified by scientific training and experience" through "scientific procedures" which "shall be based upon the application of generally available and accepted scientific data, information, or methods, which ordinarily are published, as well as the application of scientific principles, and may be corroborated by the application of unpublished scientific data, information, or methods." 21 C.F.R. § 170.30(a)–(b) (2019).

109. "Rennet" is a "mixture of enzymes that turns milk into curds and whey in cheesemaking," which traditionally was "extracted from the inner lining of the fourth stomach of calves." *What is Cellular Agriculture?*, NEW HARVEST, https://www.new-harvest.org/cell_ag_101 (last visited Nov. 6, 2019).; *id*.; *see also* Penn, *supra* note 97, at 116.

110. Penn, *supra* note 97, at 116.

111. *See* discussion *supra* Section II.B.

112. *See, e.g.*, *FDA Transcript*, *supra* note 2, at 74–75.

113. "Foods that mingle the products of many individual animals, such as . . . ground beef, are particularly hazardous because a pathogen present in any one of the animals may contaminate

in an inspection at harvest, if not before, the hand of regulators should be there to ensure that the process does not create new risks that will need to be evaluated for their safety, just as it is with traditional meats. Thus, cell-cultured meat should not be immediately regarded as GRAS, even if its ingredients are all GRAS.

2. Declare Cultured and Traditional Meat Substantially Equivalent?

Another possibility is that the doctrine of substantial equivalence could be applied to cell-cultured meats, just as it is with genetically engineered crops, better known as "GMOs." The doctrine of substantial equivalence allows the FDA to approve as *safe* foods that are substantially equivalent to existing GRAS foods.[114] Since the FDA's conclusion in 1992 that, in "most cases, the substances expected to become components of food as a result of genetic modification of a plant will be the same as or substantially similar to substances commonly found in food," the FDA "presumes that most [genetically engineered] foods are GRAS."[115] Evaluated under this framework, GMOs are exempt from "premarket review."[116]

Applying the doctrine to cell-cultured meat, the FDA could say that cell-cultured meat is safe if it is substantially equivalent to its traditional meat counterparts. Arguably, like most GMOs, cell-cultured meat will be substantially equivalent to the form of traditional meat it was derived from because the cells in the final product will be genetically identical to the original sample.[117]

However, producers are likely to make varying degrees of alterations, both intentional and unintentional, to the cells during production. For instance, producers may intentionally leave out pharmaceutical residues, alter fat content, or add artificial blood vessels to the cultured meat.[118] If

---

the whole batch. A single hamburger may contain meat from hundreds of animals. . . . A broiler chicken carcass can be exposed to the drippings and juices of many thousands of other birds that went through the same cold water tank after slaughter." CTR. DISEASE CONTROL, FOODBORNE ILLNESS: FREQUENTLY ASKED QUESTIONS 9 (Jan. 10, 2005), http://www.townofdurhamct.org/filestorage/28562/27556/27707/27719/03-26-2010_Health_Dept_foodborne.pdf.

114. *See* Trevor Findley, *Genetically Engineered Crops: How the Courts Dismantled the Doctrine of Substantial Equivalence*, 27 DUKE ENVTL. L. & POL'Y F. 119, 125–28 (2016) (discussing the nature and origin of the doctrine of substantial equivalence); FORTIN, *supra* note 12, at 286 (describing substantial equivalence as an analytical tool, important for determining safety of foods).

115. Statement of Policy: Foods Derived from New Plant Varieties, 57 Fed. Reg. 22,984, 22,985 (May 29, 1992); Trevor Findley, *Genetically Engineered Crops: How the Courts Dismantled the Doctrine of Substantial Equivalence*, 27 DUKE ENVTL. L. & POL'Y F. 119, 123 (2016).

116. Schneider, *supra* note 63, at 1007.

117. *See* discussion *supra* Section II.B.1.

118. *See* discussion *supra* Section II.B.2.

such changes are made, the doctrine of substantial equivalence should not apply.[119] Moreover, the lab setting may introduce new contaminants not found in traditional meats.[120] In such instances, the doctrine of substantial equivalence again should not apply because the risks associated with the food change substantially and will need separate approval. Ultimately, the FDA should only find that cell-cultured meat is substantially equivalent to its counterpart if it is proven that producers have not added any ingredients or contaminants that are not already found in traditional meats.

B. *The Pre- vs. Post-Harvest Contaminant Problem*

Supporters of granting FDA sole jurisdiction often rely on the argument that the lab setting used in the production of cultured meat will reduce the likelihood of contamination, so there is no need to heavily regulate production process itself, as long as the final product can be ensured as safe.[121] This argument certainly has some validity as the laboratory setting of cell-cultured meat harvest is likely to be a cleaner, more controlled environment than is found in the slaughterhouses where traditional meat is harvested. Traditional meat risks contamination at the time of slaughter due to cross-contamination between meat and fecal matter from other portions of the animal, such as the hide, intestines, and rectum.[122] In light of this dynamic, supporters of granting the FDA sole jurisdiction argue that the FDA's focus on the safety of final products and laxer regulations are appropriate.[123]

After harvest, cell-cultured meat will still need to be inspected, separated, packaged, and transported in a fashion likely similar to traditional meat. Laboratory setting or not, the possibility for cross-

119. Schneider, *supra* note 63, at 1015.

120. *See* discussion *infra* Section III.B.

121. *See, e.g.*, Linda MacDonald Glenn & Lisa D'Agostino, *The Moveable Feast: Legal, Ethical, and Social Implications of Converging Technologies on Our Dinner Tables*, 4 NE. U. L.J. 111, 124–25 (2012) ("It is vastly easier to monitor a food production operation than a farm. By moving the operation from the feedlot to the factory, there is the opportunity for better FDA oversight.").

122. *See* Farzaneh Bakhtiary et al., *Evaluation of Bacterial Contamination Sources in Meat Production Line*, 39 J. FOOD QUALITY 750 (2016) ("Bacterial spoilage of meat depends on the initial number of microorganism, time/temperature combination of storage conditions and physicochemical properties of meat. Mostly, contamination occurs because of inadequate hygienic conditions and handling in slaughterhouses, moreover the attachment properties and the biofilm formation of bacteria on surfaces facilitate cross-contamination. Preslaughter conditions like feeding and housing including spreadable contaminations from skin and feces, contents of digestion system, and contaminated water are sources of Staphylococcus, Escherichia and Bacillus cereus. Different processes in slaughterhouses like evisceration can contaminate carcasses and equipment with gut bacteria.").

123. *See FDA Transcript*, *supra* note 2.

contamination still exists. Surfaces, workers, clothing, and even the air can be shared between potentially contaminated samples and final products. While a laboratory setting may more easily satisfy USDA standards of cleanliness, etc., the setting should still be inspected to ensure that such cross-contamination is limited as much as possible.[124]

After leaving the laboratory-like production setting, cell-cultured meat, may be vulnerable to contaminants which cause foodborne illness in traditional meat, such as *Salmonella* and *E. coli*.[125] The USDA is best suited to inspect these production areas to ensure that safety protocols are followed, limiting cross-contamination. It is therefore fitting that the current agreement requires standard USDA safety inspections of cultured meat production facilities.[126]

C. *The Value of Split Jurisdiction at Harvest*

Although it is yet unclear how the FDA will regulate cell-cultured meat, the FDA's experience in cell-culture and other biotechnologies, and the likelihood of limiting exposure to contaminants pre-harvest, make it the most appropriate agency to efficiently evaluate the safety of cell-cultured meat up to the point of harvest. However, because cell-cultured meat will in essence be considered "meat" after harvest, it will likely be just as vulnerable to post-harvest contaminants as traditional meat. As compared to the FDA, the USDA has greater experience and capabilities to handle such risks. Splitting the power to regulate cell-cultured meat at the point of harvest is the best way to utilize the strengths and experience of both the FDA and USDA, ensuring efficient and safe regulation. However, the value of this dynamic ends at the point of labeling.

IV. EVALUATING THE PROPOSED USDA LABELING REGULATION OF CULTURED MEAT

Perhaps the most hotly contested issue concerning the regulation of cultured meat has been what to call it. As a result, there has been a great deal of debate over which agency should regulate labeling and what limits should be put in place.

---

124. 9 C.F.R. § 416 (2019).

125. *Foods That Can Cause Food Poisoning*, CTR. FOR DISEASE CONTROL, https://www.cdc.gov/foodsafety/foods-linked-illness.html (last modified Oct. 11, 2019).

126. *See* USDA AND FDA CULTURED MEAT MOU, *supra* note 78, at 3 ("USDA-FSIS will . . . [c]onduct inspection in establishments where cells cultured from livestock and poultry subject to the FMIA and PPIA are harvested, processed, packaged or labeled, in accordance with applicable FSIS regulations (including sanitation and physical product inspection, Hazard Analysis and Critical Control Point (HACCP) verification, product testing, and records review), to ensure that resulting products are safe, unadulterated, wholesome and properly labeled.").

There is often a seeming contradiction within these arguments. Cultured meat producers often argue that their product is similar enough to "meat" for it to bear the label "meat," but they simultaneously argue that their product is not "meat" under the statute which would allow USDA authority.[127] Conversely, traditional meat producers often argue that cultured meat is not "true" meat, and that allowing cultured meat to employ "meat" language misleads consumers and damages their brand, but they simultaneously argue that cultured meat falls under the statutory definition of "meat," such that it would fall under USDA authority.[128] Of course, both arguments have their strengths and weaknesses, but their apparent inconsistencies shed light on an irony within this discussion: is it "meat," or not?

A. *Policy and Constitutional Labeling Concerns*

1. Misleading Consumers

Arguably the most important consideration when determining whether a particular food is properly labeled is whether the label would mislead consumers. With this in mind, cultured meat should be labeled in a way that makes it clear that cultured meat is not traditional meat, but that it is almost chemically identical to its traditional form.

There will inevitably be people who, at least at first, will refuse to buy or eat cultured meat. They will want *clear* labeling that indicates to them whether meat is cultured or traditional. They would likely be very upset

127. Elaine Watson, *Cell-based Meat Cos: Please Stop Calling Us 'Lab-Grown' Meat… and We don't Use Antibiotics in Full-Scale Production*, FOOD NAVIGATOR-USA (Oct. 25, 2018, 4:33 PM), https://www.foodnavigator-usa.com/Article/2018/10/25/Cell-based-meat-cos-Please-stop-calling-us-lab-grown-meat-and-we-don-t-use-antibiotics-in-full-scale-production (providing a statement from Peter Licari on behalf of JUST, a supporter of cell-cultured meats: "With regard to labeling . . . we believe there should be both a regulatory nomenclature (e.g., statement of identity) and consumer-facing nomenclature that sufficiently differentiates cell-cultured products from traditional meat products but appropriately acknowledges these products as meat.").

128. *See id.* (providing a statement from meat producers, including: Kevin Kester on behalf of the National Cattlemen's Beef Association: "The FDA has consistently show it is unwilling or unable to enforce product labeling standards. The agency has turned a blind eye to labeling abuses from fake milk manufacturers for nearly three decades. Lab grown fake meat manufacturers must not be permitted to use the term beef and any associated nomenclature. It should only be applicable to livestock raised by farmers and ranchers." Danni Beer on behalf of the U.S. Cattlemen's Association: "We believe that cell-cultured proteins should be regulated as strictly as beef, but that these products should have their own food category and inspection process, not using our stamp or shield. The alternative protein industry should not be allowed to villainize the beef cattle industry. We should have standards of identity to establish these products as different from meat or beef . . . Consumers . . . think of what we're doing as families taking care of the land, taking care of the cattle everyday . . . they don't think about somebody putting a group of cells together and growing a new product. That's not beef.").

to learn that something labeled simply "beef" was not meat taken from a once-living cow, as they expect it to be. Further, some people will actually seek out cultured meat. Whether for dietary, environmental, or moral reasons, or simply out of curiosity, those seeking out cultured meat will want to be able to quickly identify and distinguish it from traditional meat. Thus, both those wishing to seek out and those wanting to avoid cultured meat will want labeling to provide clear identification. It would mislead both groups to simply call cultured beef "beef" or cultured chicken "chicken" without some modifier indicating its origin.

However, to not allow cultured beef to call itself "beef" at all could be dangerous. Most importantly, a significant portion of the population is allergic to certain meats.[129] Individuals with meat allergies will almost certainly be allergic to the cultured version of those meats, as well, as the two versions will be nearly chemically identical. These people *need* labeling that clearly indicates that cultured beef is "beef" and cultured chicken is "chicken." If modifiers such as "imitation beef" or "artificial chicken" are applied, or if regulators prohibit cultured meat producers from using terms like "beef" or "chicken" altogether, it is possible that people may mistakenly consume cultured meat, wrongly assuming that it is something akin to the plant-based proteins that already exist. In order to protect the interests of consumers, it is crucial that labelling clearly distinguished cultured meat from plant-based proteins.

2. Overburdening Producers

Regulators must not overburden producers when determining proper labeling restrictions for cultured meat due to policy and First Amendment considerations. While the First Amendment's protection of the freedom of speech includes protections for "commercial speech," the Court has held that there is a "'commonsense' distinction between speech proposing a commercial transaction, which occurs in an area traditionally subject to government regulation, and other varieties of speech."[130] Accordingly, "courts have found that the government can prohibit misleading speech, require manufacturers to display commercial messages in certain forms, and include additional information, warnings,

---

129. *See* Jeffrey M. Wilson & Thomas A.E. Platts-Mills, *Meat Allergy and Allergens*, MOLECULAR IMMUNOLOGY 107, 111 (2018) ("Despite traditionally being considered rare, meat allergy is being increasingly recognized in subjects of all ages.").

130. "Congress shall make no law . . . abridging the freedom of speech." U.S. CONST. amend. I; "Courts have characterized food labels as 'commercial speech.'" Melissa M. Card, *America, You are Digging Your Grave with Your Spoon-Should the FDA Tell You That on Food Labels?*, 68 FOOD & DRUG L.J. 309, 313 (2013); Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm. of N.Y., 447 U.S. 557, 562 (1980).

or disclaimers."[131] This means that while regulators do in fact have the power to regulate misleading labels, they must be careful to not infringe upon cultured meat producers' right to free speech.[132]

Regulators should take care not to overburden cultured meat producers in labeling restrictions for policy reasons, as well. If cultured meat is prevented from using the same terms used to describe traditional meat (such as "beef" and "chicken") all together, or is required to bear a modifier such as "artificial," "imitation," or even "lab-grown" that conveys a negative, undesirable tone, regulators risk alienating consumers from the beginning. Given the world of possibilities cultured meat presents, this would be a grave mistake.

Finally, it should be noted that regulators should keep fairness in mind, as well. Plant-based proteins made to imitate meats already use terms like "meat," "beef," "chicken," and "burger" to describe what they are imitating—they are simply required to provide some form of qualifier, such as "vegetarian," "garden," "meatless," "plant-based," or "soy," which indicates to the consumer that this is not actually meat.[133] Given that plant-based protein producers can place neutral and even positive qualifiers on "meat" language without confusing consumers, why not allow cultured meat producers to do the same?

---

131. Card, *supra* note 130, at 312–13.

132. Some states, such as Missouri, have already run into First Amendment problems with broad statutes that prevent both cultured meat and plant-based meat substitutes from using meat language. *See, e.g.*, Amie Tsang, *What, Exactly, Is Meat? Plant-Based Food Producers Sue Missouri over Labeling*, N.Y. TIMES (Aug. 28, 2018), https://www.nytimes.com/2018/08/28/us/missouri-meat-law-tofurky.html (reporting on a First Amendment suit over a Missouri statute that prohibits "misrepresenting a product as meat that is not derived from harvested production livestock or poultry"); Sam Bloch, *Lawmakers in Nebraska, Wyoming, and Virginia Say if it's Not a Carcass, Then it's "Imitation,"* THE NEW FOOD ECONOMY (Jan. 28, 2019), https://newfoodeconomy.org/missouri-nebraska-cell-cultured-plant-based-meat-labeling/ (reporting on statutes in Nebraska, Wyoming, and Virginia that are "following in the footsteps" of the Missouri law); Nathaniel Popper, *You Call That Meat? Not so Fast, Cattle Ranchers Say*, N.Y. TIMES (Feb. 9, 2019), https://www.nytimes.com/2019/02/09/technology/meat-veggie-burgers-lab-produced.html?smid=nytcore-ios-share (reporting on similar, newly-introduced meat-labeling bills in Arizona and Arkansas as well as past, similar bills in Virginia, Washington, and Nebraska).

133. *See, e.g.*, Adam Bryan, *16 Popular Fake Meat Brands – The Complete List of Products (2020)*, URBAN TASTEBUD, https://urbantastebud.com/fake-meat-brands/ (last visited Feb. 10, 2020) (providing examples of names of plant-based proteins and brand names, including: "Beyond Meat," "beef-less ground beef," "meatless meatballs," "garden veggie burger," "smoky chipotle meatless chicken," and "soy chorizo"); *Deli Slices*, TOFURKY, https://tofurky.com/what-we-make/deli-slices/hickory-smoked/ (last visited Feb. 10, 2020) ("Hickory Smoked Plant-Based Deli Slices"); Marissa Miller, *The 15 Best Vegetarian and Vegan Meat Substitutes* WOMEN'S HEALTH (Dec. 10, 2018), https://www.womenshealthmag.com/food/a19914260/best-meat-substitutes/ ("Vegetarian Grain Meat Sausages").

B. *Statements of Identity*

With these considerations in mind, we must again ask: what should we call cultured meat? Both the USDA and FDA will find that a food is "misbranded" if it does not prominently display its "statement of identity."[134] For some foods, statements of identity are "specified in or required by . . . [f]ederal law or regulation" and must comply with the definitions set in those laws to use those statements of identity.[135] If there is no such applicable law or regulation, the statement of identity must be a "common or usual name of the food," if one exists.[136] If there is no common or usual name, then the statement of identity must be "[a]n appropriately descriptive term, or when the nature of the food is obvious, a fanciful name commonly used by the public for such food."[137]

1. Statutory or Regulatory Statement of Identity

Currently, there is no statutory or regulatory statement of identity that should be applied to cultured meat. When a plant-based protein refers to itself as "meatless chicken" or "beef-less ground beef," the statements of identity which apply to traditional meats are not breached.[138] As such, when cultured meat refers to itself as "cultured chicken" or "cultured ground beef," the statements of identity should not be implicated. In both cases, the modifiers applied indicate a deviation from the term's normal application in a way that the consumer would understand.

This argument is similar to that made by "soy milk," "almond milk," and "coconut milk" producers in defense of their use of the term "milk" in their statements of identity.[139] The FDA has recognized that there is a statement of identity that applies to "milk" which is limited to milk obtained from cows.[140] This recognition makes sense in that, when someone refers to "milk" without modifying the statement, they are usually referring to cow's milk. Thus, if something is simply labeled "milk" in a supermarket, the typical consumer will assume that it is cow's

134. *See* 21 C.F.R. § 101.3(a)–(e) (2019) (establishing FDA's food statement of identity requirement); *see also* 9 C.F.R. § 319.1(a) (USDA's meat product statements of identity requirement); *see also* 9 C.F.R. § 381.1(b) (USDA's poultry product statements of identity requirement).

135. 21 C.F.R. § 101.3(b)(1); *see also* U.S. DEPT. OF AGRIC., A GUIDE TO FEDERAL FOOD LABELING REQUIREMENTS FOR MEAT, POULTRY, AND EGG PRODUCTS 28–29 (2007), https://www.fsis.usda.gov/wps/wcm/connect/f4af7c74-2b9f-4484-bb16-fd8f9820012d/Labeling_Requirements_Guide.pdf?MOD=AJPERES [hereinafter USDA LABELING GUIDE].

136. 21 C.F.R. § 101.3(b)(2); *see also* USDA LABELING GUIDE, *supra* note 135, at 29.

137. 21 C.F.R. § 101.3(b)(3); *see also* USDA LABELING GUIDE, *supra* note 135, at 29–30.

138. *See* Bryan, *supra* note 133 and accompanying text.

139. *See* Ang v. Whitewave Foods Co., No. 13-CV-1953, 2013 WL 6492353, at *4 (N.D. Cal. Dec. 10, 2013) (unreported).

140. 21 C.F.R. § 131.110(a) (2019).

milk. However, the same consumer will understand that "soy milk" was not obtained from a cow, even if he or she does not understand exactly how similar "soy milk" is to "milk." The addition of the modifier changes the meaning of the otherwise recognized term "milk" in a way that does not mislead consumers and, thus, is allowed. However, this has not stopped "milk" producers from contesting the FDA's policy of allowing such labeling.[141]

Although these "milk" suits have not been successful, the FDA has agreed to review its policy out of "concerns that the labeling of some plant-based products may lead consumers to believe that those products have the same key attributes as dairy products, even though these products can vary widely in their nutritional content."[142] This concern is based on "significant health consequences—contributing to under consumption of key nutrients, such as calcium and vitamin D for which dairy products are good sources in the U.S. population."[143] Although this statement does throw into question whether the FDA will continue its policy of allowing terms like "almond milk" to be used, it also clarifies that the FDA's concerns are not focused on misleading consumers as to the origin of the products, but rather of their relative nutritional content. The FDA is simply not concerned that consumers will believe that "almond milk" is derived from cows. Instead, the FDA is concerned that consumers will believe "almond milk" is a sufficient nutrient replacement for cow's milk.

In contrast to plant-based dairy products, cultured meat should not, in its basic form, have any significant nutritional deviation from traditional meats because the cells will be genetically identical.[144] Thus, there should be no concern that consumers will be misled as to the nutritional value of cultured meats. Moreover, any changes to the nutritional value of cultured meat should be beneficial, incentivizing producers to advertise those changes.[145] The FDA's current policy of recognizing that labeling modifiers affect the meaning of the statements of identity in a way that informs the consumer as to their origins should be maintained. Thus, similar modifiers should be allowed to distinguish cultured meat from traditional meat in a way that does not mislead consumers.

