Note

Volunteering to Deceive: Criminalizing Citizen-Group Espionage

Andrew Frohlich*

Table of Contents

* J.D., expected May 2010, The George Washington University Law School; B.A., 2007, University of Michigan. I would like to thank Brooke McDonough and Robert Alfred for their help and wise counsel in developing this Note, as well as Scott Pollock and *The George Washington Law Review* staff for their outstanding editorial work. I am also eternally grateful to my family and friends for their tireless encouragement and support.

Introduction: A Tale of Two Marys

By 2008, Mary McFate had spent more than a decade as an energetic crusader devoted to the gun-control movement.[1] Actively involved in multiple gun-control organizations, McFate's zealous commitment to gun-violence prevention propelled her rapid ascent to national prominence in the antigun violence community,[2] and she was named to the boards of two gun-control groups: CeaseFire PA[3] and Freedom States Alliance.[4] For another group, States United to Prevent Gun Violence, McFate led the organization's lobbying arm as the director of federal legislation.[5] According to one leading figure of the gun-control movement, she was "active in everything and involved in every single major gun violence prevention organization."[6]

In July 2008, an investigation by *Mother Jones* magazine revealed a startling secret: the Mary McFate known to the gun-violence prevention community was in reality Mary Lou Sapone, a freelance spy tasked to infiltrate the antigun movement.[7] Sapone was subcontracted by the National Rifle Association ("NRA") to penetrate gun-control groups and deliver their nonpublic information back to the NRA.[8]

---

1 *See* James Ridgeway, Daniel Schulman & David Corn, *There's Something About Mary: Unmasking a Gun Lobby Mole*, MOTHER JONES, July 30, 2008, http://www.motherjones.com/politics/2008/07/theres-something-about-mary-unmasking-gun-lobby-mole.

2 *See id.*

3 *Id.* CeaseFire PA is a nonprofit gun-violence prevention organization. *See* CeaseFire PA, Membership and Contributions, http://ceasefirepa.org/donate (last visited Sept. 10, 2009).

4 *See* Ridgeway, Schulman & Corn, *supra* note 1. Freedom States Alliance is a nonprofit gun-violence prevention organization. *See* Freedom States Alliance, About Us, http://www.freedomstatesalliance.com/mission.php (last visited Sept. 10, 2009).

5 *See* Ridgeway, Schulman & Corn, *supra* note 1.

6 *Id.*

7 *See id.* For a list of other intelligence-gathering activities McFate engaged in, see Jenna Johnson, *Informant Might Have Stood Among Gun Safety Activists*, WASH. POST, Sept. 28, 2008, at C1, C7.

8 Johnson, *supra* note 7, at C7.

Through her infiltration of the gun-control movement, Sapone had access to a plethora of confidential information. As explained by one leader in the gun-control community, Sapone could learn

> what the grassroots of the gun violence prevention movement intended; where our priorities [were] shifting; which legislation we would be promoting or fighting against and what sort of effort we would be putting into that; who our targeted legislators would be; what states and districts we deemed were important enough to put an effort into; . . . [and] what our messaging would be before we put it out there.[9]

In short, Sapone "had access to all the legislative strategy for every major issue for years."[10] This information, if delivered to the NRA, could have had a devastating effect on the agenda of the antigun community—a community that had placed its faith in the woman they knew as Mary McFate.[11]

The McFate/Sapone saga is not a mere isolated incident, but rather a misstep that has thrust into the public light an industry about which little is publicly known: citizen-group espionage.[12] Corporations—and occasionally rival nonprofit organizations—sometimes seek an unfair advantage in the debate of ideas by using espionage to gain access to confidential information possessed by citizen groups.[13] Not only is this type of activity offensive to our fundamental democratic values of openness and fair play,[14] but it also poses a threat to the functioning of our nation's venerated "marketplace of ideas."[15] Nevertheless, because this information is noneconomic in nature, both federal and state laws fail to provide a satisfactory solution to citizen-group organizations that are targeted for espionage.[16]

---

9 *See* Ridgeway, Schulman & Corn, *supra* note 1.

10 *Id.* (quoting Kristen Rand, Legislative Director of the Violence Policy Center).

11 *See* Johnson, *supra* note 7, at C1, C7.

12 The term "citizen-group espionage," as used in this Note, refers to the theft by means of deception of confidential information possessed by "citizen groups." Furthermore, the term "citizen group," as used throughout this Note, refers to any organization whose primary purpose is peaceful activism, lobbying, or raising social awareness.

13 *See* Jenna Johnson, *Corporate Espionage Detailed in Documents: Defunct Md. Agency Targeted Activists*, WASH. POST, June 22, 2008, at C1; *infra* notes 19–22, 29–30 and accompanying text (discussing citizen-group espionage).

14 *See infra* notes 52–53 and accompanying text.

15 In his dissent in *Abrams v. United States*, 250 U.S. 616, 624–31 (1919) (Holmes, J., dissenting), Justice Holmes advanced the concept of a marketplace of ideas in which ideas are allowed to compete for public acceptance in an open, uninhibited market, *see id.* at 630; *infra* notes 33–34 and accompanying text.

16 *See infra* Part II.

Groups victimized by these dishonest practices should be provided the same legal protections that currently exist for corporations that suffer economic espionage. Accordingly, this Note presents a possible solution that would address the needs of vulnerable citizen groups: Congress should enact legislation criminalizing the theft of confidential information possessed by citizen groups by means of espionage. To that end, this Note proposes a Citizen-Group Espionage Act for Congress to enact.[17] Such protection would guarantee that citizen groups are not deterred from competing in the marketplace of ideas, would prevent actors from benefiting from their deceit, and would ensure that the choices presented to the public in the marketplace of ideas were produced freely and fairly.

This Note begins in Part I by providing background on the existence of citizen-group espionage as an underground industry. Part I further explains how citizen-group espionage poses a threat to the fundamental values and the functioning of a fair and open democracy. Part II examines why current law, including four potential causes of action—theft of trade secrets, the tort of breach of confidence, the tort of invasion of privacy, and fraud—does not offer a viable solution to citizen-group espionage. Finally, Part III proposes the Citizen-Group Espionage Act ("the Act") as a solution to the problem of citizen-group espionage. It first describes why it should be Congress that regulates citizen-group espionage; it then presents the proposed text of the Act accompanied by explanations of the provisions. This Note concludes by applying the Act to the McFate facts, illustrating the effectiveness of the proposed legislation in addressing citizen-group espionage.

I. The Existence of Citizen-Group Espionage and Its Incompatibility with Democratic Principles

Though the existence of citizen-group espionage was largely unknown to the general public, Mary McFate's brazen betrayal has brought to daylight a startling reality: instead of engaging in fair and open debate, some corporations and lobbying groups have employed tactics of espionage to undermine peaceful efforts by citizen groups.[18] This Part begins by detailing how the citizen-group espionage industry functions. It then explains that citizen-group espionage should not be tolerated because it is contrary to fundamental societal values. This

---

17 *See infra* Part III.

18 Johnson, *supra* note 13, at C1, C7.

Part then concludes by arguing that noneconomic information deserves the same protection society gives to economic information.

