May 14, 2019 **ARTICLES**

Political Trade Secrets: Intellectual Property Defense to Political Hacking

An effective DTSA litigation may not immediately reverse an election result, but it might severely weaken the conspirators.

By Daniel Kegan

Share this:

Confusion, deception, and mistake are generally unlawful in marketing campaigns. 14 U.S.C. § 1125 (a) (Lanham Act section 43(a)). Yet, confusion, deception, and mistake are typically lawful in political campaigns. U.S. Const. amend. I ("Congress shall make no law . . . abridging the freedom of speech, or of the press"); amend. XIV ("No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."). Our democratic republic assumes informed and participating citizens. Yet, judicial fairness

recognizes some evidence is privileged against disclosure. Fed. R. Civ. P. 501.

"Political advertising and promotion is political speech, and therefore not encompassed by the term 'commercial.' This is true whether what is being promoted is an individual candidacy for public office, or a particular political issue or point of view." 134 Cong. Rec. H 1297 (daily ed. Apr. 13, 1989) (statement of Wis. Rep. Kastenmeier) (cited in *MasterCard Int'l, Inc. v. Nader 2000*, 70 USPQ2d 1046 (S.D.N.Y. 2004) (finding candidates use of "priceless" ad parody was political speech, thus categorically exempt from coverage by the Federal Trademark Dilution Act)). Not only are many political torts excused from principal commercial fair dealing laws—elections and their certifications are often concluded well before a final judgment is typically available. Moreover, courts disfavor involvement in political disputes. Although courts prefer that the voters and legislatures resolve the matter, political lawsuits are frequent. *E.g.*, *Bush v. Gore*, 531 U.S. 98 (2000).

Government transparency is encouraged by freedom of information laws—the Freedom of Information Act (FOIA), 5 U.S.C. § 552 (effective July 5, 1967), and state parallels, e.g., Illinois Freedom of Information Act, 5 Ill. Comp. Stat. 140 (effective Jan. 1, 2010). FOIA is sometimes also discouraged in practice (e.g., David S. Hilzenrath, "Big Oil Rules: One Reporter's Runaround to Access 'Public' Documents," *Project on Gov't Oversight*, Dec. 6,

2018) and by congressional investigative powers (U.S. House of Representatives, Investigations & Oversight). It is true that "Congress cannot constitutionally inquire 'into the private affairs of individuals who hold no office under the government' when the investigation 'could result in no valid legislation on the subject to which the inquiry referred.'" *Hutcheson v. United States*, 369 U.S. 599 n.16 (1962) (quoting *Kilbourn v. Thompson*, 103 U.S. 168, 195 (1880), and noting *Kilbourn* "severely discredited," e.g., *United States v. Rumely*, 345 U.S. 41, 46 (1953)). However, the congressional investigative power, typically delegated to a committee, supports Congress's legislative function and is a key element of the Constitution's checks and balances.

There is no general system for registering a trade secret, unlike copyrights, trademarks, and patents. A trade secret is information that has independent economic value from not being generally known and for which the owner has taken reasonable measures for it to maintain secret. The term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

> (A) the owner thereof has taken reasonable measures to keep such information secret; and

> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information[.]

18 U.S.C. § 1839(3).

Until the recent federal Defend Trade Secrets Act (DTSA), 130 Stat. 376, effective 11 May 11, 2016, trade secret law in the United States was provided by the separate states, similar to the Uniform Trade Secrets Act, but with individual state enactments and individual state case law. For example, in the Illinois Trade Secrets Act,

> "[t]rade secret" means information, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or list of actual or potential customers or suppliers, that:

> (1) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and

> (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy

> or confidentiality.

765 Ill. Comp. Stat. 1065.

The DTSA extended the Economic Espionage Act of 1996 (EEA), which criminalized some trade secret misappropriations. 18 U.S.C. §§ 1831–1839 (ch. 90). Unlike the Espionage Act of 1917, 18 U.S.C. §§ 792–799, the EEA covers commercial information, not classified or national defense information. However, EEA trade secret theft is limited to "a product," while its economic espionage requires knowledge or intent that the theft will benefit a foreign power. U.S.C. §§ 1831 & 1832.

In contrast with the economy of our nation's farmer framers, the contemporary American economy is dominated by services, not goods. According to a U.S. Bureau of Economic Analysis study, in 2009 services accounted for 80 percent of U.S. private sector gross domestic product (GDP), $9.8 trillion. Service jobs accounted for more than 80 percent of U.S. private sector employment, 90 million jobs. John Ward, Int'l Trade Admin., U.S. Dep't of Commerce, *The Services Sector: How Best to Measure It?* (Oct. 2010).The EEA is inadequate to protect trade secrets in the bulk of our current economy.