---

141. *See supra* note 26 and accompanying text.

142. *See Ang*, 2013 WL 6492353, at *4; U.S. FOOD & DRUG ADMIN., STATEMENT FROM FDA COMMISSIONER SCOTT GOTTLIEB, M.D., ON MODERNIZING STANDARDS OF IDENTITY AND THE USE OF DAIRY NAMES FOR PLANT-BASED SUBSTITUTES (Sept. 27, 2018), https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm621824.htm.

143. *Id.*

144. *See* discussion *supra* Section II.B.1.

145. *See supra* notes 59–61 and accompanying text.

Thus, regardless whether current statutory or regulatory statements of identity currently apply, or if new statements of identity are created that would apply, to traditional meat forms, cultured meat producers should be allowed to use such statements of identity as long as there is some modifier added which would distinguish them from their traditional form in a way that consumers will understand the differences between the products.

2. Common or Usual Name

Because no statute or regulation establishes statements of identity for cultured meats, the next step is to determine whether there exists a common or usual name that could be used as a statement of identity. Simply put, there are no such common or usual names. As established, cultured meat currently goes by a wide variety of names depending on who is describing it.[146] Moreover, since cultured meat has not yet experienced large-scale production, many do not even know that it exists, and would therefore not know what to call it. As such, there is no common or usual name that could be properly applied as a statement of identity for cultured meats.

3. Descriptive Term

A statement of identity for cultured meat must be a descriptive term, but one must ask: What term would be appropriate?[147] Some cultured meat producers and supporters argue that the term "clean meat" is appropriate because their product will be made without pharmaceutical residues, contaminants, etc., that are found in some traditional meats.[148] Traditional meat producers vehemently oppose the term "clean meat" because, they argue, it implies that traditional meat is "dirty."[149] Given that cultured meat may open itself to new methods of contamination, and the overall relative safety of cultured meat is yet unknown, this is a fair

146. *See supra* notes 2–5 and accompanying text.

147. There is no proper "fanciful" term here to be applied. Thus, a descriptive term alone must be used.

148. *See Clean Meat Basics*, CELLMOTIONS, https://www.cellmotions.com/pages/clean-meat-basics (last visited Jan. 19, 2020) ("Animal agriculture is unsustainable, environmentally harmful, bad for human health, and bad for animals. Clean meat mitigates or solves these problems."); s*ee, e.g.*, Bruce Friedrich, *"Clean Meat": The "Clean Energy" of Food*, GOOD FOOD INST. (Sept. 6, 2016), https://www.gfi.org/clean-meat-the-clean-energy-of-food (demonstrating that The Good Food Institute, a promoter of cultured meat and its producers, refers to clean meat in this way).

149. *See, e.g.*, Candice Choi, *Meat 2.0? Clean Meat? Spat Grows over Food Wording*, DET. NEWS (June 20, 2018), https://www.detroitnews.com/story/business/2018/06/19/meat-clean-meat-spat-grows-food-wording/36184473/ ("'It implies that traditional beef is dirty,' says Danielle Beck, director of government affairs for the National Cattleman's Beef Association.").

criticism.[150] Moreover, the modifier "clean" does not indicate to the consumer that the method of production has changed and therefore risks misleading consumers. Consumers may believe, for instance, that "clean" indicates that it is simply pharmaceutical residue-free or pathogen-free but still harvested straight from once-living animals. Since consumers care about such distinctions, "clean" is not an appropriate modifier to indicate the deviation from the typical understanding of "meat," "beef," "chicken," etc.[151]

Traditional meat producers, on the other hand, often argue that, if cultured meat is allowed to use "meat" language at all, it should bear a modifier that would indicate that it is not *truly* meat, such as "faux," "imitation," "artificial," or "synthetic."[152] However, these terms similarly fail to adequately inform consumers about what they are eating. Consumers require notice that cultured meats are, with the exception of their method of production, identical to their traditional meat counterparts; otherwise, regulators risk exposing consumers to dangerous allergens.[153] Moreover, use of these terms risk overburdening cultured meat producers, in ways which implicate both policy and First Amendment concerns.[154] Furthermore, the term "imitation" has its own legal definition which cannot apply to cultured meat.[155]

The descriptive term used to modify cultured meat should be one that indicates its method of production. Although the modifier "lab-grown" properly informs consumers on the method of production, requiring producers to label their product with a term that has an arguably negative tone is arguably too burdensome.[156]

"Cultured," on the other hand, has a neutral tone but still notifies consumers of the origin of the meat. The term indicates that cultured meat is meat without misleading the consumers into believing that they are purchasing traditionally produced meat. Further, because of its neutral tone, "cultured" does not overburden producers in a way that may be

150. *See* discussion *supra* Section III.B.

151. *See* discussion *supra* Section IV.A.1.

152. *See FDA Transcript*, *supra* note 2, at 161 ("The United States Cattlemen's Association . . . believe[s] that the term meat pertains exclusively to a protein food product that was harvested from the flesh of an animal in a traditional manner. Cultured cell protein would not be included in this definition.").

153. *See* discussion *supra* Section IV.A.1.

154. *See* discussion *supra* Section IV.A.2.

155. "Imitation" products "resemble" but are "nutritionally inferior to the standardized product." USDA LABELING GUIDE, *supra* note 135. There is no incentive for cultured meat producers to alter cultured meat to be nutritionally inferior to the traditional products that they are derived from. Thus, it would be improper for the label to be applied in absence of evidence of a cultured meat producer's intention to create a nutritionally inferior product.

156. *See* discussion *supra* Section IV.A.2.

harmful to progress, potentially unfair, and constitutionally suspect.[157] Thus, "cultured" is the best modifier to use as a descriptive term in statements of identity for cultured meat.

C. *FDA or USDA Labeling Control?*

I turn now to the question: Which agency should regulate labeling of cultured meat? Arguably, the FDA is better suited to regulate cultured meat products for the same reason that it is better suited to regulate the safety of cultured meat products pre-harvest—because it has experience in regulating other forms of biotechnology such as genetic engineering, other cultured foods, etc., which could be applied to cultured meat. For example, the FDA already has a system in place to evaluate whether a genetically modified piece of corn requires special labeling identifying it as genetically modified.[158] On the other hand, the USDA is arguably better suited to regulate cultured meat labeling because it already has a system in place to regulate traditional meats. Meat grading is one example of these important USDA functions.[159]

Based on the above considerations, the best option is to allow the FDA to determine whether a given cultured meat product qualifies as "cultured meat" as defined by the recognized statement of identity.[160] The FDA would additionally be responsible for determining, based on their investigation of the safety of the product pre-harvest, if the product requires any sort of warning regarding its production methods. The USDA would then grade the cultured meat, regulate its nutrition facts, require portions of labels, etc., as they would for a traditional meat product of the same kind.

However, under the current agreement, the USDA will require cultured meat producers to seek preapproval of labelling as they do with traditional meats.[161] This requirement would make sense if cultured meat products properly fell under current USDA standards of identity, but they do not.[162] The FDA is better suited to determine whether the product violates a standard of identity and to develop a new standard of identity.

---

157. *See* discussion *supra* Section IV.A.2.

158. "No special federal labeling requirements exist for GE food products if they meet the standard of substantial equivalence." Schneider, *supra* note 63, at 1007.

159. *See* Armour & Co. v. Ball, 468 F.2d 76, 81 (6th Cir. 1972) ("[O]ne purpose of the Wholesome Meat Act is to empower the Secretary to adopt definitions and standards of identity or composition so that the 'integrity' of meat food products could be 'effectively maintained.'").

160. *See* discussion Section V.B.

161. *See* USDA AND FDA CULTURED MEAT MOU, *supra* note 78, at 3 ("USDA-FSIS will . . . [r]equire that the labeling of human food products derived from the cultured cells of livestock and poultry be preapproved and then verified through inspection, as required by FSIS regulations.").

162. *See* discussion *supra* Section IV.B.1.

Thus, while the USDA may still require its mark of inspection, it should not require premarket approval for *all* labelling.

CONCLUSION

The road to mass production and distribution of cultured meat is going to be bumpy. The science is not quite to a point where cultured meat can be produced efficiently. Even once the science catches up, obstacles will still remain, such as the problem of actually convincing people to eat cultured meat, subject to the "ick factor."[163] Government agencies should be prepared, however, to quickly, but safely get these products on the market once they are in mainstream production. The potential benefits of this technology are too great to justify any delay longer than necessary to ensure consumer safety.

Because both the USDA and FDA have claimed jurisdiction over cultured meat, it is important to sort out the likely complex regulatory framework of regulation prior to cultured meat becoming market ready. By holding public meetings and announcing their proposed framework for agency jurisdiction of cultured meat, the USDA and FDA have taken the first step in accomplishing just that, but much is still unknown about how these products will be regulated.

Because the USDA and FDA's proposed framework properly designates the FDA to regulate the safety of cultured meat pre-harvest, the FDA needs to begin work now to determine how cultured meat will fit into its current policies, as this is presently unclear. The FDA should further be responsible for regulating post-harvest safety of cultured meat versions of the wild game and seafood that it currently regulates. Excepting these meats, the proposed framework further properly designates the USDA to regulate the safety of cultured meat post-harvest generally, because, after this point, cultured meat is effectively identical to and likely subject to the same or similar vulnerabilities as traditional meat.

The proposed framework is flawed, however, in that it improperly designates the USDA as sole regulator of cultured meat labeling. The FDA is better equipped to designate whether cultured meat products apply to a new statement of identity for the products, which should include the modifier "cultured," and to determine whether the products require some form of warning label. However, the USDA is well-equipped to label cultured meat in other fashions as it would traditional

163. One online survey found that, "although most respondents were willing to try in vitro meat, only one third were definitely or probably willing to eat in vitro meat regularly or as a replacement for farmed meat." MATTI WILKS & CLIVE J. C. PHILLIPS, ATTITUDES TO *IN VITRO* MEAT: A SURVEY OF POTENTIAL CONSUMERS IN THE UNITED STATES 1 (Stephanie S. Romanach ed., 2017), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5312878/pdf/pone.0171904.pdf.

meats, including grading and regulating nutrition facts. Thus, the agencies should split jurisdiction of labeling cultured meat as well.

FAKE NEWS (& DEEP FAKES) AND DEMOCRATIC DISCOURSE

Russell L. Weaver[*]

INTRODUCTION

The U.S. Declaration of Independence was transformational because it declared the independence of the American colonies from England and incorporated democratic ideals. In 1776, most European countries were governed by monarchs, some of which had (at one point, at least) purported to rule by Divine Right. In the Declaration of Independence, the signers implicitly rejected the idea of Divine Right by flatly asserting their right to throw off a despotic monarch and declaring that the power to govern derives from the consent of the governed.[1] As the U.S. Supreme Court recognized in *New York Times Co. v. Sullivan*,[2] quoting James Madison, "the Constitution created a form of government under which 'The people, not the government, possess the absolute sovereignty,'" dispersing "power in reflection of the people's distrust of concentrated power, and of power itself at all levels," thus creating an entirely new form of government "from the British form, under which the Crown was sovereign and the people were subjects."

In the Constitution, freedom of speech was not initially regarded as an indispensable component. Indeed, the Framers of the U.S. Constitution believed that a bill of rights (which would have included specific protections for free speech) was not needed because they had created a government of limited and enumerated powers[3]—one whose power was sufficiently checked by the doctrine of separation of powers and other

* Professor of Law & Distinguished University Scholar, University of Louisville, Louis D. Brandeis School of Law.

1. *See generally* The Declaration of Independence (U.S. 1776).
2. New York Times Co. v. Sullivan, 376 U.S. 254, 274 (1976).
3. *See* U.S. Const., Art. I, § 8.

limitations built into the new Constitution.[4] However, the people disagreed, and it rapidly became clear that the Constitution might not have enough support to gain ratification without the addition of a formal bill of rights.[5] In an effort to salvage the Constitution, proponents urged ratification of the document "as is," but promised that the first Congress would create what became the Bill of Rights.[6] Only then was ratification possible.[7] As a result, the Bill of Rights (and the right to freedom of expression) entered the Constitution as an amendment rather than in the body of the Constitution itself.[8]

Over time, it became apparent that freedom of expression and freedom of the press were indispensable components of the U.S. governmental system.[9] Indeed, the U.S. Supreme Court has declared that "Speech concerning public affairs is more than self-expression; it is the essence of self-government."[10] In a democratic system, change does not simply

4. *See* Ralph Ketcham, The Anti-Federalist Papers and the Constitutional Convention Debates: The Clashes and the Compromises That Gave Birth to Our Form of Government 6 (1986) ("Also, mindful of colonial experience and following the arguments of Montesquieu, the idea that the legislative, executive, and judicial powers had to be 'separated,' made to 'check and balance' each other in order to prevent tyranny, gained wide acceptance.").

5. *See* Wallace v. Jaffree, 472 U.S. 78, 92–93 (1985) (White, J., dissenting) ("During the debates in the Thirteen Colonies over ratification of the Constitution, one of the arguments frequently used by opponents of ratification was that without a Bill of Rights guaranteeing individual liberty the new general Government carried with it a potential for tyranny.").

6. *See* McDonald v. City of Chicago, 561 U.S. 742, 769 (2010) ("But those who were fearful that the new Federal Government would infringe traditional rights such as the right to keep and bear arms insisted on the adoption of the Bill of Rights as a condition for ratification of the Constitution.").

7. *See id.* at 769 ("But those who were fearful that the new Federal Government would infringe traditional rights such as the right to keep and bear arms insisted on the adoption of the Bill of Rights as a condition for ratification of the Constitution."); Marsh v. Chambers, 463 U.S. 783, 816 (1983) (Brennan, J., dissenting) ("The first 10 Amendments were not enacted because the members of the First Congress came up with a bright idea one morning; rather, their enactment was forced upon Congress by a number of the States as a condition for their ratification of the original Constitution.").

8. *McDonald*, 561 U.S. at 769.

9. *See generally* C. Edwin Baker, *Scope of the First Amendment Freedom of Speech*, 25 UCLA L. Rev. 964 (1978); Robert H. Bork, *Neutral Principles and Some First Amendment Problems*, 47 Ind. L.J. 1 (1971); Thomas I. Emerson, *Toward a General Theory of the First Amendment*, 72 Yale L.J. 877 (1963); Alexander Meiklejohn, *The First Amendment as an Absolute*, 1961 Sup. Ct. Rev. 245; Russell L. Weaver & Catherine Hancock, The First Amendment: Cases, Materials and Problems (Carolina Academic Press, 6th ed., 2020).

10. Connick v. Myers, 461 U.S. 138, 145 (1983) (quoting Garrison v. Louisiana, 379 U.S. 64, 74–75 (1964)); *see also* R.A.V. v. City of St. Paul, 505 U.S. 377, 422 (1992) (Blackmun, J., concurring) ("core political speech occupies the highest, most protected position"); *see also* Roth v. United States, 354 U.S. 476, 484 (1957) ("The protection given speech and press was fashioned to assure unfettered interchange of ideas for the bringing about of political and social changes desired by the people.").

"happen," but is instead driven by the people, and the "constitutional safeguard [for free expression] 'was fashioned to assure unfettered interchange of ideas for the bringing about of political and social changes desired by the people,'" so that "changes may be obtained by lawful means."[11] Indeed, free speech is so important to the U.S. governmental system that former U.S. Supreme Court nominee, Robert Bork argued that the "entire structure of the Constitution creates a representative democracy, a form of government that would be meaningless without freedom to discuss government and its policies."[12] Bork believed that protections for political speech are so essential to the democratic process that they "could and should be inferred even if there were no first amendment."[13] He defined political speech as "criticisms of public officials and policies, proposals for the adoption or repeal of legislation or constitutional provisions and speech addressed to the conduct of any governmental unit in the country."[14]

"Fake news" creates problems for democratic systems because it has the potential to mislead the public, and undermine the quality of public debate through the use of false facts. Social media is a frequent source of fake news. For example, Twitter accounts have provided a major source of propaganda and misinformation.[15] During the 2016 election, the Twitter Data Science Team found some 50,000 Russia-linked accounts that were spreading disinformation, and it also found that disinformation was being spread by both Republican and Democratic partisans.[16]

---

11. New York Times, Co. v. Sullivan, 376 U.S. 254, 269 (1964) (quoting Roth v. United States, 354 U.S. 476, 484 (1957) & Stromberg v. California, 283 U.S. 359, 369 (1931)); *see also* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 339, 341 (2010) ("Speech is an essential mechanism of democracy, for it is the means to hold officials accountable to the people. The right of citizens to inquire, to hear, to speak, and to use information to reach consensus is a pre-condition to enlightened self-government and a necessary means to protect it. The First Amendment 'has its fullest and most urgent application' to speech uttered during a campaign for political office.'" "It is inherent in the nature of the political process that voters must be free to obtain information from diverse sources in order to determine how to cast their votes."); *see also* Virginia v. Black, 538 U.S. 343, 365 (2003) ("[L]awful political speech [is] at the core of what the First Amendment is designed to protect.").

12. *See* Bork, *supra* note 9, at 23; *see also id*. at 20 ("Constitutional protection should be accorded only to speech that is explicitly political. There is no basis for judicial intervention to protect any other form of expression, be it scientific, literary or that variety of expression we call obscene or pornographic.").

13. *Id.* at 23.

14. *Id.* at 29.

15. Farhad Manjoo, *How Twitter is Being Gamed to Feed Misinformation*, N.Y. Times, June 1, 2017, at B-1, B-7 ("But the biggest problem with Twitter's place in the news is its role in the production and dissemination of propaganda and misinformation."). This article offers the example of a conspiracy theory suggesting that the murder of a staffer at the Democratic National Committee was linked to the leak of Clinton campaign emails. *Id.* at B-7.

16. Matthew Hindman & Vlad Barash, *Disinformation, 'Fake News' and Influence*

Facebook has nearly two billion users worldwide,[17] "reaches approximately 67% of U.S. adults," and 44% of U.S. adults state that they receive their news from Facebook.[18] As a result, "digging up large-scale misinformation on Facebook was as easy as finding baby photos or birthday greetings."[19] Included "were doctored photos . . . of Latin American migrants headed towards the United States border," as well as "easily disprovable lies about the women who accused Justice Brett M. Kavanaugh of sexual assault, cooked up by partisans with bad-faith agendas."[20] Indeed, "every time major political events dominated the news cycle, Facebook was overrun by hoaxers and conspiracy theorists, who used the platform to sow discord, spin falsehoods and stir up tribal anger."[21] For example, during the 2016 presidential campaign, conspiracy theorists circulated false internet rumors to the effect that then presidential candidate Hillary Clinton and her campaign manager were operating a child sex ring out of a restaurant.[22]

The situation is complicated further by two other phenomena: "bots" and "deep fakes." In recent years, "robotic speech bots" (bots) are increasingly able to disseminate speech on a mass scale.[23] Indeed, in some instances, bots can even create the content that is disseminated. "Deep fakes" involve video content that has been altered in some way.[24] For example, in 2019, someone altered a video of House Speaker Nancy Pelosi to make it appear that she was drunk and slurring her speech.[25] This false impression was possible because the pace of the video was slowed down and the pitch of her voice was raised as well.[26] In another

---

Campaigns on Twitter, Knight Found., Oct. 2018, at 4, 33.

17. Dr. Joel Timmer, *Fighting Falsity: Fake News, Facebook and the First Amendment*, 35 Cardozo Arts & Ent. L.J. 669, 672 (2017).

18. *Id.* at 672–73.

19. Kevin Roose, *Facebook Thwarted Chaos on Election Day. It's Hardly Clear That Will Last.*, N.Y. Times: The Shift, Nov. 8, 2018, at B1.

20. *Id.*

21. *Id.*

22. *See* Jennifer Ludden, *Armed Man Threatens D.C. Pizzeria Targeted by Fake News Stories*, Nat'l Pub. Radio: All Things Considered (Dec. 5, 2016), https://www.npr.org/2016/12/05/504467162/armed-man-threatens-d-c-pizzeria-targeted-by-fake-news-stories.

23. *See* Manjoo, *supra* note 15, at B-7.

24. Grace Shao, *What 'Deepfakes' Are and How They May Be Dangerous*, CNBC (Oct. 13, 2019), https://www.cnbc.com/2019/10/14/what-isfdeepfake-and-how-it-might-be-dangerous.html.

25. Drew Harwell, *Faked Pelosi Videos, Slowed to Make Her Appear Drunk, Spread Across Social Media*, Wash. Post (May 24, 2019), https://www.washingtonpost.com/technology/2019/05/23/faked-pelosi-videos-slowed-make-her-appear-drunk-spread-across-social-media/.

26. *Id.*

instance, someone altered a video of former President Barrack Obama to make it appear that he was saying something that he did not say.[27]

This Article explores the problems related to fake news, bots and deep fakes. In addition to discussing the problems that they pose for public debate, it examines whether society has effective ways to deal with these problems.

I. FAKE NEWS

Fake news, or inaccurate and misleading information, is nothing new. Some individuals have always been willing to spread lies or inaccurate information about others.[28] However, with the development of the internet, the problem has become much worse.[29] For centuries, information passed between people by word of mouth or by handwritten methods, but generally information moved at the pace at which people could move.[30] Not until the fifteenth century, when Johannes Gutenberg invented the printing press,[31] did it become possible to easily create multiple copies of documents.[32] Although the printing press did not increase the speed at which information could disseminate, the ability to create multiple copies allowed information to spread more broadly. This led to a flowering of knowledge, information and ideas, which ultimately

---

27. Hallie Jackson, *Fake Obama Warning about 'Deep Fakes' Goes Viral*, MSNBC (Apr. 19, 2018), https://www.msnbc.com/hallie-jackson/watch/fake-obama-warning-about-deep-fakes-goes -viral-1214598723984.