A. The Citizen-Group Espionage Industry

The McFate saga reveals the modus operandi of the entities behind the citizen-group espionage industry, and the responsibility of a shadowy network of sponsors of espionage, public relations firms, and private intelligence firms.[19] Sponsors, both corporate and nonprofit, may choose to resort to citizen-group espionage when, seeking a strategic or public relations advantage, they decide to forgo honest public debate and elect instead to undermine the citizen groups challenging them by means of espionage.[20] Public relations firms refer besieged clients to private intelligence groups holding expertise in espionage.[21] The private intelligence groups, using their own spies or by subcontracting freelance spies such as McFate, then use deception to infiltrate citizen groups, secure valuable confidential information, and deliver it to the sponsor.[22]

The activities of Beckett Brown International ("BBI"), a private intelligence consulting group referred by McFate to the NRA to infiltrate the gun violence prevention movement, offer a rare glimpse into the operation of the citizen-group espionage industry.[23] BBI's team of intelligence experts was comprised in part of former Secret Service and CIA agents.[24] Prior to the NRA project, BBI had engaged in numerous instances of espionage against peaceful citizen groups and nonprofit organizations on behalf of a variety of clients—both corporate and nonprofit.[25] Past targets of BBI included the environmental organizations Greenpeace and CLEAN,[26] food-safety organizations,[27]

---

19 *See id.*

20 *See id.*

21 *See id.* at C7.

22 *See* James Ridgeway, *Black Ops, Green Groups*, MOTHER JONES, Apr. 11, 2008, http://www.motherjones.com/print/15506; *see also* Johnson, *supra* note 13, at C1, C7.

23 After contracting with the NRA, BBI changed its name to S2i. *See* Ridgeway, *supra* note 22. The company has since disbanded. Johnson, *supra* note 13, at C1.

24 *See* Johnson, *supra* note 13, at C1; Ridgeway, *supra* note 22.

25 Johnson, *supra* note 13, at C1, C7; Ridgeway, *supra* note 22.

26 *See* Ridgeway, *supra* note 22; James Ridgeway, *Environmental Espionage: Inside a Chemical Company's Louisiana Spy Op*, MOTHER JONES, May 20, 2008, http://www.motherjones.com/environment/2008/05/environmental-espionage-inside-chemical-companys-louisiana-spy-op. CLEAN was a Louisiana-based advocacy group working with Greenpeace to publicize pollution caused by local industry. *See id.* Condea Vista, a chemical company responsible for a toxic chemical spill in Lake Charles, Louisiana, hired BBI to gather secret information on the strategies of CLEAN and Greenpeace. *See id.*

27 In 2000, food-safety groups launched a public campaign against Taco Bell restaurant

and even residents of Hebrew Home, a Maryland eldercare facility.[28] The diverse interests of these victim citizen groups demonstrate that, regardless of which issues they are championing, citizen groups challenging the status quo cannot be certain that they are beyond the threat of espionage.

The discovery of these infiltrations reveals the existence of a secret, multifaceted cottage industry involving for-hire operatives, private intelligence-gathering companies, and public relations firms. Although BBI is now defunct, the private intelligence industry is flourishing today.[29] Firms like Chesapeake Strategies Group, formed by one of BBI's former partners, currently offer "Competitive Intelligence" services, including "expertise in blocking or neutralizing special-interest campaigns . . . with proven investigative solutions."[30] Though data on the pervasiveness of the practice of espionage targeting citizen groups is currently unavailable,[31] the activities of McFate and companies like BBI make one thing apparent: when corporate or political interests are threatened by citizen-advocacy groups, they may be willing to turn to deception and espionage to head off any potential public harm.

B. Citizen-Group Espionage Is Antithetical to a Healthy Civil Society

The acquisition of the confidential information possessed by citizen organizations by means of deception and espionage is antithetical to a healthy civil society and the principles of American democracy. The harm that citizen-group espionage inflicts on society is threefold: (1) it undermines the core of the First Amendment, the "marketplace

---

following the revelation that the fast-food chain had served tacos with corn not approved for human consumption, causing the tacos to glow in the dark. Ridgeway, *supra* note 22. To control the potential damage, Taco Bell's owner, Kraft, hired public relations firm Ketchum, which in turn hired BBI (by then S2i). *See id.* The citizen groups BBI targeted included the Center for Food Safety, Friends of the Earth, and GE Food Alert. *See id.*

28 BBI targeted the residents of the eldercare facility by placing a spy in a meeting of residents' relatives who were concerned with the care being provided in the home. Johnson, *supra* note 13.

29 *Cf.* Arthur S. Hulnick, *Risky Business: Private Sector Intelligence in the United States*, 24 HARV. INT'L REV., Fall 2002, at 68, 70 (describing the recent push for businesses to employ private intelligence to obtain a competitive advantage).

30 Chesapeake Strategies Group, Competitive Intelligence, http://www.chesapeakegroup.net/competitiveIntelligence.php (last visited Sept. 10, 2009).

31 One possible explanation for the paucity of information on the pervasiveness of citizen-group espionage is that "corporations are typically insulated from such investigations by confidentiality agreements and multiple layers of subcontractors." *See* Johnson, *supra* note 13, at C7. Accordingly, *Mother Jones*'s obtainment of the BBI documents was exceedingly rare. *Id.*

of ideas," by stifling debate; (2) it offends common societal values of honesty and fair play; and (3) it unjustly allows the agents and sponsors of espionage to reap the rewards from their ill deeds.

First, citizen-group espionage undermines the functioning of our hallowed "marketplace of ideas." Justice Holmes explained the vital role the marketplace of ideas plays in the First Amendment right to free speech[32] in his famous dissent in *Abrams v. United States*:

> But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out. That at any rate is the theory of our Constitution.[33]

In the years since *Abrams*, Holmes's notion of a marketplace of ideas, where divergent opinions can fairly compete for public favor without restrictions, has come to be accepted as one of the fundamental pillars of the First Amendment right to political discourse, which is so vital to American democracy.[34]

Though the theory of the marketplace of ideas recognizes that the open exchange of ideas is at the core of the First Amendment, also essential to the functioning of the marketplace of ideas is the protection of information from external interference.[35] Professor Neil M. Richards calls this needed protection "intellectual privacy"—"the ability . . . to develop ideas and beliefs away from the unwanted gaze or interference of others."[36] The right to keep information from others ultimately enhances freedom of speech, because it affords refuge to develop original but perhaps disfavored ideas.[37] As Richards explains, "without the ability to speak with trusted confidants, we lack the ability to develop our own ideas in collaboration with others

---

32 U.S. CONST. amend. I.

33 Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).

34 *See* N.Y. State Bd. of Elections v. López Torres, 128 S. Ct. 791, 801 (2008) ("The First Amendment creates an open marketplace where ideas, most especially political ideas, may compete without government interference." (citing *Abrams*, 250 U.S. at 630 (Holmes, J., dissenting))).

35 *See* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 403 (2008).

36 *See id.* at 389.

