

ARTICLE

THROUGH THE LOOKING GLASS: TRADE SECRET HARMONIZATION AS A REFLECTION OF U.S. LAW¹

BY SHARON K. SANDEEN²

CONTENTS

INTRODUCTION	452
A. A BRIEF HISTORY OF TRADE SECRET HARMONIZATION EFFORTS.....	453
B. U.S. TRADE SECRET LAW: WHAT IT IS AND IS THOUGHT TO BE	459
1. <i>The identity and parameters of unprotected information</i>	461
2. <i>The meaning of the reasonable efforts requirement</i>	463
3. <i>Establishing duties of confidentiality</i>	465
4. <i>The requirement of harm</i>	467
5. <i>The fleeting nature of trade secrets</i>	469
6. <i>Ancillary limitations on the enforcement of trade secret rights</i> ..	470
C. EXPANDED PROTECTIONS UNDER THE TRADE SECRET DIRECTIVE	472
CONCLUSION	475

¹ This article will also be published in *The harmonization and protection of trade secrets in the EU – An Appraisal of the EU Directive*, Schovsbo, Minssen, Riis, eds., forthcoming, Edward Elgar Publishing Ltd. The material cannot be used for any other purpose without further permission of Professor Sandeen and Edward Elgar. It is for private use only.

² Robins Kaplan LLP Distinguished Professor in Intellectual Property Law and Director of the IP Institute at Mitchell Hamline School of Law (MHSL) and the Fulbright-Hanken Distinguished Chair in Business and Economics 2019-2020. Professor Sandeen is grateful to be invited to write this article for the above-referenced Edward Elgar publication and to present her work as part of the Boston University School of Law 2019 symposium on *Intellectual Property in a Globalized Economy: United States Extraterritoriality in International Business*. Professor Sandeen thanks MHSL Research & Instructional Librarian, Lisa Heidenreich, and her 2018-2019 Research Assistant, Lukas Bellflower, for their work on this article.

INTRODUCTION

Every sovereign nation has the right to adopt and interpret its own laws. How a nation does so typically depends upon that nation's values, needs, and legal traditions. Thus, efforts to harmonize the laws of different countries, including recent efforts to harmonize trade secret law, can create tension between countries. This is not only because harmonization efforts are often seen as an affront to sovereignty but also because of differences of opinion about what the various provisions of the harmonized laws mean and how those laws should be applied and enforced. Since every country that joins an agreement calling for harmonization is likely to have their own point of view concerning the meaning and purpose of the subject law and how best to implement it, countries that do not hew closely enough to one country's viewpoint are often criticized for failing to abide by their obligations under the agreement. A related problem is that sometimes the law at issue is not well developed or is misunderstood by the government officials and private entities that advocate for its adoption, leading to differences of opinion about what the harmonization agreement requires. These problems are magnified when harmonization efforts are not reflected in one international agreement but rather in a series of agreements by different constellations of countries, as is the case with recent efforts to harmonize trade secret law.

An example of recent trade secret harmonization efforts is the *Directive of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition*³ (hereinafter the "Trade Secret Directive" or "Directive") that is being implemented by European Union (EU) countries. The history of the Directive establishes that it is part of a coordinated effort to require more countries to conform their trade secret laws to the trade secret principles of the United States (U.S.). Thus, those who advocated for the adoption of the Trade Secret Directive, including the U.S. Trade Representative (USTR) and members of two coalitions of multinational corporations that include many U.S.-based companies (as discussed below), are certain to judge the adequacy of EU law through the lens of U.S. trade secret law. This Article sheds light on that perspective, not to suggest that the trade secret laws of each EU-Member should conform to U.S. law, but to highlight potential points of divergence and future controversy. It also identifies issues upon which EU-Member countries may wish to exercise flexibility as well as where EU trade secret principles may prove to be superior to U.S. counterparts.