28. *See* Jacob Soll, *The Long and Brutal History of Fake News*, Politico (Dec. 18, 2016), https://www.politico.com/magazine/story/2016/12/fake-news-history-long-violent-214535. Political debate his involved not only outright lies, but also satire and ridicule. *See Hustler Magazine, Inc. v. Falwell*, 485 U.S. 46, 54–55 (1988) ("Despite their sometimes caustic nature, from the early cartoon portraying George Washington as an ass down to the present day, graphic depictions and satirical cartoons have played a prominent role in public and political debate. Nast's castigation of the Tweed Ring, Walt McDougall's characterization of Presidential candidate James G. Blaine's banquet with the millionaires at Delmonico's as 'The Royal Feast of Belshazzar,' and numerous other efforts have undoubtedly had an effect on the course and outcome of contemporaneous debate. Lincoln's tall, gangling posture, Teddy Roosevelt's glasses and teeth, and Franklin D. Roosevelt's jutting jaw and cigarette holder have been memorialized by political cartoons with an effect that could not have been obtained by the photographer or the portrait artist. From the viewpoint of history it is clear that our political discourse would have been considerably poorer without them.").

29. *See* Russell L. Weaver, From Gutenberg to the Internet: Free Speech, Advancing Technology, and the Implications for Democracy 139–58 (2nd ed. 2019).

30. *Id.* at 3. Of course, over the centuries, there were attempts to move information more quickly than people could move. *Id.* at 4. Information could move faster than people could move through the use of carrier pigeons. *Id.* at 4. However, although pigeons could discreetly communicate a particular piece of information relatively quickly, they were not suited to mass communication in the sense of the modern radio, television or internet. *Id.*

31. *Id.* at 9–11.

32. *Id.* at 10–11.

contributed to dramatic societal changes, including the scientific revolution, the demise of monarchy and the Protestant Reformation.[33]

Following Gutenberg's development of the printing press, communication technologies did not advance markedly until the nineteenth century.[34] At that point, the harnessing of electricity led to the development of a series of new electrically-based communication technologies, including the telegraph, radio, television, and eventually satellite and cable technologies.[35] These new technologies allowed information to move much more quickly than the speed at which people could move.[36] The telegraph reduced the time required to send a message across the United States from a matter of weeks to a few seconds.[37] Radio made it possible for President Franklin Delano Roosevelt to transmit his fireside chats to every house in the U.S. almost simultaneously.[38] Television made it possible to communicate through both audio and video content in real time.[39]

Even though these new communication technologies revolutionized communication in important aspects, this technology came with one major drawback: they were almost invariably owned and controlled by relatively rich individuals or corporations who became the "gatekeepers" of those technologies.[40] Even the printing press, which was relatively cheap in comparison to other modern communication technologies (*e.g.*, satellites), could be relatively expensive and difficult to obtain.[41] Benjamin Franklin, who was known as a printer (among many other things), came from a family of limited means and struggled for many years to acquire the funds needed to buy a printing press.[42] He ultimately obtained one only with the help of a partner, and due to the demise of a former employer's printing business that resulted in a fire sale price for a printing press.[43]

Those who controlled communication technologies had the power to decide who could use those technologies, as well as the messages that could be communicated over them.[44] Predictably, the owners of communication platforms would only allow the dissemination of

33. *Id.* at 13–14.
34. *Id.* at 39–46.
35. *Id.*
36. *Id.*
37. *Id.* at 39–40.
38. *Id.* at 47–60.
39. *Id.* at 44–45.
40. *Id.* at 47–60.
41. *Id.* at 33–34.
42. *Id.*
43. *Id.* at 34.
44. *Id.* at 34–38.

information that favored their views and positions.[45] As a result, although there were dramatic advances in communication technologies over the centuries, these new technologies were not readily accessible by ordinary individuals.[46] Ideas and political arguments might or might not be communicated, depending on the whims of those who owned the communication technologies.[47]

The internet was transformative because it was the first technology that allowed ordinary individuals to communicate on a mass scale,[48] and generally allowed them to do so free of the censorship of the traditional gatekeepers and filters on communication.[49] This broadening of communicative capacity had a profound impact on modern societies, enabling mass communication on a scale never seen before, and resulting in significant societal changes.[50] The impact of the internet has been seen in contexts ranging from President Barrack Obama's 2008 presidential campaign, which used the internet very effectively to organize and recruit supporters, and raise money,[51] to the Arab Spring uprisings in the Middle East.[52] The impact has also been seen in a multitude of other contexts.[53]

The greatest strength of the internet—the enabling of mass communication by ordinary individuals—has also proved to be its greatest weakness.[54] By enabling ordinary people to engage in mass communication, the internet has created the potential for mischief. Some have used the internet to perpetrate fraud (haven't we all received emails from Africa soliciting help in moving money out of Africa for a handsome fee?) and has also enabled those who wish to propagate fake news. Using platforms such as Twitter and Facebook, individuals can easily distribute "facts," both real and fake. Moreover, because the internet is global in nature, individuals have the ability to distribute information across international borders. As a result, during the 2016 presidential election, some believed that Russian operatives attempted to influence the outcome of the election in favor of Donald Trump.[55]

The impact of internet speech is amplified by bots and deep fakes. Bots enable individuals to distribute their ideas broadly, and even give

45. *Id.* at 36.
46. *Id.* at 35–38.
47. *Id.* at 36–37.
48. *Id.* at 67–70.
49. *Id.*
50. *Id.* at 67–114.
51. *Id.* at 102–104.
52. *Id.* at 73–82.
53. *Id.* at 67–114.
54. *Id.* at 139–170.
55. *See* Stephen Budiansky, *The Coming War for Cyberspace*, Wall St. J., July 15–16, 2017, at C5 ("An army of Russia-based human and automated attackers ("robo-trolls") deluged the United States with pro-Trump disinformation . . .").

them the possibility of using bots to create new and additional speech on their behalf. Deep fakes allow individuals to use new technologies to created distorted views showing things that never actually happened.

A. *Possible Responses to Fake News, Bots, and Deep Fakes*

Fake news and deep fakes are inconsistent with the notion of informed self-government because they have the potential to mislead the voting public. At its worst, "fake news" can distort the public debate with ideas or facts that are made up and simply untrue.

Of course, the usual remedy for offensive or false speech is counter speech that attempts to set the record straight and helps inform the public of the truth. Whether this remedy is effective with fake news is unclear. After President Obama was elected President of the United States, there were those who questioned whether he was born in the United States, and thus whether he was eligible to serve as President.[56] While there was plenty of counter-speech, including President Obama's production of a copy of his birth certificate, rumors regarding President Obama's birth status continued to circulate.[57] Accordingly, it is not clear that responsive speech will always set the record straight, nor that the public will accept the truth even if it is made available.

B. *Governmental Regulation of Fake News?*

Should there be more stringent remedies against fake news? For example, should government be entitled to declare that "fake news," being false, is not entitled to constitutional protection? In other words, can it treat fake news like fighting words,[58] child pornography,[59] or obscenity,[60] and thus impose criminal sanctions on those who propagate it? Should government also have the power to impose civil or criminal sanctions on those who circulate fake news, or may it impose licensing restrictions or seek injunctive relief against fake news?

Any attempt to regulate fake news might lead to a number of thorny questions regarding the proper role of government in our constitutional system. Let us begin by assuming that Congress decides to create a new federal agency to regulate fake news, the Federal Truth Commission (Truth Commission). Would we, as a society, feel comfortable giving the Truth Commission the power to determine which ideas and facts are

---

56. *See* Ashley Parker & Steve Eder, *How Trump's 'Birther' Claims Helped to Stir Presidential Bid*, N.Y. Times, July 3, 2016, at A1.

57. *See* Sophie Tatum & Jim Acosta, *Report: Trump Continues to Question Obama's Birth Certificate*, CNN (Nov. 29, 2017), http://www.cnn.com/2017/11/28/politics/donald-trump-barack-obama-birth-certificate-nyt/index.html.

58. *See generally* Chaplinsky v. New Hampshire, 315 U.S. 568 (1942).

59. *See generally* Ferber v. New York, 458 U.S. 747 (1982).

60. *See generally* Miller v. California, 413 U.S. 15 (1973).

"true," and which are "false," and to prosecute those who espouse ideas and facts that the commission regards as completely false? Would we feel comfortable giving the Truth Commission the power to license news, based on its truth or falsity, and the power to seek injunctive relief against false facts and ideas?

If the Truth Commission were given such authority, how would it go about determining what qualifies as "fake news?" In order to qualify as false, must something be "completely false," or could something be regarded as "fake news" simply because it is biased or slanted in favor of one side of a debate? For example, during the Obama Administration, suppose that the Truth Commission had existed, and decided that climate change was a "fact" and that climate change denial was fake news. Could the Truth Commission have criminally prosecuted those who argued that climate change was a hoax? Would the Truth Commission have been free to redefine the truth regarding climate change when Donald Trump came to power? In other words, could the Truth Commission have changed its definition of "truth," dismissed all charges against climate change deniers, and criminally prosecuted those who were arguing that climate change is a real phenomenon? Would we, as a society, feel comfortable giving the government the power to declare that facts like these are undeniably true, and that anyone who dissents can be subject to criminal sanctions?

Of course, the Truth Commission might be given the power to prohibit not only "completely false" ideas or facts, but also to prohibit biased or partially false statements. In other words, the Truth Commission might be given the power to impose the equivalent of the Federal Communication Commission's "fairness doctrine,"[61] but instead extend that doctrine beyond broadcasting to all communications disseminated by newspapers, cable television, the internet and satellite.

If the Truth Commission were given the power to prosecute for bias or lack of "fairness," it could have many players on either side of the political spectrum to prosecute. Those on the left might argue that Fox News and other right-wing commentators should be criminally prosecuted for their allegedly biased views and statements. At the same time, those on the right, who believe that the media has a left-wing bias, might argue for the prosecution of a wide swath of left-wing journalists. Although I would personally find it offensive to prosecute anyone for simply expressing their ideas, no matter how biased or slanted, if I were forced (at gun point on threat of death) to name a news personality who exhibits extreme bias and lack of objectivity, I would name a particular National Public Radio program host whose work I often find is

61. *See* Red Lion Broad. Co. v. Fed. Commc'ns Comm'n, 395 U.S. 367, 369 (1969) (holding that the "Fairness Doctrine" required that broadcasters' discussion of public issues give fair coverage to both sides of those issues).

unreasonably partisan. Would the Federal Truth Commission be free to criminally prosecute the NPR host for biased news coverage? Would the host have a defense if there is *some truth* to his statements of fact and articulated ideas? In other words, could he only be convicted if his allegations and reporting are totally false?

A more difficult question arises if government is given the power to prosecute ideas which have elements of truth: but which can be regarded as biased or slanted? Vested with that kind of authority, I'm sure that the Trump Administration would be able to find several biased journalists to prosecute. Would we feel comfortable giving Trump that authority?

Of course, some nations have already attempted to declare truth and criminally prosecute those who transgress their versions of truth. For example, France currently makes it a crime to deny that the Holocaust occurred.[62] However, it is not clear that such crimes provide effective deterrents. There is no evidence that France's ban on Holocaust denial has eliminated Holocaust deniers from France.[63] On the contrary, France is still home to Holocaust deniers.[64] Moreover, despite the U.S.'s failure to prohibit Holocaust denial, there is no evidence that Holocaust deniers have won the day in the United States.

Any attempt to establish a Truth Commission and to allow prosecution of political and news commentators for false statements would run directly counter to the nation's free speech traditions. In *United States v. Alvarez*,[65] the Court struck down portions of the Stolen Valor Act and concluded that Congress could not impose criminal sanctions on those who falsely claim to have won the Congressional Medal of Honor. In *Alvarez*, the Court flatly rejected the proposition that false speech has no value, and therefore should be denied constitutional protection.[66] In doing so, the Court expressed concern that the government might try to create something like the Truth Commission (referencing George Orwell's Oceania Ministry of Truth), and empower it with the authority to "compile a list of subjects about which false statements are punishable."[67] The Court referred to this type of power as being a "broad censorial power," which the Court viewed as "unprecedented in this Court's cases or in our constitutional tradition," and one which involves "a chill the

62. *See* Russell L. Weaver, N. Delpierre & L. Boissier, *Holocause Denial and Governmentally Declared "Truth": French and American Perspectives*, 41 TEX. TECH. L. REV. 495, 497 (2009).

63. *Id.* at 498.

64. *Id.*

65. *See generally* United States v. Alvarez, 567 U.S. 709 (2012).

66. *Id.* at 718–19. The Court did note that certain types of false speech could be criminally prosecuted such as perjury or filing a false claim with the U.S. government. *See id.* at 734.

67. *Id.* at 723.

First Amendment cannot permit if free speech, thought, and discourse are to remain a foundation of our freedom."[68]

Alvarez is consistent with the Court's general free speech jurisprudence. If the legitimacy of our governmental system depends on the consent of the governed, it is inappropriate to give government the power to control, limit and suppress the range of ideas that the people can hear or consider. In *Ashcroft v. American Civil Liberties Union*,[69] the Court declared that as "a general matter, the First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content."[70] Likewise, in *Cohen v. California*, the Court flatly recognized that the "constitutional right of free expression is powerful medicine in a society as diverse and populous as ours," and concluded that it "is designed and intended to remove governmental restraints from the arena of public discussion, putting the decision as to what views shall be voiced largely into the hands of each of us, in the hope that use of such freedom will ultimately produce a more capable citizenry and more perfect polity and in the belief that no other approach would comport with the premise of individual dignity and choice upon which our political system rests."[71] *Cohen* went on to state that it would not "indulge the facile assumption that one can forbid particular words without also running a substantial risk of suppressing ideas in the process. Indeed, governments might soon seize upon the censorship of particular words as a convenient guise for banning the expression of unpopular views. We have been able . . . to discern little social benefit that might result from running the risk of opening the door to such grave results."[72]

Limitations on government's ability to control or censor speech are grounded in history and in our constitutional tradition. After Johannes Gutenberg invented the printing press in the fifteenth century, many countries feared that widespread use of the press might undermine their power, and therefore they sought to control and limit its use.[73] The English government used the decision in *de Libellis Famosis*,[74] to criminally prosecute those who criticized the Crown or certain religious officials of high station, and it did so in an effort to prosecute, intimidate

68. *Id.*

69. Ashcroft v. ACLU, 535 U.S. 564, 573 (2002).

70. *See Alvarez*, 567 U.S. at 717 (citing *Ashcroft*, 535 U.S. at 573); *see also* Brown v. Entm't Merchs. Ass'n, 564 U.S. 786, 790–91 (2011).

71. Cohen v. California, 403 U.S. 15, 24 (1971).

72. *Id.* at 26.

73. *See* Weaver & Hancock, *supra* note 9, at 5.

74. *See generally* De Libellis Famosis Case, 77 Eng. Rep. 250 (Star Chamber 1606).

and silence governmental critics.[75] Moreover, under English law, a defendant could not rely on the defense of truth; indeed, truth was treated as an aggravating factor. "Since maintaining a proper regard for government was the goal of this new offense, it followed that truth was just as reprehensible as falsehood and was eliminated as a defense."[76]

Similar restrictions were imposed in the American colonies where the British prosecuted "criticism directed against the government or public officials" because it was considered to be "a threat against public order and a criminal offense," and again truth was not a defense.[77] For example, British colonial officials prosecuted John Peter Zenger, a New York publisher, for seditious libel for publishing stories mocking the royal Governor and his administration.[78] Among other things, Zenger published "anti-British song-sheets and mock advertisements describing an associate of the royal governor as 'a large Spaniel, of about 5 feet 5 inches high . . . lately strayed from his kennel with his mouth full of fulsome panegyricks,' and a 'monkey . . . lately broke from his chain and run into the country.'"[79] The Royal Governor eventually managed to indict Zenger for seditious libel.[80] When the case was finally tried, Zenger's lawyer admitted that Zenger had published the allegedly libelous statements, and offered to concede the libel if the prosecution could prove that the allegations were false. When the prosecution declined, Zenger's attorney offered to prove that the statements were true. Although the court disallowed the evidence, on the valid legal basis that truth was immaterial, the jury chose to acquit Zenger in a decision that history has portrayed as an early example of jury nullification.[81]

Based on this history of speech repression, some commentators have argued that the First Amendment was designed to eliminate seditious libel, and to provide broad protections for freedom of expression. For example, Zechariah Chafee argued that the Framers of the First Amendment intended to "wipe out the common law of sedition, and make further prosecutions for criticism of the government, without any incitement to law-breaking, forever impossible."[82] Although Leonard W. Levy disputed the idea that the First Amendment was intended "to

---

75. *Id. See also* William T. Mayton, *Seditious Libel and the Lost Guarantee of a Freedom of Expression*, 84 Colum. L. Rev. 91, 103 (1984).

76. *Id.*

77. Lawrence W. Crispo, Jill M. Slansky & Geanene M. Yriarte, *Jury Nullification: Law Versus Anarchy*, 31 Loy. L.A. L. Rev. 1, 7 (1997).

78. *Id.*

79. Elizabeth I. Haynes, *United States v. Thomas: Pulling the Jury Apart*, 30 CONN. L. REV. 731, 744–45 (1998).

80. *See* Cohen v. Hurley, 366 U.S. 117, 140 (1961) (Black, J., dissenting).

81. *See* Haynes, *supra* note 79, at 7–8.

82. Zechariah Chafee Jr., Free Speech In The United States 21 (Harvard Univ. Press 1941).

eliminate the law of seditious libel,"[83] he agreed that the "American people of 1787 understood . . . that they were entitled to an explicit reservation of their rights against government, that a bill of rights is a bill of restraints upon government, and that people may be free only if the government is not."[84]

Early experiences under the U.S. Constitution were not necessarily consistent with this anti-repression principle. Less than a decade after the First Amendment was framed and ratified, Congress enacted the Alien and Sedition Act of 1798, which made it illegal to publish "false, scandalous, and malicious writing against the Government of the United States with intent to defame, or to bring them into contempt or disrepute, or to excite against them hatred of the good people of the United States, or to stir up sedition within the United States."[85]

In its more modern decisions, the Court has been sensitive to the history of speech repression in both the U.S. and Europe, and quite protective when the government seeks to repress core political speech. In general, the Court's decisions have suggested that the government should not be allowed to control either thought or speech. As the Court stated in *Ashcroft v. Free Speech Coalition*, "First Amendment freedoms are most in danger when the government seeks to control thought or to justify its laws for that impermissible end.[86] The right to think is the beginning of freedom, and speech must be protected from the government because speech is the beginning of thought." Likewise, in *Virginia v. Black*, the Court stated that the "hallmark of the protection of free speech is to allow free trade in ideas—even ideas that the overwhelming majority of people might find distasteful or discomforting."[87] This point has been made in many different ways. For example, Professor Emerson argued that the "only justification for suppressing an opinion is that those who seek to suppress it are infallible in their judgment of the truth. But no individual or group can be infallible, particularly in a constantly changing world."[88] As a result, "through the acquisition of new knowledge, the toleration of new ideas, the testing of opinion in open competition, the discipline of rethinking its assumptions, a society will be better able to reach common decisions that will meet the needs and aspirations of its members."[89]

However, there is one situation in which fake news can be prohibited, as well as bots and deep fakes: when the speech comes from outside the

83. Leonard W. Levy, *The Legacy Reexamined*, 37 Stan. L. Rev. 767, 767 (1985).
84. *Id.* at 773.
85. 1 Stat. 596 (1798). *See also* 1 Stat. 570, 577 (1798).
86. Ashcroft v. Free Speech Coalition, 535 U.S. 234, 253 (2002).
87. Virginia v. Black, 538 U.S. 343, 358 (2003).
88. Emerson, *supra* note 9, at 882.
89. *Id.*

U.S. and is designed to interfere in U.S. elections. Federal law prohibits such interference.

C. *Injunctions and Licensing as Possible Remedies?*

An alternate (or, perhaps, supplementary) approach is to give the Truth Commission two other powers: (1) to review and license new stories before they are published, and (2) to seek injunctive relief against fake, biased or slanted news. Under such an arrangement, the Truth Commission could require that all facts and all new stories be submitted to it prior to publication, and the law could further provide that nobody could publish anything without the explicit authority of the Truth Commission. The Truth Commission would then have the power to refuse to license any story that it regards as false. Alternatively, if someone published facts or stories without gaining the Truth Commission's approval, it could be given the authority to seek injunctive relief against the publication of such stories. They could also seek injunctive relief against biased or "unfair" news or ideas.

Of course, both a licensing power and an injunctive power would run directly counter to the long-established prohibition against prior restraints.[90] In the Court's landmark decision in *Near v. Minnesota*, the Court emphasized that the constitutional protection for liberty of the press was designed to prohibit "previous restraints upon publication."[91] Likewise, in *Patterson v. Colorado*, the Court declared that the "main purpose" of the First Amendment's provisions is "to prevent all such previous restraints upon publications as had been practiced by other governments."[92]

The prohibition against prior restraints is also rooted in history. After Johannes Gutenberg invented the printing press, many countries sought to control and limit its use.[93] In addition to restricting the number of printing presses that could exist, England imposed content licensing restrictions.[94] In other words, before an individual could publish a book or document, the government required the individual to submit the content of the book to governmental censors, who could veto the publication or require modifications to the content (usually modifications designed to mute or eliminate criticism of the King or the clergy).[95] In

90. *See generally* New York Times Co. v. United States, 403 U.S. 713 (1971); Lovell v. City of Griffin, 303 U.S. 444 (1938); Near v. Minnesota, 283 U.S. 697 (1931).