37 *See id.* at 403.

before we are ready to share them publicly."[38] The right to keep an idea from others before it is finally ready to be tested in the marketplace of ideas can be an important component in the ultimate success of that idea.

This need to protect the right to keep information from others is recognized in another marketplace—the economic market. In this sense, the marketplace of ideas is parallel in its functioning to our economic markets. In the economic market, producers of goods seek to keep secret from their competitors certain pieces of information—strategy, designs, etc., otherwise known as trade secrets—in order to maintain their competitiveness.[39] Senator Specter spoke of this essential need to protect trade secrets to ensure that competition exists in the economic marketplace: "In an increasingly complex and competitive economic world, intellectual property forms a critical component of our economy. . . . [O]ur economic edge depends to an ever-increasing degree on the ability of our businesses and inventors to stay one step ahead of those in other countries."[40] In this spirit, Congress saw fit to protect the economic marketplace by criminalizing the theft of trade secrets through the Economic Espionage Act of 1996.[41]

Just as espionage undermines the functioning of the economic market, we should also recognize that theft of confidential but noneconomic information undermines the functional foundations of the marketplace of ideas. Protection of confidential information allows holders to control the manner in which their message is conveyed.[42] As one commentator explains, "[i]f we could not select our audience, that is, if the choice were only between keeping ideas to ourselves and sharing them with the world at large, many ideas would remain unexpressed, to the detriment of individual health as well as the general good."[43] To ensure that debate is not silenced—that citizens are not discouraged from sharing their ideas in the public forum—we should protect the ideas of citizen groups in the same manner that we protect the ideas of businesses.

---

38 *See id.* at 424.

39 *See* 142 CONG. REC. S12,207–08 (daily ed. Oct. 2, 1996) (statement of Sen. Specter).

40 *Id.*

41 Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–1839 (2006).

42 Lynn Sharp Payne, *Trade Secrets and the Justification of Intellectual Property: A Comment on Hettinger*, 20 PHIL. & PUB. AFF. 247, 251 (1991) ("If a person has any right with respect to her ideas, surely it is the right to control their initial disclosure. A person may decide to keep her ideas to herself, to disclose them to a select few, or to publish them widely. . . . The world at large has no right to an individual's ideas.").

43 *Id.* at 253.

Second, the same moral justifications behind the enactment of trade secret law—of promoting openness and fairness—apply regardless of whether the information obtained through deceptive means is economic, as in the case of economic espionage, or noneconomic, as in the case of citizen-group espionage. "The desire to reinforce 'good faith and honest, fair dealing' in business is the mother of the law of trade secrets."[44] Speaking to this same goal, in his letter to the NRA following the revelation of Mary Lou Sapone's deceipt, Senator Frank R. Lautenberg of New Jersey espoused the need for openness and fairness in public debate: "I hope that we can agree that the gun violence prevention debate should be based on an *open and honest exchange of ideas*, not on underhanded tactics."[45] Because the same social values of openness and honesty that underlie trade secret law apply to the marketplace of ideas, society should punish those who engage in espionage, regardless of whether the target is business information or strategic social information.

Third, permitting sponsors to engage in citizen-group espionage without punishment allows them to benefit from their deceit, a concept that is contrary to the general principle of unjust enrichment. One of the major moral justifications behind trade secret law is preventing unjust enrichment.[46] The use of punitive damages in trade secret law reaffirms society's condemnation of an actor's employment of improper means to better herself.[47] Just as the law does not allow a person to benefit from her wrongdoing in business,[48] it should prevent an entity from benefiting from the use of the same deceptive means

---

44 RUSSELL B. STEVENSON, JR., CORPORATIONS AND INFORMATION 19 (1980) (footnote omitted).

45 Letter from Senator Frank R. Lautenberg to John C. Sigler, President, Nat'l Rifle Ass'n (Aug. 7, 2008) (emphasis added), *available at* http://lautenberg.senate.gov/newsroom/record.cfm?id=301911&.

46 *See* James W. Hill, *Trade Secrets, Unjust Enrichment, and the Classification of Obligations*, 4 VA. J.L. & TECH. 2, ¶ 123 (1999), http://www.vjolt.net/vol4/issue/home_art2.html; *see also* Jules L. Coleman, *Intellectual Property and Corrective Justice*, 78 VA. L. REV. 283, 284 (1992) ("The principle of unjust enrichment posits that wrongly or unjustly secured gains must be annulled.").

47 *See* Hill, *supra* note 46, ¶¶ 80–95.

48 *See* RESTATEMENT (FIRST) OF RESTITUTION § 1 (1937) ("A person who has been unjustly enriched at the expense of another is required to make restitution to the other."); RESTATEMENT (SECOND) OF CONTRACTS § 370 (1981) ("A party is entitled to restitution . . . only to the extent that he has conferred a benefit on the other party by way of part performance or reliance."); RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 3 (Discussion Draft 2000) ("A person who interferes with the legally protected rights of another, acting without justification and in conscious disregard of the other's rights, is liable to the other for any profit realized by such interference.").

for a noneconomic end. Although the sponsors of citizen-group espionage may not realize an economic benefit, they undoubtedly expect to receive a strategic or informational benefit from their deceit.

The harm caused by citizen-group espionage to civil society, the very core of our democracy, should compel Congress to provide victim citizen groups with adequate legal protection. Currently, however, such legal protections do not exist.[49] As a possible solution, Congress should enact legislation criminalizing citizen-group espionage. Such legislation would serve as a just punishment for those actors who intentionally employ dishonest practices to target citizen groups, and afford targeted citizen groups with security in the knowledge that their right to participate in the marketplace of ideas will not be undermined.

C. Extending Regulation Beyond Economic Information

Proponents of small government may contend that the government should limit its regulation to the theft of economic information because the principal rationale behind trade secret law is to protect and promote business. According to this argument, there is no justification for criminalizing the theft of noneconomic information because harm is nonexistent when information without pecuniary value is misappropriated.

But in addition to the economic justification behind trade secret law, there are moral justifications.[50] Because trade secret law punishes those who unjustly enrich themselves,[51] it promotes the social value of honesty in competition.[52] As one commentator explains, "the prohibited means of acquisition—misrepresentation, theft, bribery, breach of confidence, and espionage—all reflect general social morality. Lifting these restrictions would undoubtedly contribute to the erosion of important values outside the commercial context."[53] Turning a blind eye to theft, bribery, breach of confidence, and espionage in noncommercial contexts contributes to the erosion of morality because it allows sponsors and agents to obtain information not belonging to them through deceptive means. Furthermore, punishing theft of economic information but declining to punish theft of noneconomic information denigrates the value of social ideas by sending a message

---

49 *See infra* Part II.

50 *See* Hill, *supra* note 46, ¶ 95; Payne, *supra* note 42, at 257.

51 *See* Hill, *supra* note 46, ¶ 95.

52 *See* Payne, *supra* note 42, at 257.