Reflecting the increased commercial saliency of trade secrets, Article 39 of the Agreement between the United States, the United Mexican States, and Canada (USMCA) explicitly mandates protection of trade secrets and preventing disclosure contrary to "honest commercial practices." The treaty has been signed but not yet ratified. Other articles relevant to trade

secrets articles are Civil Protection and Enforcement (Article 20.1.1), Criminal Enforcement (Article 20.1.2), Definitions (Article 20.1.3), Provisional Measures (Article 20.1.4), Confidentiality (Article 20.1.5), Civil Remedits (Article 20.1.6), Licensing and Transfer of Trade Secrets (Article 20.1.7), Prohibition of Unauthorized Disclosure or Use of a Trade Secret by Government Officials Outside the Scope of Their Official Duties. Wikipedia, USMCA.

Paralleling the increasing salience of digital data and commercial trade secrets, protecting personal privacy and personal information are increasingly of concern to both individuals and regulators. *Examining Safeguards for Consumer Data Privacy*, Hearing Before the S. Comm. on Commerce, Science & Transportation (Sept. 26, 2018); U.S. Gov't Accountability Office, GAO-19-52, *Internet Privacy*, (Jan. 2019); "Your Data Was Probably Stolen in Cyberattack in 2018—and You Should Care," *USA Today*, Dec. 28, 2018; European Union, The EU General Data Protection Regulation (GDPR) Is the Most Important Change in Data Privacy Regulation in 20 Years; GDPR Key Changes; General Data Protection Regulation (GDPR) impacts USA entities storing data of EU residents.

The Internet now pervades not only the U.S. economy but much of the world's economy and lifestyles. Internet predecessor ARPANET first connected two network nodes on October 29, 1969: UCLA and SRI in Menlo Park, California. In 1982, the Internet Protocol Suite (TCP/IP) was standardized, permitting worldwide Internet connections. With a 2017 world population of 7.4 billion people, 48 percent are now Internet users; 81 percent in the developed world and 41 percent in the developing world. Int'l Telecommunications Union, *ICT Facts*

and Figures 2017, at 2 (July 2017).

Before computer-specific criminal laws, computer crimes in the United States were usually prosecuted, when they could be, as mail and wire fraud, a federal crime since 1872. 18 U.S.C. §§ 1341, 1342, 1346. Mail and wire fraud requires (a) intent, (b) a "scheme or artifice to defraud" or the obtaining of property by fraud, and (c) a mail or wire communication.

The Computer Fraud and Abuse Act (CFAA), enacted in 1984, prohibits accessing a computer without, or in excess of, authorization, in limited circumstances. 18 U.S.C. § 1030(a)(2). The statute is limited to "(A) information contained in a financial record or a financial institution; or of a card issuer . . . or contained in a file of a consumer reporting agency on a consumer . . . ; (B) information from any department or agency of the United States; or (C) information from any protected computer." 18 U.S.C. § 1030(a)(2). A "protected computer" is used by or for a financial institution or the U.S. government or is used in or affects interstate or foreign commerce or communication. 18 U.S.C. § 1030(e)(2).

A CFAA "loss" is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). Most courts have interpreted CFAA loss as costs that flow directly from the access, such as service interruption. Copying information may not create a CFAA loss. The statute of

limitations is two years.

The CFAA requires damage of at least $5,000 sustained during a one-year period. CFAA damage is defined as "any impairment to the integrity or availability of data, a program, a system of information." 18 U.S.C. § 1030(e)(8). Damages available under CFAA are more limited than under a trade secret claim, and they do not include the value of the misappropriated information, nor does CFAA provide for exemplary damages.

Hacking into the computer of a political candidate, official, or party and disseminating the information was not readily covered by U.S. statutes before the DTSA was enacted. Maintaining political information confidential, attempts to "hack" into it, and disinformation have been part of our political system since at least the nation's founding. Chernow, W*ashington: A Life* (Penguin Books 2010); Ron Chernow, *Alexander Hamilton* (Penguin Group (USA) LLC 2005). The DTSA provides a potential cause of action—and potentially a strong, albeit delayed, remedy.

The Senate Select Committee on Intelligence, in its *Worldwide Threat Assessment of the US Intelligence Community* (Jan. 29, 2019), lists "Cyber" as the first of 10 global threats. The report introduces its topics saying the "order of the topics presented in this statement does not necessarily indicate the relative importance or magnitude of the threat in the view of the Intelligence Community." Yet, placing Cyber as the first threat is unlikely a random, or even haphazard, act: "Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek

political, economic, and military advantage over the United States and its allies and partners." *Id.* at 5 (original in bold, italic). This article's focus on political trade secrets does not imply that commercial trade secrets are not also important, and under risk. *E.g.*, Nicole Perlroth, "Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies," *N.Y. Times*, Feb. 18, 2019.

The hacks into computers of Democratic candidate Hillary Clinton, the Democratic National Committee, and official John Podesta have spawned the Justice Department Special Counsel investigation headed by Robert Mueller, congressional investigations, over 30 indictments, and several high-profile convictions. Republican emails have also been hacked. Alex Isenstadt & John Bresnahan, "Emails of Top NRCC Officials Stolen in Major 2018 Hack," *Politico*, Dec. 4, 2018. Yet, prision sentences and financial forfeiture to the government don't compensate the hacked victims. The Defend Trade Secrets Act might help.