91. *Near*, 283 U.S. at 713.

92. Patterson v. Colorado, 205 U.S. 454, 462 (1907).

93. *See* Weaver & Hancock, *supra* note 9, at 5–6.

94. *Id.* at 5–6.

95. *Id.* at 6; *see also* Times Film Corp. v. City of Chicago, 365 U.S. 43, 55–56 (1961) (Warren, C.J., dissenting).

general, in the U.S., such speech licensing schemes are prohibited. In *Lovell v. City of Griffin*,[96] the Court struck down an ordinance which required that the written permission of the city manager must be obtained before anyone could distribute circulars, advertising, or literature of any kind in the City of Griffin. In doing so, the Court emphasized that the law stuck "at the very foundation of the freedom of press by subjecting it to license and censorship."[97] Noting that the "struggle for the freedom of the press was primarily directed against the power of the licensor," the Court held the ordinance was invalid because it "would restore the system of license and censorship in its baldest form."[98]

The Court has also denied injunctions against speech.[99] In *Near v. Minnesota*, the Court struck down a Minnesota law which authorized the abatement of any "malicious, scandalous and defamatory newspaper, magazine or other periodical."[100] The case involved an attempt to enjoin publication of *The Saturday Post* because it was "largely devoted to malicious, scandalous and defamatory articles."[101] Reaffirming the prohibition against prior restraints, the Court held that the Minnesota law imposed "an unconstitutional restraint upon publication."[102]

Thus, it is extremely unlikely that the Truth Commission could impose a licensing scheme, requiring that publishers obtain its permission before publishing information, or that it could use injunctions to prohibit the publication of "fake news."

D. *Other Potential Remedies?*

If Congress cannot vest the Truth Commission with the power to criminally prosecute or enjoin the publication of fake news, then are there other potential remedies for fake news or against the perpetrators of such news?

In appropriate cases, one potential remedy is to bring a defamation suit against someone who propagates fake news that injures another's reputation. As discussed previously, if the plaintiff is a public official or a public figure, it is extremely difficult to prevail in defamation litigation. However, if an allegation really does involve "fake news," in the sense that the defendant is "making it up," it should be possible for even a public official or a public figure to satisfy the more stringent actual malice

96. Lovell v. City of Griffin, 303 U.S. 444, 451 (1938).

97. *Id.*

98. *Id.* at 451–52; *see also* City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750 (1988).

99. *See* Madsen v. Women's Health Center, Inc., 512 U.S. 753 (1994); New York Times Co. v. U.S., 403 U.S. 713 (1971); Near v. State of Minnesota ex rel. Olson, 283 U.S. 697 (1931).

100. Near v. Minnesota, 283 U.S. 697, 701–02 (1931).

101. *Id.* at 703.

102. *Id.* at 723.

standard imposed under *New York Times Co. v. Sullivan*. But the effectiveness of this remedy is undercut by the nature of the internet. Fake information can be disseminated from all parts of the globe. Even if a potential plaintiff could locate the purveyor of false information, which might be difficult since it is often conveyed anonymously, the purveyor may be judgment proof. At the very least, the plaintiff may be forced to sue in a foreign country in order to obtain jurisdiction over the defendant. All things considered, a defamation suit might not be worth the trouble.

Another potential remedy may be responsive speech. Certainly, the government could at times weigh in with its own version of truth. To a greater or lesser extent, government has always engaged in attempts to influence public opinion. For example, the Obama Administration argued in favor of its view of climate change, and the Trump Administration has adopted its own (contrary) view of climate change. Likewise, even though Holocaust deniers cannot be prosecuted in the U.S., the government has not remained neutral on the question of whether the Holocaust actually occurred. Indeed, it helped establish the Holocaust Memorial Museum. Of course, many people are distrustful of government, particularly the U.S. government, and it is not clear whether the American people would be inclined to accept the declarations of a Truth Commission as the true and last word on any issue.

E. Third Party Remedies

Given the decline of the traditional media, and the rise of the internet, much speech now runs through private entities such as Twitter and Facebook.[103] In recent years, these private entities have tended to assert much greater control over the speech that occurs on their networks.[104] This trend can be regarded as positive in that private entities may be making much greater efforts to control fake news and other harmful speech.[105] However, the trend can also be troubling in the sense that private companies are serving as gatekeepers, as they are attempting to censor and control the flow of ideas to the public.[106]

Governmental regulation of private networks would have troubling First Amendment implications. For example, suppose that the Truth Commission sought to prohibit private networks (such as Twitter or Facebook) from transmitting fake information. Could the private networks be criminally prosecuted when fake news is aired through their

---

103. *See* Rachel Martin, *Ex-Head Of Twitter News: Social Media Companies Alone Shouldn't Regulate 'Fake News*,' Nat'l Pub. Radio: Weekend Edition Sunday (Nov. 20, 2016), https://www.npr.org/2016/11/20/502770866/ex-head-of-twitter-news-social-media-companies-alone-shouldn-t-regulate-fake-new.

104. *Id.*

105. *Id.*

106. *Id.*

systems? Alternatively, could they be subject to content licensing or injunctions in order to prevent them from transmitting fake news? Presumably, any attempt by the Truth Commission to act against private networks would run afoul of the same constitutional restrictions that would arise if the Truth Commission tried to act against private individuals.

One potential restriction on private networks might be valid: a disclosure requirement. During the 2016 presidential campaign, concerns were expressed regarding the fact that foreign entities (allegedly, the Russian government) were trying to influence the outcome of the U.S. election through such devices as fake advertisements run on Facebook.[107] There has been some talk of requiring companies like Facebook to reveal the sources of their advertisements.[108] If that were done, it would at least be more apparent when outsiders are trying to influence a U.S. election.

As private entities, social media networks can exercise a higher degree of editorial control than the government can exercise.[109] However, for a variety of reasons, their attempts to exercise such control can be troubling. Those who operate social media platforms may have ideological or political biases, and may use their censorial power to favor information that accords with their view and biases.[110] In addition, so much "fake news" is distributed over social media platforms that the reviewers are overwhelmed and have very little time to fairly evaluate information before censoring it.[111]

CONCLUSION

Democratic government is premised upon the consent of the governed, and freedom of expression is essential to the effective expression of that consent. Attempts to undermine freedom of expression, through the injection of fake or false news into the public debate, is particularly troubling in democratic systems because it tends to undermine the quality of the public debate.

The difficulty is that there are no effective legal solutions to the dissemination of fake news. In the U.S., it will typically be highly offensive for the government to criminally prosecute those who

---

107. *See* Aarti Shahani, *Facebook's Advertising Tools Complicate Efforts To Stop Russian Interference*, Nat'l Pub. Radio: All Things Considered (Oct. 30, 2017), https://www.npr.org/sections/alltechconsidered/2017/10/30/560836775/facebooks-advertising-tools-complicate-efforts-to-stop-russian-interference.

108. *Id.*

109. *See* Russell L. Weaver, *Social Media Platforms and Democratic Discourse*, 23 Lewis & Clark L. Rev. 1385, 1406 (2020).

110. *Id.* at 1408–09.

111. *Id.*

propagate false information, and injunctions would be regarded as anathema as a prior restraint on publication.

In the final analysis, James Madison's lament regarding the press remains as true today as it was then: "That this liberty [press liberty] is often carried to excess; that it has sometimes degenerated into licentiousness, is seen and lamented, but the remedy has not yet been discovered. Perhaps it is an evil inseparable from the good with which it is allied; perhaps it is a shoot which cannot be stripped from the stalk without wounding vitally the plant from which it is torn."[112] Similar principles apply to governmental regulation of fake news: the remedy may be worse than the disease. In the U.S. system, the only potentially effective response to fake news is responsive speech that points out the defects and lies inherent in that speech.

112. James Madison, *Address of the General Assembly to the People of the Commonwealth of Virginia*, *in* 6 The Writings of James Madison 332, 336 (Gaillard Hunt ed., 1906) (emphasis omitted); *see also* Near v. Minnesota, 283 U.S. 697, 718 (1931) ("Some degree of abuse is inseparable from the proper use of everything, and in no instance is this more true than in that of the press. It has accordingly been decided by the practice of the States, that it is better to leave a few of its noxious branches to their luxuriant growth, than, by pruning them away, to injure the vigor of those yielding the proper fruits. And can the wisdom of this policy be doubted by any who reflect that to the press alone, chequered as it is with abuses, the world is indebted for all the triumphs which have been gained by reason and humanity over error and oppression; who reflect that to the same beneficent source the United States owe much of the lights which conducted them to the ranks of a free and independent nation, and which have improved their political system into a shape so auspicious to their happiness?").

THE DATA BREACH EPIDEMIC: A MODERN LEGAL ANALYSIS

Laura A. Hendee[*]

Abstract

This Note sheds light on the major legal issues surrounding the numerous data breaches that plague our modern technology-driven society. Current laws in the United States vary widely in how they handle the resolution of harm to unsuspecting victims of data breaches. The issue of Article III standing is commonly at the forefront of the conflict and discussion in this area, which has resulted in a substantial circuit split in the United States. The newly enacted California Consumer Privacy Act will likely have a major impact in this area of the law and will undoubtedly influence how consumers' personal information is handled in the years to come.

* LL.M. Taxation Candidate, New York University School of Law (2021); J.D., University of Florida Levin College of Law (2020); M.S.T., University of Miami (2016); B.S.B.A. Accounting, University of Miami (2016).

INTRODUCTION

It seems like every day there is a new article headline in the news or new email in your inbox stating something to the effect of, "Company X Announces New Data Breach," or the even more alarming, "We found your information in another company's data breach." In reality, it does not just seem like it: on average, there *are* new company data breaches every day.[1] In fact, Privacy Rights Clearinghouse reports that there have been over 9,600 data breaches since 2005, exposing over 11,500,000,000 personal records.[2] These are disturbing statistics, and as the variety of industries and types of businesses impacted by breaches each year continue to increase, many consumers are beginning to realize that such breaches have become "the new normal."[3] The question is not "if" a breach will occur, but "when" a breach will occur.[4]

A "data breach" is defined as "a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion."[5] They can be caused by many things, including but not limited to weak passwords, missing software patches that are exploited, lost or stolen electronic devices, unauthorized exposure during information transit, hackers exploiting unsecured wireless networks, and social engineering (i.e., email phishing).[6] With so many data breaches occurring each year, several of them large in terms of the number of impacted individuals and the volume of data acquired, it follows that a number of those individuals are taking action.[7] Such data breaches frequently make headlines and provoke litigation brought by

---

1. *See* Davey Winder, *Data Breaches Expose 4.1 Billion Records in First Six Months of 2019*, FORBES (Aug. 20, 2019, 6:31 AM), https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/. *See also* Daniel Funke, *By the Numbers: How Common Are Data Breaches—and What Can You Do About Them?*, POLITIFACT (Sept. 23, 2019), https://www.politifact.com/article/2019/sep/23/numbers-how-common-are-data-breaches-and-what-can-/.

2. *See* Daniel Funke, *supra* note 1.

3. *See* IDENTITY THEFT RES. CTR., 2018 END-OF-YEAR DATA BREACH REPORT (Jan. 28, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

4. *Id.*

5. Margaret Rouse, *Essential Guide: GDPR Compliance Requirements for CRM Managers—Definition: Data Breach*, SEARCHSECURITY, (last updated May 2019) https://searchsecurity.techtarget.com/definition/data-breach.

6. *Id.*

7. *See* David Balser et al., *Insight: Data Breach Litigation Trends to Watch*, BLOOMBERG L. (Mar. 4, 2019, 4:01 AM), https://news.bloomberglaw.com/privacy-and-data-security/insight-data-breach-litigation-trends-to-watch.

consumers, often leading to large class action lawsuits.[8] After the passage of the Class Action Fairness Act,[9] most data breach lawsuits have been brought in federal court.[10] Because of the lack of clarity provided by courts and legislatures in the area of data privacy litigation, some of the most noteworthy data breach litigation developments in 2018 resulted in large consumer class action settlements.[11] This settlement trend will likely continue unless further guidance is provided or a more clearly defined legal standard develops surrounding the implementation of reasonable security measures that are effective in the current state of advancing technology and cybersecurity.[12]

One of the major reasons for the lack of clarity regarding data breach litigation outcomes across the country spurs from the circuit split on the issue of standing.[13] Courts dismiss many of these data breach cases because plaintiffs lack a cognizable injury-in-fact, which is a major component for Article III standing.[14] Generally, the First, Second, Fourth, and Eighth Circuits have *rejected* a finding of standing on the particular facts of the cases heard in these circuits, while leaving the door open for future cases, noting that the assessment of risk of future harm is a fact-specific inquiry.[15] Conversely, the Third, Seventh, Ninth, and D.C. Circuits have held that, based on the facts of the particular cases, the risk of future harm from a data breach *was* an injury sufficient for standing.[16] The split regarding the existence of a cognizable injury centers around the risk of future identity theft, risk of future fraud, monitoring expenditures, and other similar costs.[17] Moreover, the Supreme Court has turned down the opportunity to opine on this subject, further solidifying the circuit split.[18]

---

8. *Id.*

9. 28 U.S.C. § 1332(d) (2011) (extending federal diversity jurisdiction to all class actions in which minimal diversity exists and the amount in controversy exceeds $5 million).

10. Megan Dowty, *Life is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 686 (2017).

11. *See* Balser et al., *supra* note 7.

12. *See* Balser et al., *supra* note 7.

13. David L. Silverman, *Developments in Data Security Breach Liability*, 74 BUS. L. 217, 217 (2018).

14. Dowty, *supra* note 10, at 686.

15. *See* Silverman, *supra* note 13; *see infra* Part II (discussing specific relevant cases from each circuit in the circuit split).

16. *See* sources cited *supra* note 15.

17. Dowty, *supra* note 10, at 686–87.

18. *See, e.g.*, Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018).

Some states, such as California, are passing stricter consumer privacy laws that will likely impact the future of data privacy litigation in those particular jurisdictions.[19] There have also been attempts to pass federal legislation that would potentially preempt state laws, but so far none of those attempts have succeeded.[20] Despite this lack of a clearly defined national standard, companies need to start employing techniques that will reduce their litigation exposure. Some options for accomplishing this include the implementation of a minimum level of security controls[21] and careful drafting of arbitration clauses and class action waivers[22] in the company's terms and conditions.

I. DATA BREACHES, IMPACT OF INFORMATION THEFT & CURRENT GOVERNING LAW

A. *Data Breaches: Prevalence Today & Resulting Costs to Victims*

As data breaches and hacks continue to occur, the privacy of our personal information remains constantly at risk, even if we believe the companies that we share our data with are trustworthy and technologically adept. Hackers continue to improve their skills and find new unpredictable methods of using technology to procure personal information from companies and individuals.[23] Unfortunately, the rate of technological development by these hackers seems to consistently outpace the policy makers in this area. This contributes to the general tensions on the subject and begs the question of why there has been so little progress in preventing data breaches and the thefts that often follow.[24] For example, in the last five years alone there have been several major corporate data breaches involving companies such as Target, Yahoo!, Home Depot, Sony Pictures and Entertainment, Anthem Health

19. *See generally* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2018).

20. *See* Stephen Jones, *Data Breaches, Bitcoin, and Blockchain Technology: A Modern Approach to the Data-Security Crisis*, 50 TEX. TECH. L. REV. 783, 793–94 (2018).

21. *See* KAMALA D. HARRIS, CAL. DEP'T OF JUST., CALIFORNIA DATA BREACH REPORT 31 (Feb. 2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

22. *See* Alexis Buese, *Calif. Privacy Law Will Likely Prompt Flood of Class Actions*, LAW360 (May 15, 2019, 11:41 AM), https://www.law360.com/articles/1159313/calif-privacy-law-will-likely-prompt-flood-of-class-actions.

23. *See* Jon L. Mills & Kelsey Harclerode, *Privacy, Mass Intrusion, and the Modern Data Breach*, 69 FLA. L. REV. 771, 773 (2017).

24. *Id.* at 773.

Insurance, HSBC Finance Corporation, Ashley Madison, and Equifax, just to name a few.[25]

Data breaches impact both the consumers whose records are exposed and the companies whose lack of appropriate security measures lead to the particular breach. The companies who are hacked, and ultimately leak such consumer information, are exposed to great financial harm.[26] The average cost to businesses per leaked record is reported at $150,[27] and the global cost of data breaches is estimated to increase to $2.1 trillion[28] by the end of 2019. These figures have consistently increased since 2017 and this trend may continue.[29] Further, customers with compromised credit card information or other personal data because of a data breach are often reluctant to do business with the same company, thus severing the relationship and resulting in the loss of a customer's lifetime value for the business.[30]

Repercussions on the consumer side typically center around the risk of future identity theft or fraud and the corresponding identity theft monitoring expenses, temporary account cancellations, and generalized stress and anxiety post-breach.[31] This is especially concerning given the general population's dependence on the Internet and will likely have the greatest impact on future generations. Future generations are at risk of serious identity theft issues that may occur when these individuals are still very young, which in turn may potentially impact their future ability to obtain loans or purchase homes, cars, and other valuable assets later in life that require an inquiry into credit scores.[32] All parties to a data breach suffer to some degree, and it is up to the policy-makers of the country to ultimately combat these issues by passing effective standards that will help protect future individuals from becoming victims of such harmful actions.

---

25. *Id.* at 780–83.

26. *See* Jones, *supra* note 20, at 789.

27. IBM SECURITY, COST OF A DATA BREACH REPORT 13 (2019), https://www.ibm.com/downloads/cas/ZBZLY7KL.

28. Shayla Price, *The Real Cost of Ecommerce Data Breaches, Espionage, and Security Mismanagement*, BIGCOMMERCE: ECOMMERCE SECURITY BLOG, https://www.bigcommerce.com/blog/data-breaches/#the-costs-of-a-data-breach (last visited Apr. 2, 2020).

29. IBM SECURITY, *supra* note 27, at 19.

30. *See* Price, *supra* note 28.

31. *See* Jones, *supra* note 20, at 788; Dowty, *supra* note 10, at 686; Price, *supra* note 28.

32. Jones, *supra* note 20, at 788–89; *see also* Danielle Wiener-Bronner, *Why Millennials Should be Really Worried about the Equifax Breach*, CNN MONEY (Sept. 15, 2017, 4:21 PM), https://money.cnn.com/2017/09/15/pf/millennials-equifax-breach/index.html.

B. *Impact of Information Theft: The Hacker's Timeline*

So, what actually happens after consumer personal information is stolen in a company's data breach? Hackers use the information in a variety of ways. They may: (1) use the stolen information to interfere with business operations, for example, hackers commonly sell internal business plans, forecasts, and market analyses to competitors; (2) steal data for the purposes of extortion, for example, ransomware attacks where the hacker demands payment if the company wants to unlock the stolen or restricted files; or (3) target consumer data like names, addresses, phone numbers, email addresses, passwords, credit card numbers, and social security numbers to leverage such information for financial gain on the dark web, which often results in identity theft that is sold to the highest bidder.[33] Of further concern, identity thieves often exploit stolen information within minutes of obtaining it.[34]

The Federal Trade Commission's Office of Technology Research & Investigation (FTC's Tech. Office) performed an experiment in 2017 to discover what actually happens when stolen personal information is made public and how quickly thieves attempt to make unauthorized use of the information.[35] The FTC's Tech. Office created personal information belonging to 100 fake people that was designed to look like a stolen database of consumer credentials and posted that information on a site frequented by hackers on two occasions.[36] For two weeks after they posted to the site, the FTC's Tech. Office monitored "all email access attempts, payment account access attempts, attempted credit card charges, and texts and calls received by phone numbers."[37] The first posting of information received about 100 views, and the second posting received about 550 views.[38] After the initial posting, it only took 90 minutes for the first unauthorized attempt to use the stolen fake information; then, after the second posting, it only took nine minutes.[39] Furthermore, the total number of attempts to use the information totaled

33. *See* Price, *supra* note 28.

34. *See* Lesley Fair, *Sensitive Consumer Data Posted Online (and the FTC Knows Who Did It)*, FEDERAL TRADE COMMISSION: BUS. BLOG (May 24, 2017, 10:30 AM), https://www.ftc.gov/news-events/blogs/business-blog/2017/05/sensitive-consumer-data-posted-online-ftc-knows-who-did-it.

35. *Id.*

36. *Id.*

37. *Id.*

38. *Id.*

39. *Id.*

119 in the first week and 1,108 in the second week.[40] Tracking of attempted illegal purchases over the two weeks lead to a variety of categories of charges, with the top five including: (1) retailers; (2) unknown; (3) gaming; (4) entertainment; and (5) e-payment services.[41]

The experiment revealed how incredibly fast large amounts of stolen personal information can spread across the dark web. The above experiment only used the data of 100 hypothetical victims of information theft and only tracked the impact for two weeks following the posting of the information. For a startling perspective, the Equifax data breach exposed personal information of approximately *147 million* individuals and that breach occurred two years ago in 2017.[42] The number of attempts of unauthorized use of such information from that one data breach alone is likely massive and will undoubtedly have a negative impact on the lives of those *real* breach victims.

C. *Current Data Breach Laws in the United States*

Federal data breach regulations are limited in their scope and apply almost exclusively to industries such as banking, finance, healthcare, and credit reporting.[43] Such statutes typically mandate that companies in each industry implement reasonable procedures to protect consumer information from prohibited disclosure.[44] Though this seems like a regulation that would result in something positive, it lacks any explanation or examples of what would qualify as "reasonable procedures" and it lacks guidance on how companies should assess their vulnerability for future data breaches.[45] The ambiguity of these federal statutes creates confusion and reinforces the wide array of security standards used nationwide, which are often effective.