53 *Id.* at 258.

that the only ideas that matter are those that make money. Protection should extend to noneconomic ideas as well as those which have a pecuniary value to reaffirm that society values social thought as much as it values profit. Such protection would also reinforce society's disdain for deceptive means of acquisition and promote the open and honest exchange of thought that is the hallmark of the marketplace of ideas.[54]

II. The Inadequacies of Existing Law in Solving Citizen-Group Espionage

Although citizen-group espionage is incompatible with our democratic values,[55] this Part explains why current law fails to address the problem. In doing so, it focuses on four laws affecting the theft of information through espionage—trade secret law, the tort of breach of confidence, the tort of invasion of privacy, and the law of fraud—and explains why they lead to unsatisfactory outcomes when applied to citizen-group espionage.

A. The Inadequacies of Trade Secret Law

Trade secret law is, in part, designed to afford a holder of private information a remedy when involuntary disclosures of ideas occur so that they are not "regarded as forfeitures to the common pool of knowledge and information," whereby the holder has sacrificed the right to control its disclosure.[56] Yet trade secret law, in its various forms,[57] fails to provide an adequate remedy for victim citizen-group organizations because it requires that the information derive "*economic value*, actual or potential, from not being generally known" by competitors.[58] As this Part explains, the noneconomic nature of the information possessed by citizen groups, whose end product is not profit but instead social or political change, ensures that the misappropriation of their secret information by espionage does not fall under the umbrella of protection afforded by trade secret law.

---

54 *See supra* notes 33–48 and accompanying text.

55 *See supra* notes 33–35 and accompanying text.

56 *See* Payne, *supra* note 42, at 254.

57 This Note examines three different sources of trade secret law: RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939); the Uniform Trade Secrets Act, UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. 536, 538 (2005); and the Economic Espionage Act of 1996 § 101(a), 18 U.S.C. § 1839(3) (2006).

58 *See* UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. 536, 538 (2005) (emphasis added); *see also* 18 U.S.C. § 1839(3); RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

Trade secret law in the United States is a varied stew of state common law and state-enacted criminal and civil legislation.[59] Until recently, however, laws that punished the theft of trade secrets were almost exclusively products of the common law.[60] It was not until the American Bar Association approved the Uniform Trade Secrets Act ("UTSA") in 1979,[61] a model statute for states to adopt, that most states began enacting trade secret laws.[62] Today, the majority of states have enacted statutes modeled after the UTSA.[63] Although these state laws typically define the term "trade secret,"[64] courts, including the United States Supreme Court,[65] have consistently turned to the definition of "trade secret" in the *First Restatement of Torts*[66] ("*Restatement*") instead of the UTSA to inform their jurisprudence.[67]

The *Restatement* defines trade secret as "consist[ing] of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."[68] Under this definition of a trade secret as information conferring a competitive advantage on one's business, courts have confined the application of trade secret law to information that has economic value.[69] This interpretation is in keeping with the examples in the comments to the *Restatement* that illustrate what the drafters considered a trade secret: "It

---

59 *See generally* Hill, *supra* note 46, ¶¶ 12–15 (describing the development of trade secret law).

60 *See id.* ¶ 15.

61 The Uniform Trade Secrets Act was drafted by the National Conference of Commissioners on Uniform State Laws. *Id.* ¶ 13 n.34.

62 *See id.* ¶ 13.

63 As of 2009, forty-five states, the District of Columbia, and the Virgin Islands have enacted some form of the UTSA. *See* UNIF. TRADE SECRETS ACT, 14 U.L.A. 25–26 (Supp. 2009). These statutes typically provide for civil remedies such as injunctive relief, *see, e.g.*, CAL. CIV. CODE § 3426.2 (West 1998 & Supp. 2009) (preventing misappropriation and future use of trade secrets); VT. STAT. ANN. tit. 9, § 4602 (2008) (injunctive relief may be used to prohibit misappropriation and future use), and damages for actual loss and unjust enrichment stemming from the misappropriation of information falling within this definition, *see, e.g.*, MICH. COMP. LAWS. § 445.1904 (2008); VT. STAT. ANN. tit. 9, § 4603 (2008).

64 *See, e.g.*, 12 PA. CONS. STAT. ANN. § 5302 (2004); VT. STAT. ANN. tit. 9, § 4601 (2008); MICH. COMP. LAWS. ANN. § 445.1902 (2008).

65 *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 470–75 (1974).

66 RESTATEMENT (FIRST) OF TORTS § 757 (1939).

67 Hill, *supra* note 46, ¶ 14.

68 RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

69 *See* Religious Tech. Ctr. v. Wollersheim, 796 F.2d 1076, 1090 (9th Cir. 1986) ("To be protectable as a trade secret under . . . Restatement section 757 . . . the confidential material must convey an actual or potential *commercial* advantage, presumably measurable in dollar terms.").

may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers."[70] Each of these examples is a type of business information possessing potential economic value. The *Restatement* has accordingly been construed to apply exclusively to information conferring an economic advantage.[71]

Even if courts look to the UTSA, however, this model statute is more explicit than the *Restatement* in stating its exclusive application to information of economic value.[72] As defined by the UTSA, trade secret means:

> information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives *independent economic value*, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can *obtain economic value* from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[73]

By including the words "independent economic value," the UTSA explicitly requires what courts have long held in construing the tort of theft of trade secrets as defined in the *Restatement*—that the possessor of the information must derive "independent economic value" from that information for it to qualify as a trade secret.[74]

In 1996, Congress enacted the Economic Espionage Act[75] ("EEA") to better allow the federal government to address the theft

---

70 RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

71 *See* St. Paul's Benevolent Educ. & Missionary Inst. v. United States, 506 F. Supp. 822, 830 (N.D. Ga. 1980) (holding that surveys and data disclosed by several churches to the Center for Disease Control were not trade secrets because the churches were "not engaged in a trade or business, and the information [did] not give [the churches] any competitive advantage" (citing RESTATEMENT (FIRST) OF TORTS, § 757 (1939))).

72 *See* UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. 536, 538 (2005).

73 *Id.* (emphasis added).

74 *See, e.g.*, Cadence Design Sys., Inc. v. Avant! Corp., 57 P.3d 647, 650 (Cal. 2002) (stating that "independent economic value" is a required element of California's trade secret law); Basic Am., Inc. v. Shatila, 992 P.2d 175, 184 (Idaho 1999) (stating that "independent economic value" is a required element of the Idaho Trade Secrets Act); *see also* Stromback v. New Line Cinema, 384 F.3d 283, 305 (6th Cir. 2004) (holding that because a poem and screenplay were kept secret (and thus not "exploited publicly through broad dissemination"), they did not have independent economic value and thus were not trade secrets); Buffets, Inc. v. Klinke, 73 F.3d 965, 968–69 (9th Cir. 1996) (holding that restaurant recipes were not protected trade secrets because they were not superior in quality to the recipes of rivals and, therefore, did not possess independent economic value).

75 Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831–1839 (2006)).

of trade secrets from abroad and across state lines.[76] The EEA provides criminal penalties for the misappropriation of trade secrets but affords no private right of action for trade secret owners.[77] Similar to the *Restatement* and UTSA constructions of trade secret law, the EEA fails to address the theft of uniquely noneconomic, yet still secret, strategies that citizen groups intend to keep from nonmembers. The EEA's definition of a trade secret mirrors the language of the UTSA, requiring that the possessor "derive[ ] independent economic value" from the information.[78] General knowledge was not meant to be covered by the EEA,[79] as the motivation for the passage of the EEA was the economic goal of protecting American businesses from theft of trade secrets by foreign and domestic actors.[80] Hence, like the UTSA and the *Restatement*, the EEA fails to include noneconomic information, the type of information most important to preventing citizen-group espionage.