After a hack of political information, balanced dissemination should not be expected. Wikipedia, WikiLeaks; Cherie Blair & Ema Vidak Gojkovic, "WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evidence," *ICSID Rev.*, Feb. 3, 2018. More common are intentional falsification, predicate innuendo, and negative advertising (Jill G. Klein & Rohini Ahluwalia, "Negativity in the Evaluation of Political Candidates," *J. Marketing* (Jan. 2005)), and often media blitz very shortly before the election day. Daniel Kegan, "Political Trademarks: Intellectual Property in Politics and Government," Ill. State Bar Ass'n, *44 Intellectual Prop. Newsl.* no. 1 (Oct. 2004). Harsh responses to one's disfavored political positions too often displace civility and rational discourse, emulating Gresham's law

of bad money displacing the good. Representative Preston Brooks (SC) brutally caning Senator Charles Sumner (MA), on May 22, 1856, over Sumner's speech for Kansas being admitted to the Union as a free state is a salient example. U.S. Senate, The Caning of Senator Charles Sumner.

Given a court finding of misappropriation, a court may award damages. 18 U.S.C. § 1836(b)(3)(B). Given a court finding of willful and malicious misappropriation, exemplary damages of up to double may be awarded. 18 U.S.C. § 1836(b)(3)(C). The EEA, of which the DTSA became a part, provides that the law applies to conduct outside the United States if (a) the offender is a citizen or permanent resident of the United States, (b) the offender is a U.S. corporation, or (c) an act furthering the offense was committed in the United States. 18 U.S.C. § 1837.

The federal conspiracy statute is broad. Its reach may include actors for whom other evidence of committing a substantive crime might be difficult to obtain:

> If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.

> If, however, the offense, the commission of which

> is the object of the conspiracy, is a misdemeanor only, the punishment for such conspiracy shall not exceed the maximum punishment provided for such misdemeanor.

18 U.S.C. § 371.

Federal conspiracy is a continuing offense. Its statute of limitations, five years, begins on the date of the last overt act, by anyone in the conspiracy. 18 U.S.C. § 371. Most federal crimes have a five-year limitations period; capital offenses may be tried at any time. 18 U.S.C. § 3281. A conspiracy is deemed to continue until its purpose is achieved or abandoned. An individual's "withdrawal" from a conspiracy starts the statute of limitations running for that individual. Withdrawal from a conspiracy for limitations purpose requires the conspirator to take affirmative action by full disclosure to authorities or communicating his or her disassociation to the other conspirators. U.S. Dep't of Justice, *Criminal Resource Manual § 652*.

Now, with the Defend Trade Secrets Act, a hacker, the knowing disseminator, and all involved in the conspiracy may be subject to significant damage awards. The damage of unauthorized dissemination of political campaign information is not measured by lost sales or the tortfeaser's wrongful profits. Nor would the salary of the involved political office likely be an appropriate measure very often.

The Copyright Act provides a model procedure for determining damages. "In establishing the infringer's profits, the copyright owner is required to present proof only of the infringer's gross

revenue, and the infringer is reuired to prove his or her deductible expenses and the elements of profit attributable to fators other than the copyrighted work." 17 U.S.C. § 504(b). For political trade secret liability, in establishing the damage to a plaintiff trade secret owner, the plaintiff may be required to present proof only of the defendant's campaign expenses, including unpaid debts, plus unspent contributions, and the infringer would be required to prove any damage apportionment claimed not due to the trade secret tort.

Prudence suggests the plaintiff be prepared with its alternative allocation evidence. For many political campaigns, federal and state laws require periodic reporting of campaign expenses and contributions. Federal Election Commission; Nat'l Conference of State Legislatures, State Campaign Finance Laws: An Overview; Ballotpedia, Federal Campign Finance Laws and Regulations; Ill. State Bd. of Elections, Frequently Asked Questions about Campaign Disclosure. ("Who must file campaign disclosure reports? Any individual, trust, partnership, committee, association, corporation, or any other organization or group of persons which receives or spends more than $5,000 on behalf of or in opposition to a candidate or question of public policy, meets the definition of a political committee and must comply with all provisions of the Illinois Campaign Financing Act, including the filing of campaign disclosure reports. The $5,000 threshold does not apply to political party committees. In addition, any entity other than a natural person that makes expenditures of any kind in an aggregate amount of more than $3,000 during any 12-month period supporting or opposing a public official or candidate must organize as a political committee.")

One measure of the damage could be the total amount spent, including unpaid debts, plus unspent contributions, in the campaign by the candidate or referendum campaign, supported, explicitly or implicitly, by the tortfeasor. If the defendant does not provide its full expense and contribution information, then the plaintiff's expense and contribution amounts might be used, with no apportionment by the defendant. Hacking and dissemination of likely stolen political information will usually be found to be willful and malicious, supporting double damages.

An effective DTSA litigation may not immediately reverse an election result, but it might severely weaken the conspirators. *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974).

Daniel Kegan practices law at Kegan & Kegan, Ltd., in Chicago, Illinois. He also writes regularly about

---