If consumers recognize that they are victims of such statutory violations under the industry-specific federal law and bring a complaint against a company, they usually face an additional hurdle when arguing for federal standing and the interpretation of the injury requirement.[46] The

---

40. *Id.*

41. *Id.*

42. Lesley Fair, *$575 Million Equifax Settlement Illustrates Security Basics for Your Business*, FED. TRADE COMMISSION: BUS. BLOG (July 22, 2019, 6:48 AM), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/575-million-equifax-settlement-illustrates-security-basics.

43. Jones, *supra* note 20, at 792.

44. *See* Jones, *supra* note 20, at 792.

45. *See* Jones, *supra* note 20, at 792. *See also* 15 U.S.C. § 1681e(a).

46. *See infra* Section II.A.

Supreme Court of the United States has arrived at conflicting conclusions in regard to what actually satisfies this requirement, which has resulted in a federal circuit split.[47] Inevitably this adds to the outcome uncertainty for both plaintiffs and defendants, and since companies typically settle their disputes out of court,[48] courts have not been able to give opinions regarding their judgment on the merits of these claims. Notably, this impacts future litigation because the judicial system has not yet had the opportunity to interpret the meaning of what "reasonable procedures" should be in place to satisfy what is mandated by the federal statutes for protection of consumer personal information.

Every state (plus the District of Columbia and a number of United States Territories) has enacted legislation requiring entities to notify victims of security breaches that release personally identifiable information.[49] Each state's laws on security breaches usually set forth who must comply with the law, a definition of what constitutes "personally identifiable information" (which, surprisingly, varies state to state), what constitutes a breach, timing and appropriate method of notice, and certain exemptions.[50] Companies involved in a data breach are expected to comply with the various data-related statutes for each state where they do business.[51] However, the large range of varying regulations in this area, coupled with the added confusion related to standing present a burden for both the breached companies and the consumers seeking relief.[52]

Though data breach laws at the state level vary, they typically share the exception that notification is only required when compromised data was not encrypted (or when the encryption key was also compromised in the breach).[53] A number of state statutes require companies that collect consumer personal information to implement "reasonable procedures" to

47. Jones, *supra* note 20, at 794–95; *see* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 440–41 (2013) (suggesting a high burden of proof to meet the "certainly impeding" harm requirement); Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016) (holding that though the plaintiff alleged a federal statutory violation by the defendant, a concrete injury must also be shown); *see also infra* Section II.A.

48. *See* Jones, *supra* note 20, at 793.

49. *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Sept. 29, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/ security-breach-notification-laws.aspx [hereinafter NCSL].

50. *Id.*

51. Jones, *supra* note 20, at 791–92; *see generally* NCSL, *supra* note 49 (showing the varying statutes related to this subject for each state).

52. *See* Jones, *supra* note 20, at 792.

53. Jones, *supra* note 20, at 796.

protect the information.[54] However, similar to the federal statutes that require such "reasonable procedures," the state laws do not provide any guidance regarding the types of procedures considered reasonable and they also do not shed light on how companies should assess their vulnerability for future data breaches.[55] And the most notable differences across the state statutes are how broad or narrow they define "personal information," whether they provide consumers with an express cause of action, the severity of the penalties for violations, and the range of time that breached companies have to notify consumers and regulatory agencies of the breach.[56]

The state of Florida's data and personal information protection statutes are typical examples of what any state statutes may look like in this area. These data breach laws apply to any entity that acquires, maintains, stores, or uses personal information.[57] Entities are required to take "reasonable measures" to protect and secure data in electronic form containing personal information.[58] The statute defines "breach of security" or "breach" as unauthorized access of data in electronic form containing personal information, with an exception for certain situations where information is accessed in good faith by employees or agents.[59] It does not apply to encrypted or redacted information, or information secured in some other way that renders it unreadable (as long as the encryption key is not also compromised).[60] Within the statute "personal information" is defined as an individual's first and last name or first initial and last name plus one or more of the following: Social Security number, driver's license or passport number, military identification number, any similar form of government identification number that can be used to verify the individual's identity, financial account number or credit or debit card number with any security codes required, medical information, or health insurance policies or subscriber identification numbers.[61] Additionally, personal information may also include a username or e-mail address, in combination with a password or security question and answer

54. Jones, *supra* note 20, at 796–97.

55. Jones, *supra* note 20, at 797.

56. Jones, *supra* note 20, at 796–97.

57. FLA. STAT. § 501.171(1)(b) (2019).

58. *Id.* § 501.171(2). The vague "reasonable measures" language, *id.*, provides little guidance to businesses for best prevention practices.

59. *Id.* § 501.171(1)(a).

60. *Id.* § 501.171(1)(g)(2).

61. *Id.* § 501.171(1)(g)(1)(a).

that would permit access to an online account.[62] Florida's statute does not provide a private cause of action.[63]

Florida's notification requirement varies depending on whether the breached entity is notifying an individual or a regulatory agency.[64] For individuals, notifications must be given in writing to each individual in the state whose personal information was, or if the entity reasonably believes it was, accessed as a result of the breach.[65] The notice shall be made "as expeditiously as practicable and without unreasonable delay . . . but no later than 30 days after the determination of the breach or reason to believe the breach occurred" and must include the date(s) of the breach, a description of the personal information accessed or believed to be accessed, and contact information for the breached entity.[66] For regulators, the breached entity must notify the Florida Department of Legal Affairs no later than 30 days following the identification of the breach if 500 or more individuals within the state are affected by the breach.[67] Further, third parties that maintain personal information on behalf of the breached entity must notify that entity no later than 10 days after determination of the breach.[68] Violations of the notice requirement may result in civil penalties and are considered "unfair or deceptive trade practices."[69] The civil penalties may consist of up to $1,000 per day for each day up to the first 30 days following a violation and $50,000 for each subsequent 30-day period or portion thereof for up to 180 days, capping at a ceiling of $500,000.[70] These penalties are per breach, not per affected individual.[71]

The difficulties that both consumers and businesses must overcome from the current data breach regulations on the federal and state levels are clear. Unfortunately, the subsequent path going forward after overcoming those difficulties is not so clear. The following sections of this Article summarize and examine the split among the federal circuit courts, the forthcoming state regulations that will likely have a substantial impact on data protection laws across the country, and the potential

62. *Id.* § 501.171(1)(g)(1)(b).
63. *Id.* § 501.171(10).
64. *Compare* FLA. STAT. § 501.171(3), *with* FLA. STAT. § 501.171(4).
65. *Id.* § 501.171(4)(a), (d).
66. *Id.* § 501.171(4)(a), (e).
67. *Id.* § 501.171(3)(a). Fifteen additional days may be allowed if there is good cause for delay provided in writing to the department within 30 days after determination of the breach or reason to believe a breach occurred. *Id.*
68. *Id.* § 501.171(6)(a).
69. *Id.* § 501.171(9)(a).
70. *Id.* § 501.171(9)(b).
71. *Id.* § 501.171(9).

measures that companies can implement to mitigate their litigation exposure in this area.

II. A SPLIT AMONG THE CIRCUIT COURTS

Data breach cases typically include one or more of three different categories of alleged injuries: (1) the plaintiff's personal or financial information has been stolen by a third party, and that party has used that information illegally (i.e. to make purchases using the plaintiff's money); (2) the plaintiff's information has been accessed but that information has not been used (i.e. to open bank accounts, make unauthorized purchases, or otherwise harm the plaintiff), yet, the plaintiff still claims other forms of damages (i.e. incurring costs for credit-monitoring services, paying the cost of cancelling and receiving new bank bards, suffering loss of reward points from cancelled cards, and experiencing general anxiety that their information will be used in an unauthorized manner in the future); and (3) the plaintiff brings a suit based on a belief that his information is not being protected and a third party could potentially access it in the future.[72] From these above categories of injuries, those in (1) involve an injury sufficient to meet the injury-in-fact requirement, those in (2) are the type of injuries involved in the circuit split that focuses on whether the indirect costs and expenses are sufficient to meet the injury-in-fact requirement, and those in (3) are the least likely to meet the injury-in-fact requirement.[73]

The lack of a uniform standard set by the Supreme Court for what constitutes injury in the context of data breaches has resulted in a circuit split as to how much injury is sufficient for standing purposes. Generally, the First, Second, Fourth, and Eighth Circuits have consistently *rejected* a finding of standing for alleged injury categories (2) and (3) above, while emphasizing that the assessment of risk of future harm is a fact-specific inquiry.[74] Conversely, the Third, Seventh, Ninth, and D.C. Circuits have consistently held that the alleged injury category (2)—risk of future harm from a data breach that has already occurred—*was* an injury sufficient for standing.[75]

---

72. Caroline C. Cease, Note, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395, 398, 399, 404 (2014).

73. *Id.* at 398, 399, 404.

74. Silverman, *supra* note 13, at 217.

75. Silverman, *supra* note 13, at 217.

A. *First Things First: Standing*

1. The "Injury-in-Fact" Requirement

The Constitution establishes Article III standing as a "threshold question in every federal court case."[76] To satisfy this standing requirement, a plaintiff must have suffered an injury that is: (1) concrete, particularized and actual or imminent (as opposed to merely conjectural or hypothetical); (2) fairly traceable to the challenged conduct of the defendant; and (3) likely to be redressed by a favorable ruling.[77] Standing issues for data breach cases usually center around the first requirement—that there is an "injury-in-fact." However, the Supreme Court has not yet directly ruled on this subject in the context of a data breach.

Many data breach cases addressed by lower courts have relied on *Clapper v. Amnesty International USA* for guidance on analyzing the existence of a sufficient injury-in-fact.[78] *Clapper* involved a United States citizen who engaged in sensitive international communications with individuals whom they believed might be the targets of American surveillance at some point in the future under the 2008 Amendments to the Foreign Intelligence Surveillance Act.[79] The plaintiffs claimed to have suffered an injury-in-fact because of a reasonable likelihood that their communications with foreign contacts would be intercepted, and because the risk of surveillance required them to take costly and burdensome actions to protect the confidentiality of their communications.[80] However, there was no evidence that the plaintiffs' communications had been targeted or that the government was going to target their communications in the future.[81]

As a result, the Court held in a 5-4 decision that the plaintiffs did not have standing under Article III.[82] The Court "reiterated that [the] 'threatened injury must be *certainly impending* to constitute injury-in-fact,' and that '[a]llegations of *possible* future injury' are not sufficient."[83] Specifically, the Court found that plaintiffs' theory of future injury was "too speculative," and not actual or "certainly impending," with the plaintiffs' allegations for standing based on a "highly attenuated

76. United States v. One Lincoln Navigator 1998, 328 F.3d 1011, 1013 (8th Cir. 2003).
77. Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010).
78. *See generally* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).
79. *Id.* at 401–05.
80. *Id.* at 401.
81. *Id.* at 411.
82. *Id.*
83. *Id.* at 409 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

chain of possibilities."[84] Further, the Court found that plaintiffs' "contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm [was] unavailing . . . [because they] cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[85]

Since *Clapper*, cases have been inconsistent on the issue of Article III standing and the injury-in-fact requirement. The injury-in-fact analysis is very fact-specific in nature, with some courts finding no standing on imminence grounds, reasoning that the plaintiff had suffered no actual injury, while others find standing in cases involving similar facts and claims. In fact, there are several notable data breach and privacy class action cases that have contributed to this split of authority.

2. Circuits Finding Injury Sufficient for Standing: Third, Sixth, Seventh, Ninth, & D.C.

In the Third Circuit, the decision in *In re Horizon* involved two stolen laptops that contained unencrypted personal information (specifically, health insurance data, names, addresses, dates of birth, and social security numbers) of more than 839,000 Horizon members.[86] Of those with information stolen, only one named plaintiff experienced *actual* misuse in the form of a fraudulent tax filing.[87] The plaintiffs alleged willful and negligent violations of the Fair Credit Reporting Act and numerous violations of state law, centering around Horizon's failure to take reasonable and appropriate measures to secure the stolen laptops and safeguard the member's information.[88] In its opinion, the court clarified the standing requirements for plaintiffs asserting violations of certain federal statutes.[89]

The court held that the plaintiffs, by alleging an unauthorized transfer of personal identifying information in violation of the Fair Credit Reporting Act, had established a sufficient *de facto* injury for standing, even if that information was not improperly used.[90] This decision narrowed the lack of standing defense in this particular type of data

84. *Id.* at 401, 410.

85. *Id.* at 415.

86. *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 630 (3d Cir. 2017).

87. *Id.*

88. *Id.* at 629, 631.

89. *Id*. at 639–40.

90. *Id.* at 629, 636.

breach case, where the claim involved arose from certain statutory rights. However, the result still leaves open whether other federal statutes may recognize data breaches as injuries-in-fact, and whether more technical violations of statutes could constitute a harm for standing.

In the Sixth Circuit, the data breach in *Galaria v. Nationwide Mutual Insurance Co.*, involved the theft of personal information (specifically, names, dates of birth, driver's license numbers, and social security numbers) of 1.1 million customers of Nationwide Mutual Insurance Company by hackers of the company's computer network.[91] Plaintiffs sued Nationwide for violating the Fair Credit Reporting Act (failure to adopt adequate procedures to protect personal information) and for common law torts of negligence and bailment.[92] Plaintiffs alleged that they had incurred costs associated with mitigating the risk, including purchasing credit reporting and monitoring services for credit reports and bank statements.[93] Ultimately, a split panel held that plaintiffs had sufficiently demonstrated standing by alleging that the Nationwide hack had subjected them to significantly heightened risk of fraud and identity theft.[94]

The court found that even though plaintiffs claimed no incidences of actual fraud or identity theft, their claimed injury was not merely "hypothetical."[95] The court reasoned, while distinguishing the facts of this case from those in *Clapper*, "[t]here is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals. . . . Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for . . . fraudulent purposes."[96] Further, the court also noted that Nationwide seemed to recognize the severity of the risk because it offered free credit monitoring and identity theft protection for one year; thus Nationwide's mitigation efforts were actually used against them in the end.[97] This decision is one of the most favorable to plaintiffs in the data breach context because no plaintiffs even alleged any actual fraud or identity theft as a result of the data theft.

In the Seventh Circuit, the data breach in *Remijas* involved hackers attacking Neiman Marcus and stealing the credit card numbers of

91. Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 386 (6th Cir. 2016).
92. *Id.*
93. *Id.* at 386–87.
94. *Id.* at 388.
95. *Id.*
96. *Id.*
97. *Id.*

approximately 350,000 of its customers.[98] Some of these customers found fraudulent charges on their cards around the same time of the breach.[99] The court asserted that *Clapper* did not consummately bar consumers from bringing suit based on substantial risk of future injury and found that the costs incurred by the plaintiffs were material enough to be considered particularized injuries.[100] Neiman Marcus' major objection was that the plaintiffs could not show that their injuries were fairly traceable to the Neiman Marcus breach instead of a breach involving Target, which occurred around the same time.[101] The court responded by stating that, "if there are multiple companies that could have exposed the plaintiffs' private information to hackers, then the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury."[102] The court ultimately held that "injuries associated with resolving fraudulent charges and protecting oneself against future identity theft" were sufficient to confer Article III standing.[103]

In the Ninth Circuit, the data breach in *Krottner v. Starbucks Corp.* involved the theft of a laptop containing the personal information (specifically, names, addresses, and social security numbers) of Starbucks employees.[104] While the leaked information had not yet been misused, the plaintiff's sued Starbucks for negligence and breach of implied contract, emphasizing that the data leaked had increased their risk of identity theft.[105] Here, the court asserted that plaintiffs alleged "a credible threat of real and immediate harm stemming from the theft of the laptop containing their unencrypted personal data."[106] It explained that had the allegation been more conjectural or hypothetical (i.e., if no laptop had been stolen and the plaintiffs sued based on the risk that it would be stolen in the future), the threat would be much less credible.[107] Thus, plaintiff's satisfied the injury-in-fact requirement for Article III standing by stating that an injury-in-fact can be satisfied by a threat of future harm, or by an act which harms the plaintiff only by increasing the risk of future

98. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 689–90 (7th Cir. 2015).
99. *Id.*
100. *Id.* at 694.
101. *Id.* at 696.
102. *Id.*
103. *Id.*
104. Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010).
105. *Id.* at 1140–41.
106. *Id*. at 1143.
107. *Id.*

harm that plaintiff would have otherwise faced, absent defendant's actions.[108]

Though *Krottner* occurred before the Supreme Court's decision in *Clapper*, the Ninth Circuit subsequently decided another data breach case in *In re Zappos.com, Inc.*, where it reiterated its expansive view of injuries involving the risk of future harm for standing.[109] In that case, the court unanimously held that plaintiffs, whose personal information (specifically, payment card data) was stolen but not actually misused, had standing to sue because they faced a substantial risk of identity theft.[110] This is important because it held that *Krottner* is still good law after the decision in *Clapper*.[111]

Finally, in the D.C. Circuit, the data breach in *Attias v. CareFirst, Inc.* involved a cyberattack where 1 million CareFirst's customers' personal information (specifically, names, dates of birth, email addresses, and subscriber information) was stolen.[112] Plaintiffs argued that CareFirst violated state laws and legal duties by failing to safeguard their information and exposing them to an increased risk of identity theft.[113] The court stated that this injury was sufficient to establish standing because it was "at the very least . . . plausible" to infer that the hackers had the intent and ability to use the stolen data for illegal purposes.[114]

The above cases from this side of the circuit split present the hurdles a defendant must clear to secure dismissal of a data breach claim. Generally, they collectively held that the risk of future harm from a data breach was, on its face, injury sufficient for standing. Based on these plaintiff-favorable rulings on the standing issue, these circuits will likely emerge as the forums of choice for data breach class actions. And as the Supreme Court recently denied *certiorari* in 2018 for *CareFirst*, this split remains in place for the foreseeable future.

3. Circuits Finding No Injury Sufficient for Standing: First, Second, Fourth, & Eighth

In the First Circuit, the case of *Katz v. Pershing* involved a unique set of facts in this context because the case was actually filed before any data

108. *Id.*
109. *In re* Zappos.com, Inc., 888 F.3d 1020, 1030 (9th Cir. 2018).
110. *Id.* at 1023, 1030.
111. *Id*. at 1023.
112. Attias v. CareFirst, Inc., 865 F.3d 620, 622–23 (D.C. Cir. 2017), 865 F.3d at 622.
113. *Id*. at 623.
114. *Id.* at 628.

breach occurred.[115] Plaintiff alleged that she experienced an increased risk of potential future loss due to the defendant's alleged failure to adhere to reasonable security practices and privacy regulations.[116] The court held that such allegations were not sufficient to meet the requirements for Article III standing.[117] It reasoned that the allegations of harm were too speculative and could not show impending injury because the facts alleged left too many unknown variables, including whether the plaintiff's data would actually be stolen or lost, and even then, whether the data would be misused in a way that would harm her.[118] Ultimately, the plaintiff's standing theory rested "entirely on the hypothesis that at some point an unauthorized, as-yet unidentified, third party might access her data and then attempt to purloin her identity."[119]

In the Second Circuit, the data breach in *Whalen v. Michaels Stores, Inc.* involved the theft of customers' credit card and debit card data (specifically, card numbers and expiration dates).[120] Relying on the standard from *Clapper*, the court deemed the named plaintiff's allegation of two attempted fraudulent credit card charges insufficient to make the risk of future harm "certainly impending."[121] Because plaintiff was never asked to pay, nor did she pay, any fraudulent charges and because her stolen credit card was promptly canceled after the breach and no other personally identifying information (such as her date of birth or social security number) was alleged to have been stolen, the court concluded that she had alleged no injury that would satisfy the constitutional standing requirements of Article III.[122]

In the Fourth Circuit, *Beck v. McDonald* consolidated two cases against a Veteran's hospital.[123] The first involved a stolen laptop with limited data (specifically, names, dates of birth, last four digits of social security numbers, and physical descriptors) and the second involved stolen boxes of pathology files with information (specifically, names, social security numbers, and medical diagnoses) about deceased persons.[124] Interestingly, the court denied standing for both sets of facts,

115. Katz v. Pershing, LLC, 672 F.3d 64, 64 (1st Cir. 2012).
116. *Id.* at 78.
117. *Id.* at 80–81.
118. *Id.* at 80.
119. *Id.* at 79.
120. Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017).
121. *Id.*
122. *Id.* at 90–91.
123. Beck v. McDonald, 848 F.3d 262, 266 (4th Cir. 2017).
124. *Id.* at 267, 268.

but adopted the reasoning from *Krottner* and *Remijas* (which, as explained above, are on the opposite side of the circuit split), implying that some breaches do make future harm certainly impending.[125] Ultimately, it seems that, for this specific case, the fact that three years had passed without any visible misuse of the personal information proved decisive and the court found that the threat of identity theft stemming from these breaches was too speculative to establish an injury-in-fact for these claims.[126]

In the Eighth Circuit, *In re SuperValu, Inc.* involved two data breaches on a chain of retail grocery stores in which hackers gained access to the payment information of customers (specifically, names, credit or debit card numbers, card expiration dates, card verification value codes, and personal identification numbers).[127] The plaintiffs alleged that the defendant failed to take adequate measures to protect customers' information; for example, the defendant allegedly used default or common passwords, failing to lock out users after several failed login attempts and not segregating access to different parts of the computer network or use firewalls to protect customer information.[128] The plaintiffs claimed that customer information was stolen as a result of the breaches, subjecting plaintiffs to "an imminent and real possibility of identity theft."[129] One plaintiff also alleged that he suffered a fraudulent charge on his credit card statement, resulting in the replacement of the card.[130] In the end, however, the court found that the individual plaintiffs who had not experienced any fraudulent charges or identity theft following the breaches and had not sufficiently alleged a substantial risk of future injury.[131] But the court did find that the injury of the one plaintiff who alleged fraudulent use of this card gave rise to standing in his individual case.[132]

The above cases from this side of the circuit split have generally held that plaintiffs must allege an actual injury in the form of fraudulent charges on existing credit or debit card accounts or the opening of fraudulent financial accounts resulting from their stolen personal information to establish the requisite injury-in-fact for Article III

125. *Id.* at 273, 274.
126. *Id.* at 274–75.
127. *In re* SuperValu, Inc., 870 F.3d 763, 766 (8th Cir. 2017).
128. *Id.*
129. *Id.*
130. *Id.* at 767.
131. *Id.* at 771–72.
132. *Id.* at 774.

standing. They have determined that general allegations of a heightened risk of identity theft from stolen personal information alone do not constitute an injury-in-fact, raising the pleading requirements for plaintiffs in data breach cases in these jurisdictions. Thus, with the circuit split firmly in place, the potential for standing will largely depend on both where the suit is filed and on that court's interpretation of the standard to prove sufficient standing.[133]

B. *Next Step: Causation & Redressability*

For those cases that are fortunate enough based on their particular factual situations to make it past the first hurdle of injury-in-fact for Article III standing, the next challenge presented focuses on causation and redressability. The data breach context presents a somewhat unique circumstance surrounding causation (typically meaning that the injury must be fairly traceable) because of the ability of a data thief to aggregate data from multiple sources. This creates issues for courts who enforce a strict "rule of enablement," which means that the data stolen must have been sufficient by itself to enable the alleged misuse.[134] And while forensic testing may reveal how a breach was achieved and what data was stolen, such evidence-based results seldom exist to prove a direct connection between the act of the breach and a particular subsequent misuse that resulted in injury.[135]

As noted by the court in *Remijas* above, once a set of mostly immutable personal information has been involved in multiple breaches, causation becomes an even harder element to prove.[136] Courts have approached this issue in different ways. Most notable from a public policy standpoint was that of *In re Yahoo! Inc. Customer Data Security Breach Litigation*, where the court "refused to consider that any instances of actual misuse might have resulted from other data breaches, as this would create a perverse incentive for stewards of consumer data."[137] But some courts analyzing data breach cases deem that this standing requirement has been satisfied where a business admits customer information has been exposed by issuing data breach notifications (as they are legally required to give such notifications under state privacy laws) or where a business

133. *See* Cease, *supra* note 72, at 404.