Under any of the aforementioned constructions of trade secret law—whether by the UTSA, the *Restatement*, or the EEA—the information possessed by citizen groups is not protected because the information possessed by citizen groups is noneconomic.[81] Citizen groups are not engaged in a business and they do not derive economic profits from their strategic information. The information has value, but not the kind that is covered by trade secret law. Because of trade secret law's single-minded focus on the requirement that the information be economic in nature at both the state and federal levels, victim citizen groups cannot rely on trade secret law for legal protection when they are harmed by espionage.

---

76 *See* Statement on Signing the Economic Espionage Act of 1996, 2 PUB. PAPERS 1814–15 (Oct. 11, 1996); 142 CONG. REC. S12,208 (daily ed. Oct. 2, 1996) (statement of Sen. Specter) (explaining the "glaring gap in Federal law").

77 *See* Hill, *supra* note 46, ¶ 15.

78 *See* 18 U.S.C. § 1839(3) (2006).

79 *See* 142 CONG. REC. S12,213 (daily ed. 1996) (Managers' Statement for H.R. 3723, The Economic Espionage Bill).

80 *See id.* at S12,207–08 (daily ed. 1996) (statement of Sen. Specter); *see also* United States v. Hsu, 155 F.3d 189, 195 (3d Cir. 1998) (explaining that the EEA was Congress's response to the problem of "*economic* espionage" (quoting H.R. REP. NO. 104-788, at 7 (1996) (emphasis added)), with the aim of protecting "U.S. proprietary *economic* information" (quoting S. REP. NO. 104-359, at 11 (1996) (emphasis added))).

81 For instance, the type of information obtained through citizen-group espionage by McFate was noneconomic information pertaining to lobbying strategies. *See supra* note 9 and accompanying text.

B. The Unavailability of the Tort of Breach of Confidence

The tort of breach of confidence, currently enforced primarily in England,[82] could theoretically provide a solution for victim citizen groups. American courts, however, have been reluctant to embrace the breach-of-confidence theory of liability.[83] Furthermore, because it is a common law doctrine, the application of the tort of breach of confidence in different jurisdictions could generate inconsistencies in the protections given to citizen groups from state to state. Accordingly, the tort is not an ideal means to combat espionage against citizen groups.

On a basic level, the tort of breach of confidence focuses on the existence of a duty of confidentiality pertaining to a relationship:

> A plaintiff can establish a breach of confidence action by proving the existence and breach of a duty of confidentiality. Courts have found the existence of such a duty by looking to the nature of the relationship between the parties, by reference to the law of fiduciaries, or by finding an implied contract of confidentiality.[84]

The modern law of confidentiality was clarified by the English courts in *Coco v. A.N. Clark*,[85] which prescribed three elements to demonstrate a breach of confidence. First, the information "must 'have the necessary quality of confidence about it.'"[86] This is essentially a negative test: if the information is neither trivial nor in the public domain, it is confidential.[87]

The second element required to show a breach of confidence is that the information "must have been imparted in circumstances importing an obligation of confidence."[88] Generally, this can be satisfied "whenever information is imparted, either explicitly or implicitly, for a limited purpose."[89] Finally, there must be an "unauthorised use of that information to the detriment of the party communicating it."[90]

---

82 *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 156–59 (2007).

83 *See id.* at 158.

84 *See id.* at 157.

85 Coco v. A.N. Clark (Eng'rs) Ltd., [1969] R.P.C. 41 (U.K.).

86 *Id.* at 47.

87 *See* Richards & Solove, *supra* note 82, at 162; *see also* FRANCIS GURRY, BREACH OF CONFIDENCE 4 (1984) ("As a general rule, confidentiality is established by showing that the information is inaccessible to the public: 'It must not be something which is public property and public knowledge.'" (citation omitted)).

88 *See Coco*, [1969] R.P.C. at 47.

89 *See* GURRY, *supra* note 87, at 4.

90 *See Coco*, [1969] R.P.C. at 47.

Where these three criteria are met, liability may extend to subsequent third parties who hold information obtained through a breach of confidence.[91] Courts have held that liability under the breach of confidence tort also extends to "a third party who induces a breach of a trustee's duty of loyalty, or participates in such a breach or knowingly accepts any benefit from such a breach."[92] Liability extends to third parties because it is the *idea* of the information that is protected, not simply the theft that is punished;[93] whoever subsequently obtains the information may not have misappropriated the information himself, but the idea she now possesses is still not intended to be made public.

The tort of breach of confidence, however, is not an ideal solution to the problem of citizen-group espionage. Although some American courts have recognized the tort, the majority of jurisdictions have not.[94] Hence, for most citizen groups, a tort claim under a breach of confidentiality is simply not available at this time. One could make an argument that American jurisprudence should recognize the validity of the tort claim, but such an argument goes beyond the intended scope of this Note.

Furthermore, even if American courts were to recognize the tort, because breach of confidence is a common law doctrine, its application to citizen-group espionage could generate uncertainty if different jurisdictions applied the law inconsistently. As such, a federal statute covering citizen-group espionage would be preferable because it would create a uniform rule.[95] Hence, the tort of breach of confidence is not an ideal solution for the victims of citizen-group espionage in the United States.

---

91 *See* Prince Albert v. Strange, (1848) 41 Eng. Rep. 1171, 1171 (Ch.) (holding that liability for publication of private sketches extended to the publisher).

92 Richards & Solove, *supra* note 82, at 158. As one commentator explains, "[t]he obligation of confidence thus formed extends not only to those confidants who have received confidential information for a limited purpose, but also to any third parties to whom the confidant discloses the information in breach of his obligation." GURRY, *supra* note 87, at 4.

93 *See* GURRY, *supra* note 87, at 20–21 (explaining that because the *idea* of Prince Albert's etchings was protected, liability extended to the third party that published the works).

94 Richards & Solove, *supra* note 82, at 158.

95 *See infra* Part III.

C. The Failure of Privacy Law to Address Citizen-Group Espionage

The *Second Restatement of Torts* ("*Second Restatement*") recognizes a private right of action to sue for invasion of privacy.[96] Invasion of privacy, however, is not a suitable mechanism for combating citizen-group espionage because the interest protected by the tort is an individual right and not a group right.

"[T]he existence of a right of privacy is now recognized in the great majority of American jurisdictions that have considered the question."[97] According to the *Second Restatement*, "[o]ne who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other."[98] The *Second Restatement* divides the tort into four separate rights of action: appropriation of another's name or likeness, unreasonable publicity given to the other's life, false light, and intrusion upon seclusion.[99]

As explained in the comments to the *Second Restatement*, "each involves interference with the interest of the *individual* in leading, to some reasonable extent, a secluded and private life, free from the prying eyes, ears and publications of others."[100] Because, as the *Second Restatement* recognizes, the interest protected by the right of privacy is chiefly an *individual* right,[101] it offers no protection for the interests of an organization as a whole. This alone makes the tort inadequate in addressing the type of wrong suffered by citizen-group organizations due to espionage. Tailored to individuals, not organizations, the tort of invasion of privacy is not a sufficient remedy for victim citizen-group organizations.