This Article is divided into three parts. Part A gives a brief history of trade secret harmonization efforts, showing how the Trade Secret Directive is the result of a coordinated international effort to require countries to adopt U.S. trade

³ Directive 2016/943, of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, 2016 O.J. (L 157) 1 (EU) [hereinafter EU Trade Secret Directive].

secret principles that began around 2010. Part B explains how U.S. harmonization advocates may understand U.S. trade secret law and, in the process, identifies potential points of disagreement. A quick summary is that U.S. trade secret law does not provide the degree of protection that many believe, partly due to the fact that U.S. trade secret law cannot interfere too much with U.S. patent and copyright law, but also because of the principles of free competition and employee mobility that underlie its limits. Part B also identifies relevant flexibilities contained in the Directive and areas of U.S. trade secret law that are underdeveloped. Both types of flexibilities provide opportunities for EU-Member countries to adopt trade secret laws that are reflective of their own values and needs. Part C discusses how the Trade Secret Directive differs from U.S. law by providing greater trade secret protection and, consequently, where EU-Member countries may wish to limit protection. The Article concludes with some general reflections about how EU trade secret law may improve trade secret law.

A. A BRIEF HISTORY OF TRADE SECRET HARMONIZATION EFFORTS

In the U.S., efforts to harmonize trade secret law began in the 1960s with attorney-initiated proposals for a uniform law that all fifty states could adopt.⁴ These efforts ultimately culminated in the adoption of the Uniform Trade Secrets Act (UTSA) by the National Conference of Commissioners on Uniform State Laws in 1979.⁵ While the drafting history of the UTSA reveals that its proponents wanted to broaden the definition of a trade secret by eliminating the use requirement, those who were involved in the drafting process seemed more concerned with the need to cabin a definition that was deemed too unpredictable.⁶ They also feared that if not properly limited, trade secret law would be preempted by U.S. patent law.⁷ Ultimately, proponents of a uniform law struck a balance between the desire to protect trade secrets and concerns about the potential anticompetitive effects of trade secret enforcement. They did so by, among other things: (1) clearly defining the elements of a claim for trade secret misappropriation; (2) recognizing that reverse engineering and independent development are “proper means” of acquiring trade secrets; (3)

⁴ See Sharon K. Sandeen, *The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act*, 33 HAMLINE L. REV. 493, 504-20 (2010) [hereinafter Sandeen, *The Evolution of Trade Secret Law*].

⁵ See *id.* (detailing the history of the UTSA). As of the date of the publication of this Article, every state but New York and North Carolina has adopted the UTSA, although North Carolina has adopted a statute that is similar to the UTSA. See *Trade Secrets Laws and the UTSA – A 50 State and Federal Law Survey Chart (updated for Massachusetts)*, FAIR COMPETITION LAW (Aug. 10, 2018), <https://www.faircompetitionlaw.com/2018/08/10/trade-secrets-laws-and-the-utsa-a-50-state-and-federal-law-survey-chart-updated-for-massachusetts/> [https://perma.cc/J5FG-EV3Q] (last visited Mar. 25, 2019).

⁶ Sandeen, *The Evolution of Trade Secret Law*, *supra* note 4, at 542.

⁷ *Id.* at 508-09.

rejecting the concept of perpetual injunctions; and (4) precluding other tort claims for the misappropriation of “competitively significant information.”⁸

Internationally, trade secret harmonization efforts did not emerge until the late 1980s during negotiations that ultimately led to the World Trade Organization Agreement on Trade-related Aspects of Intellectual Property Law (TRIPS Agreement).⁹ However, the only major accomplishment of those negotiations in relation to trade secret law was to add the misappropriation of “undisclosed information” to a list of unfair methods of competition that were already precluded by Article 10*bis* of the *Paris Convention*.¹⁰ The TRIPS Agreement provides few specifics aside from a definition of “undisclosed information” and a footnote which lists wrongful acts.¹¹ In pertinent part, Article 39.2 of the TRIPS Agreement requires that: “Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices.”¹²