134. *See* David L. Silverman, *Developments in Data Security Breach Liability*, 73 BUS. LAW. 215, 218–19 (2017) [hereinafter 2017 Data Breach Developments].

135. *See* Silverman, *supra* note 13, at 221.

136. *See* Silverman, *supra* note 13, at 221–22.

137. *See* Silverman, *supra* note 13, at 222.

issues new customer cards themselves due to a breach.[138] Ultimately, some courts are more reluctant than others to recognize causation, so jurisdiction choice will also impact this outcome regarding the standing determination.

Redressability is the final step in the Article III standing analysis, and it has been invoked the least often in data breach cases.[139] The injurious standard to satisfy is that "it must be likely, as opposed to merely speculative, that [an] injury will be redressed by a favorable decision."[140] Major issues in this area typically center around failures to allege any quantifiable damages resulting from the breach and instances where credit card companies or other parties have already remedied some of the victims' injuries.[141] If these issues are present, the plaintiffs' claimed injuries may struggle to pass the test for redressability.

III. ATTEMPTS AT A FEDERAL STANDARD & FORTHCOMING STATE LEGISLATION

Though there have been a number of attempts at passing a uniform federal standard, the United States lacks a comprehensive federal law that regulates the collection and use of consumer personal information. As a result, many states have passed their own laws, which often contain different and sometimes incompatible provisions regarding what categories and types of personal information are protected or which entities are covered. In addition, the judicial circuits have also diverted from a single interpretation in the data breach standing context, which only adds to the inconsistency and confusion across the board. Congress's ability to successfully pass a uniform federal data breach standard is highly dependent on the political state of the country, and with the current stark divide surrounding political views on the subject of federal regulation, such a federal standard is not likely to be enacted anytime soon. Fortunately, California's new privacy regulation possesses the potential to cause a seismic shift in the landscape of data privacy law, not just in California, but across the country.

138. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696 (7th Cir. 2015); *In re* Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 487 (D. Minn. 2015).

139. *See* 2017 Data Breach Developments, *supra* note 134, at 220.

140. Lujan v. Defs. Of Wildlife, 504 U.S. 555, 561 (1992).

141. *See, e.g.*, Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 857 (S.D. Tex. 2015).

A. *Attempts at a Federal Standard*

Many have called on Congress to enact flexible and technologically neutral privacy and security laws. For example, in 2014, the "Data Security Breach Notification Act" was introduced in the Senate; however, it did not move past referral to a Senate subcommittee.[142] Then, the Barack Obama presidential administration put forth plans in 2015 for the "Personal Data Notification & Protection Act," which proposed many measures aimed at promoting data security, data privacy, and protection against identity theft, including a "Consumer Privacy Bill of Rights."[143] This was largely based on the Fair Information Practice Principles, which are thought of as general processes and procedures that organizations should implement, recognizing that Americans have a strong interest in how information about them is collected, used, and shared by companies.[144]

The 2015 Act aimed to protect "sensitive personally identifiable information," including: (1) first and last name in combination with several different elements; (2) a government-issued identification number, including a social security number or driver's license number; (3) biometric data including fingerprints or voice prints; (4) unique account identifiers; and (5) a username in combination with a password or security question.[145] It also contained a strict standard of notification requirements which would have been enforced by the Federal Trade Commission and state Attorney Generals.[146] A major point of contention in this bill was that the Personal Data Notification & Protection Act would supersede any state laws covering breaches of computerized data from businesses.[147] Unfortunately, this proposal lost momentum shortly after a draft of the bill was put forward and it also did not move past subcommittee review.[148] Most recently, the Donald J. Trump presidential

142. *See* Martha Wrangham & Gretchen A. Ramos, *Calls for Federal Breach Notification Law Continue After Yahoo Data Breach*, THE NAT'L L. REV. (Oct. 5, 2016), https://www.natlawreview.com/article/calls-federal-breach-notification-law-continue-after-yahoo-data-breach.

143. *See* OFFICE OF THE PRESS SEC'Y, FACT SHEET: SAFEGUARDING AMERICAN CONSUMERS & FAMILIES (Jan. 12, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families.

144. *See* Brendan McDermid, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

145. Personal Data Notification & Protection Act, H.R. 1704, 114th Cong. § 112(12) (2015).

146. *Id.* at § 101(c); *see also id.* §§ 107–108 (explaining the rules and methods of enforcement).

147. *See id.* § 109.

148. *See* Wrangham & Ramos, *supra* note 142.

administration's lack of appetite for technology policy or regulation in general has left this issue and any attempts at a federal data breach standard at a standstill for the foreseeable future.[149]

B. *The California Consumer Privacy Act*

California has always had a strong policy regarding the subject of privacy, often enumerating more elaborate and stricter privacy laws than other states. In fact, California even enumerated the right to privacy in its constitution.[150] Once again, California is charging forward in the world of privacy legislation and on June 28, 2018, with subsequent minor amendments, it has enacted the California Consumer Privacy Act (CCPA).[151] The CCPA will go into effect starting January 1, 2020, and it will generally restrict certain businesses' ability to collect and sell the "personal information" of consumers.[152] Though the CCPA will take effect in a single state, its reach will extend well beyond the borders of California, and its expansive protections mark a major shift in the nation's data privacy regime.[153]

The CCPA applies to any for-profit business (regardless of where it is located) that collects the personal information of California residents and satisfies at least one of the following criteria:

> (1) generates gross revenues above $25 million (and such threshold is not limited to revenue earned in the State of California), (2) engages in the buying, selling, receiving, or sharing of the personal information of at least 50,000 California residents, households, or internet-connected devices, or (3) derives at least 50% of its annual revenues from the sale of consumers' personal information.[154]

The definition of this type of business for purposes of the CCPA also includes "[a]ny entity that controls or is controlled by a business, as

149. *See* McDermid, *supra* note 144.

150. CAL. CONST. art I, § 1 (providing that "[a]ll people are by nature free and independent and have inalienable rights . . . enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy").

151. *See* WILSON C. FREEMAN, CONG. RESEARCH SERV.: LEGAL SIDEBAR, CALIFORNIA DREAMIN' OF PRIVACY REGULATION: THE CALIFORNIA CONSUMER PRIVACY ACT AND CONGRESS 1 (Nov. 1, 2018).

152. *See* CAL. CIV. CODE § 1798.105.

153. *See* FREEMAN, *supra* note 151.

154. CAL. CIV. CODE § 1798.140(c)(1).

defined in [the main "business" definition], and that shares common branding with the business.[155]

The CCPA also contains a limited number of exemptions to the definition of "business." If every aspect of the commercial conduct takes place wholly outside of California, then such business is exempt from the CCPA.[156] Also exempted from its coverage is the collection of certain information covered by other statutes, including HIPAA, the FCRA, the GLBA, and the DPPA, as well as "publicly available information," which includes information lawfully made available from government records.[157] The CCPA's definition of "personal information" is very inclusive, encompassing all "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[158]

---

155. *Id.* § 1798.140(c)(2).

156. *Id.* § 1798.145(a)(6).

157. *Id.* § 1798.145. *See also* FREEMAN, *supra* note 151, at 2.

158. *Id.* § 1798.140(o)(1). The CCPA includes examples of what is included in the definition of "personal information":

> (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
>
> (B) Any categories of personal information described in subdivision (e) of Section 1798.80.
>
> (C) Characteristics of protected classifications under California or federal law.
>
> (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
>
> (E) Biometric information.
>
> (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.
>
> (G) Geolocation data.
>
> (H) Audio, electronic, visual, thermal, olfactory, or similar information.
>
> (I) Professional or employment-related information.
>
> (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights

Such a broad definition illustrates the intent of the CCPA's drafters regarding the statute's breath and its ability to provide expansive protections to consumers.[159] And ultimately, even with the exemptions, these provisions will likely reach a considerable number of businesses with a website accessible in California.

The CCPA confers three major "rights" on consumers: the "right to know," the "right to opt out," and the "right to delete."[160] The "right to know" is derived from the fact that businesses must, in advance of any collection, "inform consumers [by mail or electronically] as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used."[161] Further, in addition to requiring this advance collection disclosure, consumers also have the right to request that a business that collects personal information about the consumer disclose to the consumer the specific pieces of personal information that the business has collected or sold from the consumer, the categories of sources from which the information was collected, the business purposes for collecting or selling the personal information, and the third parties with whom the information was shared.[162]

Next, the "right to opt out" derives from the requirement that businesses must inform consumers of the right to opt out of the sale of a consumer's information, and if a consumer so directs a business not to sell the consumer's personal information, the business cannot again sell the consumer's information unless the consumer subsequently provides the business express authorization.[163] It also requires an affirmative "opt

---

and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. *Id.*

159. *See* FREEMAN, *supra* note 151, at 3.

160. *See* CAL. CIV. CODE §§ 1798.100, 1798.120, 1798.105.

161. *Id.* § 1798.100(b). This information will be provided to the consumer free of charge. *Id.* § 1798.100(d).

162. *Id.* § 1798.110(a).

163. *Id.* § 1798.120. With respect to the "right to opt-out," businesses must provide a "clear and conspicuous link" on their homepage entitled "Do Not Sell My Personal Information" that opens an Internet Web page enabling a consumer to opt-out of the sale of the consumer's personal information. *Id.* § 1798.135(a)(1). Additionally, the business must also include a description of consumers' opt-out rights, along with a separate link to the "Do Not Sell My Personal Information" webpage in its online privacy policy. *Id.* § 1798.135(a)(2).

in" for consumers under the age of 16 (by the consumer directly if they are between the ages of 13 and 16 or by the consumer's parent of guardian if the consumer is under 13).[164] Finally, the "right to delete" derives from the requirement that businesses, if requested by a consumer, must delete any information collected about such consumer.[165] The CCPA provides some exceptions to this right, including: when the information is needed to complete a particular transaction for the consumer, to detect security incidents or protect against fraud, or where such retention enables solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.[166]

As an additional protection for consumers, the CCPA contains a nondiscrimination rule to backstop the discussed rights. Specifically, it provides that no business may discriminate against a consumer by "denying goods or services," by "charging different prices or rates," or by "providing a different level or quality of goods or services" to consumers who exercise their rights under the CCPA.[167] However, the CCPA *does* allow businesses to "offer financial incentives" for the collection, sale, or non-deletion of personal information. It also provides that a business may offer a different price to consumers who exercise their rights "if that price . . . is directly related to the value provided to the consumer by the consumer's data."[168]

Enforcement of the CCPA will largely fall under the authority of the California Attorney General. Businesses that are in violation of the CCPA and do not cure those violations within 30 days are liable for civil penalties of up to $2,500 for each violation, which increases to $7,500 if the violation is intentional.[169] Moreover, it gives California residents a civil right of action for injunctive or declaratory relief, as well as monetary damages (no less than $100 and no more than $750 per incident, or actual damages, whichever is greater) against businesses that fail to implement *reasonable security measures* to protect their personal information.[170] Significantly, "reasonable security measures" are not defined by the CCPA, and in the absence of a specified definition, a definition will likely be determined by the judicial system and analyzed

164. *Id.* § 1798.120(d).

165. *Id.* § 1798.105. Following such a request, the business must delete the information from its own records, as well as the records of it service providers. *Id.* § 1798.105(c).

166. *Id.* § 1798.105(d).

167. *Id.* § 1798.125(a)(1).

168. *Id.* §§ 1798.125(b)(1), (a)(2).

169. *Id.* § 1798.155(b).

170. *Id.* § 1798.150(a)(1).

on a case-by-case basis. Such actions can only be brought if a consumer provides a business with 30 days' written notice and provides the business with the opportunity to "cure" the violation, unless the consumer suffered actual pecuniary damages.[171] This safe harbor cuts both ways: on the one hand, it will provide business with advance notice of the claims and the ability to engage plaintiffs before litigation progresses; and on the other hand, because of the uncertainty in the statute as drafted (i.e., how to "cure" is not defined), it is not clear what an actual cure of a data breach would look like.[172]

Overall, the CCPA will regulate how businesses with an online presence in California collect, share, and use consumer personal information. This unprecedented change in California's privacy law will invite an explosion of consumer litigation as plaintiffs seek to recover statutory damages under the private right of action.[173] Whereas thus far, plaintiffs have often struggled to sufficiently demonstrate that theft of their data has resulted in an injury-in-fact for standing purposes, the new allowance for statutory damages has cleared a major litigation hurdle for plaintiffs since they will no longer need to demonstrate that an actual financial injury has been suffered.[174] It is very likely that because of its expansive scope and jurisdictional reach, the CCPA will become the standard for best practices in privacy and data protection for United States residents unless it is later preempted by federal law, or another state adopts a law with more demanding requirements.

IV. POTENTIAL MITIGATION OF LITIGATION EXPOSURE

The best chance for avoiding litigation exposure from the company's perspective, is to implement adequate security measures to prevent data breaches in the first place. As previously stated, the federal and state data security statutes generally require that companies in possession of customer personal information implement adequate security measures, though they do not offer any further explanation of what would qualify or how such companies should assess vulnerabilities. For some guidance on this matter, the Center for Internet Security's Critical Security Controls identifies a minimum level of information security that all organizations that collect or maintain personal information should meet in order to meet the standard for reasonable security.[175] The minimum security controls for effective cyber defense are listed below.[176]

171. *Id.* § 1798.150(b).
172. *See* Buese, *supra* note 22.
173. *See* Buese, *supra* note 22.
174. *See* Buese, *supra* note 22.
175. *See* HARRIS, *supra* note 21, at 30.
176. *See* HARRIS, *supra* note 21, app. at 39.

CSC 1 Inventory of Authorized and Unauthorized Devices
CSC 2 Inventory of Authorized and Unauthorized Software
CSC 3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CSC 4 Continuous Vulnerability Assessment and Remediation
CSC 5 Controlled Use of Administrative Privileges
CSC 6 Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7 Email and Web Browser Protection
CSC 8 Malware Defenses
CSC 9 Limitation and Control of Network Ports, Protocols, and Services
CSC 10 Data Recovery Capability
CSC 11 Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12 Boundary Defense
CSC 13 Data Protection
CSC 14 Controlled Access Based on the Need to Know
CSC 15 Wireless Access Control
CSC 16 Account Monitoring and Control
CSC 17 Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18 Application Software Security
CSC 19 Incident Response and Management
CSC 20 Penetration Tests and Red Team Exercises

These controls should serve as a starting point, and the failure to implement all twenty that apply to a particular company's data environment could constitute a lack of reasonable security.[177]

Further, companies should make multi-factor authentication available on consumer-facing online accounts that contain sensitive personal information, such as requiring something biometric (i.e., a fingerprint) or an additional code to enter that comes through as a text or other one-time-password token.[178] Such requirements would make it much more difficult for a third party to breach the account because access to the account would require more than just the baseline username and password combination. Companies are also well advised to consistently use strong

177. *See* HARRIS, *supra* note 21, at 30.

178. *See* HARRIS, *supra* note 21, at 34–35.

encryption methods to protect personal information on mobile electronic devices (such as laptop computers or smart phones) that could be physically lost or stolen.[179] Ultimately, in this context the motto really is "better safe than sorry." When in doubt it is better to implement as many security controls as are feasibly possible for the particular type and size of the company, based upon the sensitivity of the stored personal information.

Additional methods for reducing a company's litigation exposure incorporate the use of an arbitration clause and a class action waiver in the website's terms and conditions, which could prohibit users from prompting mass litigation.[180] The Supreme Court has confirmed that class action waivers in arbitrations provisions are enforceable.[181] Such arbitration provisions and waivers should be conspicuous both in the company's notice of its terms and conditions for service, and in the terms and conditions themselves.[182] For example, to maximize the likelihood of enforcement, they should be "easily accessible and displayed in a sufficiently large viewing window to provide the user an adequate opportunity to review the terms, thereby eliminating any doubts that a reasonable user would have noticed them" and they should include easily understandable, balanced provisions to avoid a finding of unconscionability.[183] Additionally, best practices would require users to affirmatively accept the contractual terms before proceeding to the next step in the transaction or service provided.[184]

CONCLUSION

Protection of consumer personal information is a major issue faced not only by Americans, but by consumers across the globe. Both the frequency and severity of data breaches in the modern day of technology and internet usage have consistently increased throughout the twentieth century, developing into what some consider to be a modern "data breach epidemic." Neither federal nor state regulations fully address this epidemic in a way that provides consumers and businesses with clarity regarding their respective rights and duties post-data breach.[185] After their personal information is exposed, consumers face uncertainty in seeking relief, and the current circuit split in this area makes the choice of where

179. *See* HARRIS, *supra* note 21, at 36.

180. *See* Buese, *supra* note 22.

181. *See* Buese, *supra* note 22; *see, e.g.*, DirecTV Inc. v. Imburgia, 136 S. Ct. 463 (2015); AT&T Mobility LLC v. Concepcion, 563 U.S. 333 (2011).

182. *See* Buese, *supra* note 22.

183. Buese, *supra* note 22.

184. *See* Buese, *supra* note 22.

185. *See* Jones, *supra* note 20, at 813.

to file a claim of paramount importance if the injury is based on the theory of an increased risk of future harm (such as the increased risk for identity theft). From the perspective of businesses in possession of consumer personal information, conflicting laws relating to compliance creates an unnecessary burden for large businesses that operate in multiple jurisdictions.

There have been some attempts at a federal standard, but none have ultimately succeeded. Though it seems unlikely under the current political climate, enacting a federal data breach notification and data protection statute would go a long way in solving many of the issues currently faced by consumers and businesses. Confronted with this intimidating and rapidly changing technological landscape, California's new sweeping privacy legislation, the CCPA (effective January 1, 2020), will impose a multitude of new, extremely demanding notice, disclosure, and consent requirements on an array of business entities that conduct operations or handle the personal information of California residents. The CCPA will likely cause a shift in the landscape of data privacy law not just in California, but across the entire United States.

The data breach epidemic is not going away anytime soon, so in the meantime consumers should take extra precautions when evaluating whether, and with whom, they share their personal information. Additionally, businesses that use, collect, or store consumer personal information should maximize their security controls in place to prevent or decrease the likelihood of a data breach, and should also incorporate the use of both class action waivers and mandatory arbitration provisions to mitigate the potential effects of post-data breach litigation.

HB 409, A DRASTIC DEPARTURE FROM FLORIDA'S TRADITIONAL STANCE ON WILL EXECUTION FORMALITIES

Justin Shifrin[*]

Abstract

The baby boomer generation is aging, and many of the citizens that belong to this generation are retiring to Florida. Accordingly, Florida is expected to host one of the largest wealth transfers in history. And while the baby boomer population ages, our society is becoming more digitized. Things we traditionally did by pen and paper are now increasingly done by computer and keystroke, and wills are no exception. What was previously considered a document whose sacred nature could only be appreciated by the affixation of a handwritten signature at the bottom thereof, wills are now being drafted, signed, witnessed, and stored digitally. This Note analyzes Florida's recently enacted legislation, HB 409, that authorizes electronic wills and the remote witnessing of such wills. The analysis proceeds against a backdrop defining the term "electronic will" and explaining how electronic wills diverge from what society has traditionally deemed a will. I begin by explaining the policy reasons behind statutory will act formalities and the four functions that are served by these traditional formalities. I also discuss the various positions that courts have taken when deciding whether to admit any purported will to probate. Next, I discuss the three categories of electronic wills and the shortcomings that each of these categories faces with respect to the "Four Functions." After a brief discussion of how lawmakers and courts nationally and internationally have addressed the rise of electronic wills, this Note will turn the reader's attention to Florida's HB 409. This Note provides a summary of the legislation's main provisions and an analysis of its specific "functional" shortcomings. After June 1, 2020, Florida courts should expect an influx of digitally signed and remotely witnessed electronic wills. Florida courts should also be aware of the entirely new grounds for will contests that HB 409 creates.