D. The Failure of Fraud to Address Citizen-Group Espionage

Victims of citizen-group espionage cannot rely upon the law of fraud because they generally will not suffer a pecuniary loss. Common law fraud includes misrepresentations and misleading omissions and "embraces all of the multifarious means that human ingenuity can devise and that are resorted to by one individual to gain advantage over another by false suggestions or by suppression of truth."[102] Al-

---

96 *See* RESTATEMENT (SECOND) OF TORTS § 652A (1965).

97 *Id.* § 652A cmt. a.

98 *Id.* § 652A(1).

99 *See id.* § 652A(2).

100 *See id.* § 652A cmt. b (emphasis added).

101 *See id.*

102 *See* 37 AM. JUR. 2D *Fraud and Deceit* § 1 (2001).

though the specific definitions of fraud may vary, there is a general consensus as to the fundamental requirements: "[T]here must be [1] a false representation or promise [2] as to a material fact, [3] knowledge of its falsity when made . . . , [4] intent to deceive, or suppression, and [5] reliance *with resulting damages*."[103] Though the first four elements of fraud are likely met when imagining hypothetical instances of espionage in the model of the McFate example, the fifth element, reliance with resulting damages, is not so certain.

Citizen groups do not suffer a recognized injury when they are deceived by spies falsely holding themselves out as loyal to the citizen-group movement. As the Seventh Circuit explained in *Krejci v. U.S. Army Material Development Readiness Command*,[104] "[d]eceit at common law was and is, essentially, fraud—the deliberate effort to obtain *something of value* by deceiving another."[105] The loss of "something of value" is understood to mean a pecuniary loss,[106] such that the non-pecuniary loss of noneconomic information by citizen groups is not encompassed within the general understanding of fraud.[107]

For this reason, fraudulent misrepresentation cannot apply to citizen-group espionage. The *Second Restatement* notes that "pecuniary loss" is required to satisfy the elements needed to be shown to succeed in an action for fraudulent misrepresentation.[108] Once again, the loss of the confidential information possessed by citizen-group organizations, their lobbying strategies and movement proposals, are decidedly noneconomic.[109] While the information is undoubtedly valuable to the groups and to their rivals who desire the information enough to steal it, there is seemingly no pecuniary loss in the manner envisioned by the authors of the *Second Restatement*, as citizen groups do not suffer a monetary loss when espionage occurs. Because fraud without

---

103 *See id.* § 23 (emphasis added).

104 Krejci v. U.S. Army Material Dev. Readiness Command, 733 F.2d 1278 (7th Cir. 1984).

105 *Id.* at 1281 (emphasis added).

106 Black's Law Dictionary defines "pecuniary loss" as "[a] loss of money or of something having monetary value." BLACK'S LAW DICTIONARY 1030 (9th ed. 2009).

107 *See* 37 AM. JUR. 2D *Fraud and Deceit* § 272 (2001) ("[D]eceit belongs to that class of tort for which a pecuniary loss generally constitutes a necessary part of the cause of action.").

108 "One who fraudulently makes a misrepresentation of fact, opinion, intention or law for the purpose of inducing another to act . . . in reliance upon it, is subject to liability to the other in deceit for *pecuniary loss* caused to him by his justifiable reliance upon the misrepresentation." RESTATEMENT (SECOND) OF TORTS § 525 (1965) (emphasis added).

109 *See supra* note 81 and accompanying text (explaining how the information possessed by citizen groups is noneconomic in nature).

damages is not sufficient,[110] it is not a viable solution to the problem of citizen-group espionage.

Today, citizen groups lack adequate legal protections when they are harmed by noneconomic espionage. Trade secret law, the breach of confidence tort, the tort of invasion of privacy, and the law of fraud fail to provide a sufficient legal solution for victim organizations. Without threat of legal consequences, corporations and rival citizen groups will have no reason to stop the practice of citizen-group espionage. To give citizen groups the protection they need, the next Part proposes a possible solution: that Congress enact a statute—the Citizen-Group Espionage Act.

III. The Citizen-Group Espionage Act

Without threat or fear of punishment, actors will likely have no disincentive to engage in espionage, and some will continue to opt for deceptive methods to accomplish their respective agendas. Citizen groups that are victimized by espionage are currently without adequate legal protections. As a possible solution to close the current legal loophole that allows actors to engage in citizen-group espionage and escape punishment, Congress should enact legislation to criminalize this behavior and grant victim citizen groups a private right of action. Such legislation should deter sponsors of citizen-group espionage, and it should ultimately promote the right to free speech through the exchange of ideas in the marketplace of ideas.[111]

This Part first explains why it should be Congress that regulates citizen-group espionage. It then proposes the Citizen-Group Espionage Act for Congress to enact. The proposed Act melds trade secret law with concepts from the breach of confidence tort, forming a hybrid criminal statute that would punish both the agents of citizen-group espionage and their sponsors. Finally, this Part applies the Act to the Mary McFate situation to demonstrate its efficacy in solving the problem.

A. The Need for Federal Regulation

Congress should fill the legislative void and enact legislation criminalizing citizen-group espionage. Congress has the power to regulate most instances of citizen-group espionage pursuant to its author-

110 37 Am. Jur. 2d *Fraud and Deceit* § 21 (2001); *see, e.g.*, Lichtenberg v. Burdell, 281 P. 518, 525 (Cal. Dist. Ct. App. 1929).

111 *See supra* notes 33–41 and accompanying text (discussing the marketplace of ideas).

ity under the Commerce Clause,[112] as it is probable that the agents and sponsors of espionage will use the channels or instrumentalities of interstate commerce (e.g., mail, telephone, or Internet) to transmit collected information across state lines.[113] In the rare situation where the espionage occurs entirely intrastate, Congress could regulate the activity by showing that citizen-group espionage has a substantial effect on interstate commerce.[114] Congress could determine that a substantial effect on interstate commerce exists by looking to charitable donations. Charitable donations typically are solicited through the Internet, mail or other instrumentalities of interstate commerce and frequently are transmitted interstate from donor to donee.[115] Citizen-group espionage could substantially affect interstate commerce because citizen groups that receive and depend on interstate contributions for their success may find that potential donors are more hesitant to donate when there is a risk that the organization's efficacy will be undercut by espionage. Though citizen-group espionage targets noneconomic information, for the purposes of the Commerce Clause there is a substantial effect on interstate commerce that gives Congress the authority to regulate.

A federal statute criminalizing citizen-group espionage has certain benefits over a state statute that accomplishes the same end. Namely, a single federal statute codifying the crime of citizen-group espionage would avoid problems of uniformity that may emerge if the states are left with the choice to enact their own laws governing the issue. State legislatures that are weary of citizen groups may decline to protect them. And corporations that engage in citizen-group espionage may be able to use their resources to influence receptive state legislatures to not enact legislation, or to water down legislation passed by the state. Leaving regulation to the states has the potential to produce a situation where a citizen group's right to be secure in its

---

112 U.S. CONST. art. I, § 8, cl. 3.

113 The Commerce Clause gives Congress the authority to regulate the use of the channels of interstate commerce (e.g., roads, mail). *See* United States v. Lopez, 514 U.S. 549, 558 (1995). It also grants Congress the power to regulate the instrumentalities (e.g., trains, trucks), persons, or things in interstate commerce. *See* id. "It is well established that telephones, even when used intrastate, constitute instrumentalities of interstate commerce." United States v. Weathers, 169 F.3d 336, 341 (6th Cir. 1999). Similarly, courts have held that the Internet is an instrumentality of interstate commerce. *See, e.g.*, United States v. MacEwan, 455 F.3d 237, 245 (3d Cir. 2006).

114 Pursuant to its Commerce Clause authority, Congress has the power to regulate activities having a substantial relation or effect on interstate commerce. *See Lopez*, 514 U.S. at 558.

115 Charitable donations, therefore, are interstate commerce in the sense that they are both things in interstate commerce and things solicited through the channels and instrumentalities of interstate commerce. *See id.*

proprietary information depends entirely on what state the group is located in. To ensure uniform protection, a federal statute is needed. Accordingly, Congress should utilize its enumerated power under the Commerce Clause to enact a law criminalizing citizen-group espionage.

B. The Citizen-Group Espionage Act: Protecting Against Theft of Confidential Noneconomic Information

The Citizen-Group Espionage Act must seek to protect secret, strategic information, regardless of its economic value. Combining the definition of confidential information from the breach of confidence tort with the structure and definitions of trade secret laws produces a hybrid act that would effectively criminalize citizen-group espionage and grant a private right of action to victim citizen groups. The proposed Act has two sections.

Section 1 of the Citizen-Group Espionage Act contains the definitions for the Act. For guidance, the Act looks to the definition of confidential information protected by the tort of breach of confidence. The essential philosophy behind the breach of confidence tort is that "communicating an idea in confidence to another should not render it part of the common pool of knowledge."[116] This is also the Act's motivation: the information that citizen groups store and what members share with each other in closed-door meetings and through members-only e-mails or phone calls is not meant to be rendered part of the common pool of knowledge. When conferred or stored under confidential circumstances, the noneconomic information possessed by citizen groups should fall under the protection of the law.

Because the tort of breach of confidence recognizes that the holder has a duty to faithfully uphold its confidentiality, it is useful in designing legislation combating citizen-group espionage. As such, the definition for confidential information, the information to be protected by the Act, borrows in part from the definition of confidential information protected under the law of confidentiality[117]:

> Section 1(a): Confidential Information:
>
> (i) "Confidential information" as used in this statute means all information that is:
>
> (A) neither trivial, nor in the public domain; and

116 Payne, *supra* note 42, at 253.

117 *See supra* Part II.B.

> (B) transmitted, stored, or held under a reasonable expectation that that information will be kept from the public domain and exterior parties.
>
> (ii) There shall be no requirement that information possess economic or pecuniary value to qualify as "confidential information" under this Act.
>
> (iii) "Confidential information" shall not be construed to include any information pertaining to illegal activities or instances of harassment.

This definition of confidential information explicitly eliminates the requirement in trade secret law that the information have economic value, while narrowly tailoring the scope of protection to cover only that information which should reasonably be expected to be kept from external parties. Thus, divulging the contents of ordinary, everyday conversations would not fall within the ambit of the Act. By omitting information pertaining to illegal activities or harassment from the purview of the Act, subsection (a)(iii) is designed to ensure that whistleblowers who sound the alarm on illegal behavior or harassment will not be dissuaded from exposing the criminal behavior or bringing civil claims.

This definition should allay possible concerns that the term "confidential information" is overinclusive because it creates potential criminal liability for otherwise ordinary conversations. By limiting liability to where there is a reasonable expectation of confidentiality, the Act imposes an objective standard for people to follow when they acquire information, but before they decide whether to disseminate it.

Additionally, the Act provides definitions for "improper means" and "misappropriation." Section 1 of the UTSA[118] gives an accurate description of the type of behavior that espionage sponsors and agents engage in when targeting citizen groups. Accordingly, Sections 1(b) and 1(c) of the Act look to the definitions of the terms in the UTSA, but substitute "confidential information" for "trade secret":

> Section 1(b): "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means;
>
> Section 1(c): "Misappropriation" means:

---

118 UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. 536, 537–619 (2005).

> (i) acquisition of confidential information of another by a person who knows or has reason to know that the confidential information was acquired by improper means; or
>
> (ii) disclosure or use of confidential information of another without express or implied consent by a person who
>
> (A) used improper means to acquire knowledge of the confidential information; or
>
> (B) at the time of disclosure or use, knew or had reason to know that his knowledge of the confidential information was
>
> (I) derived from or through a person who had utilized improper means to acquire it;
>
> (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
>
> (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
>
> (C) before a material change of his or her position, knew or had reason to know that it was confidential information and that knowledge of it had been acquired by accident or mistake.

The requirement that there be theft, misappropriation, or unauthorized appropriation limits the imposition of liability to when information is obtained through morally questionable means. In this sense, the disclosure of information obtained in innocent conversation will go unpunished, so long as the transmission of the information to the public is authorized.

The final definition that must be included in the Act is for the term "citizen group." As the goal of the Citizen-Group Espionage Act is to criminalize only espionage that harms the marketplace of ideas by undermining social and political discourse, a line must be drawn such that not every single association in society is included.[119] To avoid being overinclusive, the Act defines the term "citizen group" as follows:

---

119 Without a narrow definition, opponents of big government could argue that a "citizen group" is overinclusive and vague. There may be concern that the statute would allow for government regulation to extend into ordinary interactions of every type of organization or group that Americans participate in daily.

> Section 1(d): "Citizen group" means any organization whose primary purpose is peaceful activism, lobbying, or raising social awareness.

It is essential for the efficacy of the law that, at a minimum, groups like CeaseFire PA, Greenpeace, and other peaceful activist organizations are extended protection by the Act. At the same time, the Act must not have the unintended effect of regulating every association in society. If the government were to criminalize misappropriation of noneconomic information from a member of a community cheerleading club or weekly bridge tournaments—clubs that have a recreational purpose rather than an activist agenda—it would not be serving the goal of promoting open and honest political discourse. To address this potential problem of overinclusiveness, the definition of "citizen group" limits the application of the law to information held by those organizations that have the social purposes of "peaceful activism, lobbying, or raising social awareness." Such a definition would allow courts to apply the statute narrowly and ensure that its intended purpose of promoting open and honest social and political discourse is achieved in an appropriate manner.