---

[*] Juris Doctor, University of Florida Levin College of Law. I would like to thank Professor Lee-Ford Tritt and William Hennessey for encouraging me to explore the issues presented in this note and their guidance during the drafting process. I would also like to thank my family, fiancé, and the UF Law Class of 2020 for their unwavering support.

INTRODUCTION

Americans are increasingly storing personal data on electronic devices.[1] In 2016, the American Community Survey determined that eighty-nine percent of American households own a computer.[2] Seventy-eight percent of Americans own a smartphone, and fifty-five percent own a tablet device.[3] Prior to the introduction of the iPhone in 2007, the mere ownership of an electronic device capable of connecting to the internet did not mean that Americans were constantly connected to the internet. iPhones and other smartphones, however, set the stage for humanity's incessant connection to the internet and electronics.[4] We continuously upload and store personal data on our phones, our computers, our cars, and even our refrigerators, leaving behind our digital footprints.[5] Our electronic devices have become extensions of ourselves.[6] In an effort to capitalize on our fixation with the electronic storage of personal data, "cloud" storage companies such as Dropbox and Evernote have come into existence and recruited hundreds of millions of users.[7]

Humanity's steadfast attachment to electronic devices and the internet has advanced the manner in which we record and monitor our financial

1. *See* Michael Lynch, *Leave My iPhone Alone: Why Our Smartphones Are Extensions of Ourselves*, GUARDIAN (Feb. 19, 2016, 6:29 PM), https://www.theguardian.com/technology/2016/feb/19/iphone-apple-privacy-smartphones-extension-of-ourselves.

2. Camille Ryan, *Computer and Internet Use in the United States: 2016*, U.S. CENSUS BUREAU (Aug. 8, 2018), https://www.census.gov/library/publications/2018/acs/acs-39.html.

3. Leo Sun, *Foolish Take: Nearly 80% of Americans Own Smartphones*, USA TODAY (Feb. 24, 2018, 6:30 AM), https://www.usatoday.com/story/money/markets/2018/02/24/a-foolish-take-nearly-80-of-americans-own-smartphones/110342918/.

4. *See* Lynch, *supra* note 1.

5. *See id.*

6. *Id.*

7. *See Developments in the Law — More Data, More Problems*, 131 HARV. L. REV. 1715, 1790–91 (2018).

lives.[8] We use electronic devices and the internet to make our daily purchases, pay our bills, and record our thoughts. And now, courts are beginning to grapple with the issue of testators' drafting and storing estate planning documents on these electronic devices.[9] Many online websites offer testators the opportunity to draft a will electronically.[10] However, under traditional law, the resulting document is invalid unless it is then printed out, notarized, signed by the testator in the presence of two witnesses, and then signed by the two witnesses.[11]

The aging baby boomer population lives among the eighty-nine percent of Americans that own a computer.[12] By 2030, the entirety of the baby boomer population will have reached the age of 65, making one fifth of all U.S. residents at or above the retirement age.[13] Florida, the state with the highest percentage of residents age 65 or older, is expected to harbor over six million of these retirees.[14] Thus, as the richest generation in history prepares to pass down their assets to their successors, millennials stand to inherit a record $30 trillion from baby boomers, with much of this wealth transferring in the state of Florida.[15] Florida courts will face the issue of probating an increasing number of electronic wills. In anticipation of this issue, the Florida legislature recently enacted the Florida Electronic Wills Act, effective June 1, 2020.[16] This legislation comes as a surprise because Florida has traditionally been a strict compliance state that has not admitted holographic wills to probate.[17]

This Note provides a background of the general will act requirements for a valid will, an overview of electronic wills, and a discussion of how

---

8. *See* Recent Case, *Trusts and Estates — Electronic Wills — Michigan Court of Appeals Holds Electronic Document to be Valid Will Under Harmless Error Rule.* — In re Estate of Horton, *No. 339737 (Mich. Ct. App. July 17, 2018) (per curiam)*, 132 HARV. L. REV. 2082, 2082 n.1 (2019).

9. *See, e.g.*, *In re* Estate of Castro, No. 2013ES00140, 2013 WL 12411558, at *1 (Ohio C.P. Lorain Cty. 2013).

10. Paul Sullivan, *A Will Without Ink and Paper*, N.Y. TIMES (Oct. 18, 2019), https://www.nytimes.com/2019/10/18/your-money/electronic-wills-online.html.

11. *See* JESSE DUKEMINIER, ROBERT H. SITKOFF & JAMES LINDGREN, WILLS, TRUSTS, AND ESTATES 226 (8th ed. 2009).

12. Ryan, *supra* note 2.

13. Jodie Distler, Commentary, *Re-considering Undue Influence in the Digital Era*, 44 ACTEC L. J. 131, 131–32 (2019).

14. Bob Niedt, *11 Reasons You Don't Want to Retire in Florida*, KIPLINGER (Feb. 28, 2019), https://www.kiplinger.com/slideshow/retirement/T047-S001-reasons-you-don-t-want-to-retire-in-florida/index.html.

15. Brittany De Lea, *Get Ready for One of the Greatest Wealth Transfers in History*, N.Y. POST (Mar. 13, 2018, 3:43 PM), https://nypost.com/2018/03/13/get-ready-for-one-of-the-greatest-wealth-transfers-in-history/.

16. H.B. 409, 121st Reg. Sess. (Fla. 2019).

17. *E.g.*, *In re* Estate of Salathe, 703 So. 2d 1167, 1168 (Fla. Dist. Ct. App. 1997) (citing FLA. STAT. § 732.502(2) (1995)) ("The decedent's holographic will is without force or effect under Florida law.").

states, such as Florida, have responded to the anticipated rise of electronic wills. It concludes by directing the reader's attention to newer, possibly unanticipated issues that could arise from the way the Florida electronic wills act is drafted in its current form.

I. WHAT IS A WILL?

The hallmark of the American law of donative transfers is the freedom of disposition.[18] Accordingly, "[p]roperty owners have the nearly unrestricted right to dispose of their property as they please."[19] One way that property owners dispose of their property after death is through a will. A will is a donative document that lays out a testator's estate plan in detail, which "transfers property at death, amends, supplements, or revokes a prior will, appoints an executor, nominates a guardian, exercises a testamentary power of appointment, or excludes or limits the right of an individual or class to succeed to property of the decedent passing by intestate succession."[20] In order to create a will that is valid within a particular state, a testator must comply with the will act formalities prescribed by that state.

Every state has enacted will act formalities, which are rules that govern the validity of attested wills, notarized wills, and holographic wills.[21] While all states accept attested wills, various states differ on whether they accept notarized wills and holographic wills.[22] Attested wills may be either handwritten or typewritten, but they are always witnessed.[23] States also differ on the how strictly the will act formalities must be followed.[24] However, the core formalities that are generally accepted for crafting an attested will are the writing, signature, and attestation requirements.[25] To satisfy the attestation requirement of the will act formalities, states have required the witnesses to be present in either one of two ways during the will execution. Some states require the witness to be within the testator's "line of sight" while others take a more

18. RESTATEMENT (THIRD) OF PROP.: WILLS & OTHER DONATIVE TRANSFERS § 10.1 cmt. a (AM. LAW INST. 2003).

19. *Id.*

20. *Id.* at § 3.1 cmt. a.

21. ROBERT H. SITKOFF & JESSE DUKEMINIER, WILLS, TRUSTS, AND ESTATES 142 (Wolters Kluwer, 10th ed. 2017).

22. *See, e.g.*, *In re* Kimmel's Estate, 123 A. 405 (Pa. 1924); *In re* Estate of Gonzalez, 855 A.2d 1146 (Me. 2004).

23. It is important to note the distinction between a handwritten will that was attested and a holographic will, which is a will that was handwritten and not attested.

24. Florida is a strict compliance state, requiring the will to be in writing, signed, and attested by two witnesses. FLA. STAT. § 732.502 (2019).

25. SITKOFF & DUKEMINIER, *supra* note 21, at 142.

relaxed stance, requiring only that the witness be within the testator's "conscious presence."[26]

The function of these formalities is to permit a court, absent the live testimony of the deceased testator, to easily and reliably assess whether the purported will is authentic and the true testamentary wishes of the decedent.[27] Accordingly, these formalities serve what are routinely referred to as the evidentiary, channeling, cautionary, and protective functions (hereinafter "The Four Functions").[28]

The evidentiary function of the will act formalities provides a court with reliable evidence of the testator's intent to dispose of his assets by will. The writing, signature, and attestation requirements all serve to satisfy the evidentiary function. By requiring the will to be "in writing," the state ensures "evidence of testamentary intent will be cast in reliable and permanent form."[29] The requirement that the will be signed at the end provides evidence of authenticity and also prevents the will from being subsequently altered.[30] The attestation requirement provides evidence that the actual signing of the will was witnessed by disinterested spectators.[31]

The channeling function of the writing, signature, and attestation formalities ensures uniformity in the "organization, language, and content of most wills."[32] As a society, we value this uniformity because it lowers the cost of judicial administration and ultimately benefits the estate and its beneficiaries with lower court costs.[33] Thus, when the formalities are routinely followed, courts do not have to guess whether a document was meant to be a will.

The cautionary function of the will act formalities impresses upon the testator the seriousness of adopting an instrument as his last will and testament. The writing and signature formalities serve this function. Since wills are ambulatory and only take effect at the death of the testator, a testator does not give up any incidents of ownership at the time he drafts a will. Thus, we require the document to be in writing and signed to mitigate against the risk that the document is only a "preliminary draft,

---

26. To satisfy a "line of sight" requirement, a testator need not have seen the witnesses sign, but rather, they need only to have been able to see the witnesses were they to look. *Id.* at 152. The testator must be able to see the witnesses without changing positions. *Id.* To satisfy a "conscious presence" requirement, a testator need not have seen the witnesses sign, but rather, they need only be able to see the witnesses were they to look. *Id*. Skype and other video conferences would probably not satisfy the conscious presence requirement or the line of sight requirement.

27. SITKOFF & DUKEMINIER, *supra* note 21, at 141.

28. *Id.* at 144–45.

29. *Id.* at 145.

30. *Id.*

31. *Id.*

32. *Id.*

33. *Id.*

an incomplete disposition, or [the result of] haphazard scribbling."[34] Many times we say or write things we don't intend to have a lasting effect. However, when we are required to write and sign the document we intend to be a will, we are cautioned that our words have legal significance and will take effect at death.

Lastly, the will act formality of attestation serves to protect the testator from disposing his property via a document he does not intend to be his will. The presence of disinterested bystanders when the will is signed helps to "protect" against the substitution and probate of a fraudulent document purported to be a will. These bystanders may be called upon by a court to testify about the circumstances that took place at the time the will was signed and to the will's overall validity.

The will acts of each state are generally classified into three categories based on the level of compliance required for an attested will to be valid: strict compliance, substantial compliance, or harmless error. Strict compliance states require all of the will act formalities of: (1) writing, (2) signature, and (3) attestation to be present or else the purported will fails.[35] States that follow substantial compliance have excused or corrected one or more innocuous defects in the will execution when The Four Functions have otherwise been satisfied.[36] Put simply, the will meets The Four Functions but there was a mistake in the formalities.

Courts that follow substantial compliance require clear and convincing evidence that the testator intended the document to be his will and the will *substantially* complies with the will act formalities.[37] These courts have opined that substantial compliance effectuated testator intent when literal compliance with the statutory formalities would have invalidated a will that was the deliberate and voluntary act of the testator.[38]

The last category, harmless error, was drafted by the uniform probate code and has been adopted by statute in only a handful of states.[39] Known as a dispensing power, harmless error allows a court to excuse noncompliance with the state's will act formalities if there is clear and

---

34. *Id.*

35. *Id.* at 146.

36. *Id.* at 170.

37. *See, e.g.*, *In re* Will of Ranney, 589 A.2d 1339, 1341–42 (N.J. 1991) (Admitting the will to probate even though the witnesses signed in the wrong location); *In re* Snide, 418 N.E.2d 656, 657–58 (N.Y. 1981) (holding that the decedent's will was valid because the instrument in question was undoubtedly genuine and executed in the manner required by the state, despite the fact that the decedent and his wife each executed by mistake the will intended for the other).

38. *Ranney*, 589 A.2d at 1344.

39. UNIF. PROB. CODE § 2-706 (UNIF. LAW COMM'N 1990, as amended 1997); *In re* Estate of Hall, 51 P.3d 1134, 1135 (Mont. 2002); *Ready or Not, Here They Come: Electronic Wills Are Coming to a Probate Court Near You*, 33 PROB. & PROP. 5 (Oct. 2019) (stating that 11 states have adopted the harmless error rule by statute).

convincing evidence that the decedent intended the document or writing to be his will.[40] States that have a harmless error statute allow courts to essentially ignore the will act formalities of that state if the proponent of the will can prove the document was intended to be a will.

Florida is a strict compliance state without a harmless error statute.[41] In addition, Florida has historically required wills to be attested in the testator's conscious presence.[42] To date, the author is not aware of any Florida courts that have admitted a will to probate under either the substantial compliance or harmless error doctrines.

II. WHAT IS AN ELECTRONIC WILL?

Until recently, the term "Electronic Will" was ambiguous and generally referred to a multitude of situations posing very distinctive questions about validity. While legislators, scholars, and practitioners have proposed ideas to address issues related to the rise of "electronic wills," the creation of a bright line rule to be adopted by the states has been difficult because the term "electronic will" could mean so many different things.[43] However, the "one-size-fits-all term 'electronic will'" may now be broken down into three categories: (1) offline electronic wills; (2) online electronic wills; and (3) qualified custodian electronic wills.[44]

Offline electronic wills are typically typed or handwritten by stylus onto an electronic device by the testator.[45] They are signed by the testator typing his name or putting a signatory mark into the document and then saved to the electronic device's hard drive.[46] They are not printed, attested, or uploaded to the internet.[47] They are most easily analogized to traditional holographic wills. Online electronic wills are drafted similarly by the testator, except they are uploaded by the testator to a third party, private actor via the internet.[48] These third parties do not intend for their services to be utilized for the storing and preservation of testamentary documents, yet testators view them as an outlet to upload testamentary

40. *Id.*

41. FLA. STAT. § 732.502, (2019).

42. Vignes v. Weiskopf, 42 So. 2d 84 (Fla. 1949); 75 A.L.R.2d 318 (originally published in 1961).

43. *Developments in the Law — More Data, More Problems*, s*upra* note 7, at 1791 ("As used today, an electronic will could mean any writing along a broad spectrum from a will simply typed into a word-processing program by the testator on the computer and stored on its hard drive to a will signed by the testator with an authenticated digital signature, witnessed or notarized via webcam, and stored by a for-profit company.").

44. *Id.* at 1791–92.

45. *Id.* at 1792.

46. *Id.*

47. *Id.* at 1796.

48. *Id.*

documents.[49] Online electronic wills are also usually not printed or witnessed. An example of an online electronic will would be a testator typing and uploading his testamentary wishes to a Facebook post. Facebook does not intend to be used as an outlet for creating and storing testamentary instruments, however the testator has utilized it to do just that. Lastly, qualified custodian electronic wills involve a company that intends to be a "qualified custodian," charged with the creation, execution, and preservation of the testator's will.[50] Qualified custodians are governed by specific rules and regulations set forth by state legislatures.[51] Qualified custodians perform online will execution ceremonies where the testator may sign the will and have it witnessed via webcam.[52]

Currently, all three types of electronic wills would likely not be admitted to probate in a Florida court. However, the Florida's electronic wills act, HB 409, changes that. The Florida electronic wills act, taking effect on June 1, 2020, is intended to validate qualified custodian wills and gives Florida courts the green light to begin admitting them to probate in 2020.[53]

III. WHAT ARE THE "FUNCTIONAL" ISSUES RELATED TO EACH TYPE OF ELECTRONIC WILL?

Each type of electronic will carries its own unique evidentiary and validity issues that potentially compromise The Four Functions of the traditional will act formalities. Consequently, lawmakers addressing the rise of electronic wills need to be aware that a bright line rule will not cover each electronic will category, and states have to decide the level of leniency to apply to each purported electronic will.[54]

The primary "functional" issues related to offline electronic wills are evidentiary. Offline electronic wills lack sufficient evidence to determine their authenticity. Arguably, they are the category of electronic wills most susceptible to fraud and obsolescence. Since the testator would likely create an offline electronic will in the comfort of his home on his computer, the document lacks protective safeguards as it is prone to undue influence, inadvertent deletion, and could even be edited or drafted

49. *See id.* at 1803. Dropbox and other cloud computing services are regulated by statutes governing the preservation of personal data. *Id.* They also have terms and agreements limiting their retention of stored data over a period of time. *Id*.

50. *Id.* at 1792; *see, e.g.*, WILLING, https://willing.com (last visited May 22, 2020).

51. *Developments in the Law — More Data, More Problems*, *supra* note 7, at 1808.

52. *Id.* at 1806.

53. H.B. 409, 121st Reg. Sess. (Fla. 2019).

54. That is, the state must decide whether it wants to apply the traditional will act formalities of writing, signature, and attestation or other doctrines such as substantial compliance and harmless error.

by some other person with access to the same computer. Without a witness present when the will is drafted, the testator is left unprotected by the evidentiary safeguard of someone whose live testimony would authenticate the will execution. Furthermore, a computerized document can always be edited and resaved, leaving a court without the ability of knowing if the purported will was an original copy or even a final product. While computerized documents do contain metadata, a court would require a tremendous amount of time and effort sifting through the metadata to determine the originality, finality, and drafter of the document. Even if a court chose to expend such effort, the metadata still cannot convey the testator's mental capacity or show the presence of someone unduly influencing the testator when the document was drafted. For example, it will not show whether the testator was forced to draft the will at gunpoint. Consequently, even in a jurisdiction with the most lenient of the three levels of will compliance, harmless error, a court would likely have trouble finding clear and convincing evidence that the testator intended an offline electronic will to be his last will and testament.[55]

Offline electronic wills also do not sufficiently comply with the cautionary and channeling functions. It is very easy for anyone to pull up a blank document and start typing wishes without any forethought or serious contemplation. Someone in a temporary quibble with a family member could, in the heat of the moment, disinherit the family member in a computer document, save it to the hard drive, and die the next day. Theoretically, that document would be probated and have monumental, lasting effects the testator would never have fathomed in such a short period of time. In contrast, the cautionary safeguards supplied by the traditional signature and attestation requirements would likely remind the testator of the serious, drastic, and long-lasting effects that disinheriting a family member can have.[56] Furthermore, offline electronic wills would probably have to be considered on a case by case basis. Unless the testator used a standardized form with the usual testamentary jargon and legalese, the document would be in the testator's own vocabulary and would require the court to determine if the document was just an ordinary, non-

55. *See* Mahlo v. Hehir, [2011] QSC 243 (19 Aug. 2011) (Austl.), https://www.queensland judgments.com.au/case/id/74284 (refusing to admit an offline electronic file entitled "This is the last will and testament of Karen Lee Mahlo" to probate when testator's father testified that the testator had previously handed him a printed and signed paper copy of the electronic document). *But see* Yazbek v. Yazbek, [2012] NSWSC 594 (01 June 2012) (Austl.), https://www.caselaw .nsw.gov.au/decision/54a637ad3004de94513d9a45 (admitting an offline electronic file entitled "Will.doc" to probate when the testator mentioned he had a will saved on his computer and the court, after analyzing the metadata associated with the document, determined that the document had not been altered).

56. This is known as the "Wrench of Delivery." *E.g.*, SITKOFF & DUKEMINIER, *supra* note 21, at 145.

testamentary communication or a will.[57] This defeats the channeling function of the will act formalities.

Online electronic wills, on the other hand, potentially satisfy the evidentiary function to a greater extent than offline electronic wills. Since an inadvertent, neutral third party is added to the mix, the proponent of an online electronic will may be able to introduce evidence of authenticity stored by the third party. However, this data is likely subject to the Terms and Conditions agreement between the testator and the third-party service provider. Depending on the service provider, the Terms and Conditions agreement may limit the retention period for documents stored on its servers. For example, if the testator drafts a will and uploads it to a site like Dropbox, Dropbox might delete the document after the testator has not paid his or her service fees or the document has not been accessed for several years. In either situation, the service provider might not be under an obligation to continue retaining the document on its servers. Thus, should a probate court consider the testator to have had constructive notice of the will's deletion from the Terms and Condition agreement, giving rise to presumption of revocation?[58] Or should the probate court accept extrinsic evidence to reconstruct what would be a validly executed lost will?[59] Even if the third-party servicer has not deleted the will or its metadata, it is still the owner of that information. Accordingly, the company may rightfully refuse to share any of this information, making it essentially impossible for the will proponent to authenticate the online electronic will.

In order to combat the issue of executors being unable to obtain access to a decedent's digital property stored on third-party servers, a majority of states have adopted the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA). While the act allows executors to manage the decedent's digital property, they may only access the decedent's electronic communications if the decedent consented to such access in a will or other document.[60] If the document that authorizes the executor to access the testator's online electronic will is the online electronic will itself, a court might refuse to enforce the protections provided by the RUFADAA.

The channeling, cautionary, and protective functional vulnerabilities that are associated with offline electronic wills are similarly applicable to online electronic wills. Someone can still hold a gun to the testator's head and pressure him to draft a will on the testator's social media account. The testator can also upload a will with language that departs from the traditional testamentary language that supports the channeling function.

57. *Developments in the Law — More Data, More Problems*, *supra* note 7, at 1798.
58. *Id.* at 1803.
59. *Id.*
60. REVISED UNIF. FIDUCIARY ACCESS TO DIG. ASSETS ACT § 7 (UNIF. LAW COMM'N 2015).

However, online electronic wills may be even less supportive of the cautionary function because social media postings and emails tend to be associated with day to day expressions that are less serious in nature.

Of the three types of electronic wills, qualified custodian wills support the evidentiary function the most. Qualified custodians are engaged to assemble evidence of testamentary intent that substantiates will authenticity and to preserve the will in its original form on an online platform. Qualified custodians are able to do this by recording will execution ceremonies and ensuring that the will is accessible in the future.[61] However, the potential evidentiary risks of a data breach, inadvertent obsolescence, or deletion of the electronic will record do remain. By conducting online will execution ceremonies, similar to traditional will execution ceremonies, qualified custodians are also able to satisfy the cautionary function. Testators can enjoy the same "wrench of delivery" as they would during a traditional will execution.[62] Additionally, qualified custodians are likely to provide their testator clients with standardized forms that incorporate common testamentary language to satisfy the channeling function.

However, despite the qualified custodian's ability to satisfy the evidentiary, cautionary, and channeling functions by performing online will execution ceremonies, protective "functional" issues still remain. The testator is still able to be unduly influenced or coerced by a party standing outside the frame of the video recording device. The qualified custodian might also not have proper guidelines in place to authenticate the identity of the testator. Without a qualified custodian having personal knowledge of the testator's mental capacity or what the testator looks and sounds like, a third person could fraudulently misrepresent themselves as the testator and execute the will. In an era where software such as Photoshop exists to enhance and alter still photographs and video recordings, the possibilities for video fraud are endless.[63]

---

61. However, if the qualified custodian goes out of business or suffers a data breach, the will would be prone to obsolescence and/or deletion similar to online electronic wills. This potential issue would leave the evidentiary function unsatisfied.

62. SITKOFF & DUKEMINIER, *supra* note 21, at 145.

63. *See generally What Happens When Photoshop Goes Too Far?*, PBS NEWSHOUR (July 26, 2015), https://www.pbs.org/newshour/show/now-see-exhibit-chronicles-manipulated-news-photos#audio.

IV. HOW HAVE LAWMAKERS AND COURTS ADDRESSED ELECTRONIC WILLS?

Scholars discussing the probate of electronic wills in the United States usually begin with *In re: Estate of Castro*.[64] The Ohio Court of Common Pleas, Probate Division, admitted a will to probate that was drafted by the testator's brother on a Samsung Galaxy Tablet.[65] The testator, who was dying in the hospital, signed the will on the tablet followed by two witnesses who were present throughout the will execution. The court analyzed three questions: (1) was the electronically drafted will a "writing" under the applicable Ohio statute; (2) did the testator's electronic signature on the tablet satisfy the Ohio statute "signature" requirement; and (3) was there sufficient evidence to prove the tablet contained the last will and testament of the testator.[66] The court found clear and convincing evidence, via multiple witnesses (two of whom were present during the will's execution), that the tablet contained the testator's last will and testament and it held the will valid under Ohio's harmless error statute. While the court validated the will under Ohio's harmless error statute, its analysis suggests that the will would have also been valid under Ohio's traditional will act formalities had it not been in an offline electronic format. This case suggests that just the electronic nature of the will's medium could create a plethora of outcomes across courts in the United States due to the varying degrees of strict compliance, substantial compliance, and harmless error adopted by U.S. courts.

More recently in 2018, the Michigan Court of Appeals admitted an online electronic will to probate via Michigan's harmless error statute.[67] Prior to committing suicide, the testator handwrote a note in his journal stating that his "final note, my farewell" was saved on his phone.[68] The "final note" was a typed document that existed only in electronic form on a note-taking phone application called Evernote.[69] The Evernote document was login and password protected, and both credentials were provided in the handwritten journal entry.[70] In addition to apologies, personal sentiments, religious comments, funeral requests, and "self-deprecating comments," the note contained directions on how the

64. *E.g.*, *Ready or Not, Here They Come: Electronic Wills Are Coming to a Probate Court Near You*, *supra* note 39; *Developments in the Law — More Data, More Problems*, *supra* note 7, at 1800.

65. *In re* Estate of Castro, No. 2013ES00140, 2013 WL 12411558, at *1 (Ohio C.P. Lorain Cty. 2013).

66. *Id.* at 414.

67. *In re* Estate of Horton, 925 N.W.2d 207, 215 (Mich. Ct. App. 2018) (per curiam).

68. *Id.* at 209.

69. *Id.*

70. *Id*.

decedent wanted his property distributed after his death. The decedent specifically indicated in the note that he did not want any of his property to go to his mother, his only living heir if he died intestate.[71] While the note did not satisfy Michigan's traditional will act formalities or the less formal holographic will requirements,[72] the court nevertheless held that Michigan's harmless error statute was an "independent exception" regardless of whether the testator attempted to satisfy either of the formalities. The court ultimately found clear and convincing evidence of testamentary intent from the testator's apologies, explanations of his suicide, final farewells, and directions for the distribution of his property written in what would be considered an online electronic will.[73]

Courts outside of the United States have addressed more complex issues involving offline and online electronic wills with varying results. In *Macdonald v. The Master*, a South African court probated a document stored on the decedent's personal computer when the decedent left a handwritten note beside his bed stating, "I, Malcom Scott MacDonald, ID 5609065240106, do hereby declare that my last Will and testament can be found on my PC at IBM under directory C:/windows/mystuff/mywill/personal."[74] The court reasoned that the decedent was the only person who could have drafted the document, and therefore held that there was clear evidence the document was intended to be the testator's will.[75] However, in 2011, the Supreme Court of Queensland in *Mahlo v. Henhir*, refused to probate an offline electronic copy of the testator's will saved on her computer, reasoning that the testator had previously handed her father a printed, signed document she claimed to be her will and thus knew a valid will required more than "typ[ing] or modify[ing] a document on her computer."[76]

Just two years later, the Supreme Court of Queensland in *Re: Yu* probated an online electronic will beginning with the words "This is the last Will and Testament" that was saved on the testator's iPhone.[77] The Court reasoned there was evidence the decedent intended the document to be operative based on its creation shortly after a number of final farewell notes and its instructions for the distribution of his property.[78]

---

71. *Id*.

72. MICH. COMP. LAWS § 700.2502 (2019).

73. *In re Horton*, 925 N.W.2d at 214.

74. *Macdonald v. The Master*, 2002 (5) SA 64 (N) (S. Afr.).

75. *Id.* South Africa has a harmless error statute. *See* Scott S. Boddery, *Electronic Wills: Drawing a Line in the Sand Against Their Validity*, 47 REAL PROP. TR. & EST. L.J. 197, 204–05 (2012).

76. *Mahlo v. Hehir*, [2011] QSC 243 (19 Aug. 2011) (Austl.).

77. *Re: Yu* [2013] QSC 322 (6 Nov. 2013) (Austl.).

78. *Id.* Australia has a harmless error statute. John H. Langbein, *Excusing Harmless Errors in the Execution of Wills: A Report on Australia's Tranquil Revolution in Probate Law*, 87 COLUM. L. REV. 1, 1 (1987).

Then again in 2017, the Court held similarly when an unsent text message containing a series of property dispositions and the testator's typed initials and date of birth was admitted to probate.[79]

It is important to note that neither Ohio nor Michigan has adopted an electronic wills statute addressing the aforementioned issues related to offline and online electronic wills. The U.S. courts and the international courts relied on harmless error statutes to admit the electronic wills to probate. Accordingly, if a state has a harmless error statute, it is possible that a court in that state would admit an offline or online electronic will to probate. However, without a harmless error statute or a statute that specifically addresses electronic will, it is unlikely that a state court would probate any of the aforementioned offline or online electronic wills. That being said, legal scholars and legislatures have taken steps to draft and enact electronic wills statutes that would validate qualified custodian wills.

Currently, four states and the Uniform Law Commission have passed electronic wills statutes. Nevada passed the first electronic wills statute in 2001, authorizing testators to draft wills via an electronic record maintained by the testator or a qualified custodian and to execute the will with a digital signature.[80] The next state to pass an electronic wills statute was Indiana in 2018.[81] The Indiana statute authorizes testators to draft wills using electronic records, electronic signatures, and it specifically addresses qualified custodian wills.[82] However, the Indiana statute prohibits the use of remote witnessing by expressly requiring the testator and the attesting witnesses to be in the same physical locations as one another.[83] Arizona's electronic wills statute that went into effect on July 1, 2019, similarly provides for electronic signatures and storage by qualified custodians but also does not allow for remote witnessing.[84] Florida is the fourth state to enact an electronic wills statute that goes into effect June 1, 2020.[85] However, unlike Indiana and Arizona, Florida's law takes a more liberal stance and does allow remote witnessing.[86] A discussion of Florida's legislation shortly follows.

---

79. *See Nichol v. Nichol*, [2017] QSC 220 (9 Oct. 2017) (Austl.) (reasoning that the text message, which was an online electronic will, showed clear testamentary intent).

80. S.B. 33, 2001 Leg., 71st Sess. (Nev. 2001). The Nevada legislature made several amendments in 2017, including specific provisions for qualified custodian wills, electronic signatures, and methods of authenticating the testator. *See* NEV. REV. STAT. §§ 133.085–.086 (2019).

81. IND. CODE § 29-1-21-1 (2019).

82. IND. CODE § 29-1-21-10 (2019).

83. IND. CODE §§ 29-1-21-3(1), -4(a) (2019).

84. ARIZ. REV. STAT. ANN. § 14-2518 (2019).

85. H.B. 409, 121st Reg. Sess. (Fla. 2019).

86. *Id.*

The Uniform Law Commission approved the Uniform Electronic Wills Act in July 2019, providing a statutory template for states to authorize wills that are electronically drafted, electronically signed, remotely witnessed, and stored in the cloud.[87] Since 2000, the Uniform Electronic Transactions Act (UETA) and the federal E-SIGN law have provided that "a transaction is not invalid solely because the terms of a contract are in an electronic format." However, both UETA and E-SIGN expressly excluded wills from their purview, acknowledging the traditional will act formalities that usually require paper and pen. Members of the drafting committee rationalized that it was time to bridge the gap in UETA by allowing testators to execute a will electronically, while maintaining the protections available for traditional wills.[88] The Uniform Law Commission also incorporated the harmless error concept into its Electronic Wills Act. However, as mentioned earlier, only eleven states follow the harmless error rule,[89] and it remains to be seen how receptive states will be to the Uniform Law Commission's attempt at a universal electronic wills statute.

V. FLORIDA'S RESPONSE TO ELECTRONIC WILLS, HB 409

Florida's first attempt at an electronic wills statute took place in May 2017.[90] HB 277 passed the Florida legislature, but was vetoed by Florida's then-acting Governor, Rick Scott, on June 26, 2017.[91] HB 277 kept Florida's standard two-witness requirement but would have allowed the testator and witnesses to sign the will electronically via videoconferencing technology. In his veto letter, Governor Scott stated that HB 277 did not strike "the right balance between providing safeguards to protect the will-making process from exploitation and fraud while also incorporating technological options that make wills financially accessible."[92] In support of his veto, Governor Scott stated that the bill (1) failed to ensure the identity of the parties involved in the will execution; (2) allowed nonresidents of Florida to overburden Florida Probate courts by bringing their wills into Florida; and (3) would benefit

87. UNIF. LAW COMM'N, UNIFORM ELECTRONIC WILLS ACT (2019), https://www.uniformlaws.org/committees/community-home?CommunityKey=a0a16f19-97a8-4f86-afc1-b1c0e051fc71.

88. *Ready or Not, Here They Come: Electronic Wills Are Coming to a Probate Court Near You*, *supra* note 39, at 62. The committee believed that requiring the will (1) to exist in electronic text while being signed and (2) to be witnessed, either physically or virtually in the testator's presence, was enough to retain the traditional will act formalities.

89. *Id.* at 63.

90. Dan DeNicuolo, *The Future of Electronic Wills*, 38 BIFOCAL 75, 76 (2017), *available at* https://www.americanbar.org/groups/law_aging/publications/bifocal/vol_38/issue-5--june-2017/the-future-of-electronic-wills/.

91. *Id.*

92. *Id.*

from further revisions to the remote witnessing and notarization clauses.[93] Governor Scott encouraged legislators to reintroduce a revised bill during the next legislative session.[94]

Rather than heed the advice of Governor Scott or the Real Property, Probate and Trust Law Section of The Florida Bar,[95] lawmakers simply waited until the completion of his term, and on June 7, 2019, HB 409 was signed into law by Florida's incumbent governor, Ron DeSantis.[96] HB 409 authorizes the creation of electronic wills as well as the remote signing, remote notarization, and remote witnessing of estate planning documents.[97] To utilize remote witnessing, the testator must answer a series of questions regarding the testator's physical and mental condition to the satisfaction of an online notary that is remotely present, via audio/visual technology, during the will execution. However, in an attempt to alleviate concerns over the potential for undue influence and the lack of testamentary capacity of vulnerable adults, HB 409 prohibits remote witnessing when a "vulnerable adult" is the testator and requires witnesses to be physically present under such circumstances.[98] Section 415.102 of the Florida Statutes defines "vulnerable adult" broadly to include persons over the age of eighteen whose ability to perform normal activities or provide for his or her own care or protection is impaired due to a "mental, emotional, sensory, long-term physical, or developmental disability or dysfunction, or brain damage, or the infirmities of aging."[99] HB 409 also elicits the use of a qualified custodian for testators that wish to have their wills self-proved.[100]

Florida defines a qualified custodian, under the new § 732.524, as someone domiciled, incorporated, organized or residing in Florida who regularly employs a secure system to secure the electronic records of electronic wills.[101] Qualified custodians may only provide access to the testator, persons authorized by the testator in a will, the personal representative of the testator's estate, or the court. The qualified custodian is required to hold onto the electronic records of the testator's will for the lesser of five years from the conclusion of probate or 20 years after the

93. *Id.*

94. *Id.*

95. *See* REAL PROP., PROB. & TR. LAW SECTION OF THE FLA. BAR, WHITE PAPER ON 2019 PROPOSED ENACTMENT OF THE FLORIDA ELECTRONIC WILLS ACT (2019).

96. H.B. 409, 121st Reg. Sess. (Fla. 2019).

97. *Id.*

98. FLA. S. JUDICIARY COMM., *BILL SUMMARY CS/CS/HB 409 — ELECTRONIC LEGAL DOCUMENTS 1*, https://www.flsenate.gov/PublishedContent/Session/2019/BillSummary/Judiciary_JU0409ju_0409.pdf (last visited Apr. 29, 2020).

99. FLA. STAT. § 415.102(28) (2019).

100. H.B. 409, 121st Reg. Sess. (Fla. 2019).

101. *Id.*

testator's death.[102] If a qualified custodian negligently fails to safeguard the electronic will or adequately execute its duties after the testator's death, the qualified custodian is statutorily liable for any damages and may not limit its liability for such damages.[103] Accordingly, to be recognized by the state of Florida as a qualified custodian, HB 409 also contains rules regarding the bond and insurance requirements that must be satisfied.[104]

VI. WHAT ARE THE "FUNCTIONAL" ISSUES WITH HB 409?

Florida courts have traditionally required strict compliance with Florida's will act formalities to have a will properly admitted to probate.[105] Consequently, holographic wills have been held invalid.[106] And without the benefit of a harmless error statute, testamentary documents that were clearly and convincingly intended to be the decedent's last will have not been probated in Florida. This strict stance encourages testators to seek out the help of an attorney to ensure that all testamentary documents are properly written, signed, and witnessed, and it promotes the "Four Functions" to the greatest extent possible.

With the enaction of HB 409, Florida has taken a significant departure from its traditional stance on will executions. Florida's prohibition of holographic wills does remain intact, continuing Florida's position that unattested offline and online electronic wills are invalid. The policy reasons for prohibiting unattested electronic wills, both online and offline, were noted previously: they are subject to an increased risk of fraud, undue influence, and lack sufficient evidence of authenticity and finality. However, with HB 409, Florida now accepts electronically drafted, signed, and witnessed wills, such as the will drafted in *In re: Estate of Castro*,[107] and also authorizes "robo-witnesses," "robo-notaries," and qualified custodian wills.[108]

There are many risks associated with the authorization of qualified custodian wills. As mentioned earlier, qualified custodian wills are subject to potential data breaches, inadvertent obsolescence, and deletion

---

102. *Id.*

103. *Id.*

104. *Id.*

105. *See, e.g.*, Allen v. Dalk, 826 So. 2d 245, 247 (Fla. 2002) ("A testator must strictly comply with [§ 732.502]'s statutory requirements in order to create a valid will."); *In re* Estate of Olson, 181 So. 2d 642, 643 (Fla. 1966) (reasoning that an unattested will should not be admitted to probate because strict compliance with the attestation requirement assures the will's authenticity and avoids fraud); *In re* Estate of Watkins, 75 So. 2d 194, 197–98 (Fla. 1954) (holding a will invalid where one of the two witnesses failed to sign the document).

106. *In re* Estate of Salathe, 703 So. 2d 1167, 1168 (Fla. Dist. Ct. App. 1997).

107. *In re* Estate of Castro, No. 2013ES00140, 2013 WL 12411558, 413–18 (Ohio C.P. Lorain Cty. 2013).

108. H.B. 409, 121st Reg. Sess. (Fla. 2019).

of the electronic will records. While HB 409 requires that a qualified custodian maintain a "secure system" for its electronic will records, it does not set forth any specific minimum storage and security standards. That being said, HB 409 does set out the minimum electronic records retention standards and the liability exposure of qualified custodians who fail to follow them. These protections alleviate some of the evidentiary functional concerns that are associated with qualified custodian wills. However, the authorization of remotely present robo-witnesses and robo-notaries severely jeopardizes the protective function that strict compliance previously served.

A testator wishing to utilize remote witnessing must have an online notary present during the will execution ceremony. Pursuant to the newly created § 117.265 of the Florida Statutes, the online notary will confirm the identity of the testator and the witnesses by either personal knowledge of each individual or by: (1) remote presentation of a government ID; (2) credential analysis of each government issued ID; and (3) identity proofing each individual in the form of a knowledge-based identification.[109] The testator will then answer a series of questions related to his capacity to the satisfaction of the online notary. Unfortunately, these procedures do not provide sufficient protections against fraud, identity theft, undue influence, and lack of testamentary capacity. Someone attempting to impersonate the purported testator could show the camera a fake ID with the imposter's photograph on it or even try to alter his appearance to look like the purported testator. In addition, an undue influencer could be standing just outside the frame of the video camera, unbeknownst to the witnesses and notary. Should a subsequent action for undue influence arise, the electronic record would provide little to no indicia of undue influence. The robo-notary and robo-witnesses would likely not know who drafted the will, who else was present when the will was signed, or at what location the will was signed. The author suggests that an in-person identity proofing process prior to the will execution would be a substantial improvement to simply requiring that testators and witnesses hold their ID's up to the video camera. It would also provide the notary and witnesses with the same indicia of undue influence that would be present during a traditional will execution.

Despite its best efforts to protect those who are deemed the most susceptible to undue influence and a lack of testamentary capacity, Florida's "vulnerable adult" exception to remote witnessing is overbroad and will likely lead to an increase in will contests. The exploitation statutes define "vulnerable adult" to include a wide range of people, including those whose abilities to perform normal activities or care for themselves are impaired due to the "infirmities of aging." The statute

109. H.B. 409, 121st Reg. Sess. (Fla. 2019).

does not define what constitutes "normal activities" or the "infirmities of aging." Thus, any determination that a testator is a "vulnerable adult," incapable of remote witnessing, is entirely subjective, and must be decided by either the testator himself, the online notary, or the remote witnesses.

Unless the testator reads the exploitation statutes himself and then finds himself to lack the mental capacity and ability to perform "normal activities" required to execute an online will, he is not likely to object on his own to remote witnessing. It was either his decision or an undue influencer's decision to use remote witnessing in the first place. This leaves the online notary or the remote witnesses with the decision of whether the testator is a "vulnerable adult"; individuals who are not in the same room as the testator and may have never met him. In the event that the testator was in fact a "vulnerable adult" and the online notary or remote witnesses were none the wiser, we end up with an executed will that likely would not have been valid in a traditional, in-person setting. In a traditional will execution setting, the drafting attorney, notary, and witnesses—who are more likely to have a longstanding relationship with the testator—would be able to determine the testator's diminished mental capacity and the presence of an undue influencer.

As a result of HB 409, will contestants seeking to invalidate a will that was remotely witnessed have new grounds to claim that the testator was a "vulnerable adult." But for the remote witnessing, the testator would not have been able to execute the purported will. A probate court hearing such a claim will have to look at the video record, hear the testimony from the robo-witnesses and notary, and determine for itself whether the testator was of sound mind and free from undue influence. However, the video will contain nothing more than what the robo-notary and robo-witnesses saw for themselves and decided was not indicative of "vulnerable adult" status.

CONCLUSION

It remains to be seen whether Florida's electronic wills statute will be problematic. Despite Florida's enaction of HB 409, testators are still free to execute their wills by consulting an attorney and using the traditional will act formalities. Testators with substantially large estates exceeding the current estate and gift tax exemption of $11,400,000[110] are not likely to be affected HB 409. It is expected that these individuals will continue consulting tax attorneys for estate planning advice. In addition, testators with an estate less than the estate tax exemption who wish to make use of a revocable trust with a pour-over will are also not likely to be affected by HB 409. Both documents are usually drafted by an attorney and then

110. Rev. Proc. 2018-57.

traditionally executed at the attorney's office. Thus, it may take years before a Florida probate court is forced to admit a remotely witnessed, electronic will. Only then will we see if, and to what extent, Florida's electronic wills act fails to serve The Four Functions.