Next, section 2 contains the structure of the Act, criminalizing citizen-group espionage. Although trade secret laws do not currently address the appropriation of noneconomic information,[120] they provide helpful guidance for crafting an Act that criminalizes the theft of noneconomic secrets. At its core, the prevention of activist espionage shares the same goal as trade secret law: the involuntary disclosure of information—whether it be through deceit, espionage, or theft—should not result in a forfeiture of the information.[121]

The structure of the EEA, by punishing the attainment of nonpublic information through means of deception and extending liability to third-party recipients of that information, provides an ideal model for the criminalization of citizen-group espionage. Section 2 of the Act, therefore, is modeled after section 1832 of the EEA[122] and incorporates the definitions from section 1 of the Act:

---

120 *See supra* Part II.A.

121 *See supra* note 56 and accompanying text.

122 The EEA reads:

> (a) Whoever, with intent to convert a trade secret . . . to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies,

Section 2: Citizen-Group Espionage:

(a) Whoever, with intent to convert confidential information, that is owned by a citizen group, to the benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that confidential information, knowingly—

(1) steals, misappropriates, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen, misappropriated, or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any individual that commits any offense described in subsection (a) shall be fined not more than $1,000,000.

(c) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

(d) Any individual or organization that commits any offense described in subsection (a) shall be liable to the citizen group

---

replicates, transmits, delivers, sends, mails, communicates, or conveys such information; (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both. (b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

18 U.S.C. § 1832 (2006).

> they committed espionage against, and such citizen group may sue either at law or in equity in any court of competent jurisdiction to recover punitive damages and obtain an injunction against the release, disclosure, or further dissemination of any of the information described in section 1(a) of this Act. The statute of limitations will run five (5) years after the date such citizen group gains knowledge of the commission of any of the acts in subsection (a).

In structuring the Citizen-Group Espionage Act after the EEA, criminal sanctions extend to both agents and sponsors of citizen-group espionage, as well as any other beneficiaries of espionage. By extending criminal penalties to all beneficiaries of citizen-group espionage, the Act stops citizen-group espionage at its very source, the sponsor. Furthermore, by providing a private right of action, the Act would allow for citizen groups to independently bring their own suits should the government fail to prosecute citizen-group espionage by its own initiative. The potential for civil liability for both sponsors and agents of citizen-group espionage is an added deterrent to the strong criminal penalties in the Act. Additionally, citizen groups would be able to obtain an injunction against the further release of any of the confidential information, thereby plugging the information leak. In the same way that the UTSA allows states to extend legal protections to businesses victimized by theft of trade secrets, and reflecting third-party liability of the breach of confidence tort,[123] this proposed Act would allow the government to provide proper legal protections to citizen groups that are victimized by espionage.

Criminal sanctions, with liability extending to third parties, as well as a private right of action for victim citizen groups, would deter individuals and rival interest groups from using deceptive means to acquire secret, noneconomic information.[124] By enacting the proposed law, Congress would reaffirm the sanctity of the American marketplace of ideas and reinforce values of open and honest debate.

C. Application of the Act to the McFate Case

Applying the Citizen-Group Espionage Act to the facts of the Mary McFate case[125] demonstrates the utility of the Act in remedying

---

123 *See supra* note 91 and accompanying text.

124 *Cf. Economic Espionage: Hearing Before the Subcomm. on Crime of the H. Comm. on the Judiciary*, 104th Cong. 13–16 (1996) (prepared statement of Louis J. Freeh, Director, Federal Bureau of Investigation) (discussing deterrent effect of criminal sanctions on economic espionage).

125 *See supra* notes 1–11 and accompanying text.

the problem. Although McFate and the NRA suffered no punishment for their conduct, had the proposed Act been in force, it is probable that both McFate and the NRA would have been held criminally liable.

First, the information obtained by McFate from the gun-control groups would fall within the definition of "confidential information" under section 1(a) of the Act. The information was not trivial—it was essential information about the future lobbying strategies of the groups—and it was not in the public domain.[126] Furthermore, the information was obviously not meant to be made known to the NRA, and was thus "transmitted under a reasonable expectation that that information will be kept from the public domain and exterior parties [the NRA]."[127] It was implicit in the circumstances of the strategic board meetings and phone calls that the information was not to be made known to their competitors in the NRA, for that would have clearly undermined the group's lobbying strategies. Thus, section 1(a)(i) is easily satisfied. Section 1(a)(ii) expressly states that the noneconomic nature of the information is inconsequential for purposes of the Act.

Second, McFate misappropriated the information by improper means as defined under the Act.[128] She obtained her information by misrepresenting herself as a crusader for the gun-control movement.[129] She then disclosed the confidential information without express or implied consent.[130] McFate was not authorized to transmit the lobbying strategy she obtained to the NRA or other competing organizations and that unauthorized use of the information was to the detriment of the groups, as it could have permitted competing groups to prepare for the lobbying strategies by preempting and marginalizing those efforts.[131] By acquiring the information as a third party from a source that it knew did not have consent, the NRA also misappropriated the information under the definition. Third, as the primary purpose of the gun-control groups was peaceful activism, the groups would fit squarely within the statute's definition of a "citizen group."

---

126 *See supra* note 9 and accompanying text.

127 See section (1)(a)(i)(B) of the model Citizen-Group Espionage Act, discussed *supra* in Part III.B.

128 See section (1)(b) of the model Citizen-Group Espionage Act, discussed *supra* in Part III.B.

129 *See supra* notes 1–11 and accompanying text.

130 *See supra* notes 1–11 and accompanying text.

131 *See supra* notes 1–11 and accompanying text.

Bearing these facts and definitions in mind, McFate and the NRA would be criminally liable under section 2 of the Act. Both the NRA and McFate intended to convert the confidential information owned by the citizen groups, they did so for their own benefit, and they intended to injure the citizen groups' lobbying efforts. McFate knowingly misappropriated the information, and the NRA received the information from McFate knowing it to have been misappropriated.

Having satisfied all the elements of the Act, both McFate and the NRA would be criminally liable. McFate could be imprisoned for up to ten years and fined up to $1,000,000; the NRA could be fined up to $5,000,000. Additionally, both McFate and the NRA could be subject to civil liability if the victim gun-control groups elected to exercise their private right of action under the Act. Such punishments, and potential civil liability, would likely deter sponsors like the NRA and agents like McFate from engaging in espionage against citizen groups, forcing sponsors instead to champion their competing beliefs through legitimate debate in the marketplace of ideas.

Conclusion

Mary McFate's betrayal of the gun-control community has shined a light on the shadowy industry of citizen-group espionage. Instead of engaging in open and honest debate with citizen groups, corporations and rival interest groups have used deception and espionage to obtain strategic, confidential information held by citizen groups. This practice poses a threat to the vitality of the marketplace of ideas, offends traditional notions of fairness and honesty, and allows actors to benefit from their deception. The law in its current state fails to provide an effective solution for organizations that are targeted by citizen-group espionage. The law of trade secrets, the breach of confidence tort, the invasion of privacy tort, and the laws of fraud all fail to address the unique need of citizen groups to protect their vital noneconomic information. As such, Congress should enact legislation that would criminalize the theft of confidential, noneconomic information. The Citizen-Group Espionage Act will dissuade potential agents and sponsors of citizen-group espionage while encouraging the healthy dialogue upon which a strong civil society depends.