Between 1994, when the TRIPS Agreement entered into force, and 2010 there were few additional efforts to harmonize trade secret law. Two post-2010 exceptions include efforts by the USTR to include more robust trade secret provisions in the (now abandoned) Trans-Pacific Partnership Agreement and the recently concluded United States-Canada-Mexico Agreement.¹³ In the early 2010s, business interests sowed the seeds for more widespread trade secret harmonization efforts when they became increasingly concerned about threats to their trade secrets, particularly from foreign interests.¹⁴ Three events likely

⁸ See generally *id.*

⁹ General Agreement on Tariffs and Trade - Multilateral Trade Negotiations (The Uruguay Round): Agreement on Trade-Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods, Dec. 15, 1993, 33 I.L.M. 81 (1994) [hereinafter TRIPS Agreement]. See also SHARON K. SANDEEN, *The Limits of Trade Secret Law: Article 39 of the TRIPS Agreement and the Uniform Trade Secrets Act on Which It Is Based*, in THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH 537 (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2011) [hereinafter SANDEEN, *The Limits of Trade Secret Law*] (presenting a detailed history of Article 39 of the TRIPS Agreement).

¹⁰ SANDEEN, *The Limits of Trade Secret Law*, *supra* note 9, at 552.

¹¹ TRIPS Agreement, *supra* note 9, at §7, art. 39.2, art. 39.2 n.10.

¹² *Id.*

¹³ See Agreement Between the United States of America, the United Mexican States, and Canada, arts. 20.70-20.78, Nov. 30, 2018, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/20_Intellectual_Property_Rights.pdf [<https://perma.cc/7PMM-PFU4>].

¹⁴ This is reflected in the 2012 Special 301 Report, an annual report on international IP protection and enforcement prepared by the U.S. Trade Representative. For the first time, it included a separate heading reporting on the trade secret misappropriation concerns of U.S. businesses, stating in part: “U.S. companies are experiencing an increase in the theft of their trade secrets outside of the U.S. The United States urges its trading partners to ensure that they have robust systems for protecting trade secrets, including deterrent penalties for criminal

precipitated these concerns. First, the economic downturn caused by the international financial crisis of late 2008 and the subsequent belief of many countries and companies that innovation could be the answer to their economic woes.¹⁵ Second, China's adoption of its Twelfth [Five-year] Plan (2011-2015) in early 2011, the theme of which was "scientific development" with a commitment to increasing China's technological knowledge and capabilities.¹⁶ Third, in 2009, DuPont (a key player in trade secret harmonization efforts) initiated a lawsuit against a South Korean company, Kolon Industries, Inc., alleging that trade secrets related to its Kevlar technology had been stolen.¹⁷

In the EU, trade secret harmonization efforts were apparently sparked by the formation of the Trade Secrets & Innovation Coalition (TSIC) represented by Thomas Tindemans, first of the law firm of White & Case and later with Hill & Knowlton Strategies.¹⁸ Although it is not entirely clear why TSIC was formed, its formation coincided with the 2010 issuance of the European Commission's *Europe 2020* strategy which, while not mentioning trade secrets, focused on strategies to get the EU out of its economic doldrums.¹⁹ In a March 2010 letter to Margot Froehlinger, then the Director of the European Commission unit dealing with intellectual property rights, Mr. Tindemans wrote:

In these difficult times R&D efforts are being undermined by products resulting from trade secret theft entering the European market. The implementation of the coalition's proposals, namely (i) that the Commission publicly recognise the protection and enforcement of trade secrets and (ii) ultimately the harmonisation at European level, would go a long way towards alleviating this pressure.²⁰

trade secret theft." Office of the UNITED STATES TRADE REPRESENTATIVE, 2012 SPECIAL 301 REPORT (Apr. 2012), *available at* https://ustr.gov/sites/default/files/2012%20Special%20301%20Report_1.pdf.

¹⁵ See *infra*, note 17.

¹⁶ See *China's Twelfth Five Year Plan (2011-2015) - the Full English Version*, CBI CHINA DIRECT (May 11, 2011), https://cbi.typepad.com/china_direct/2011/05/chinas-twelfth-five-new-plan-the-full-english-version.html [<https://perma.cc/LNG6-PDT3>].

¹⁷ See *E.I. duPont de Nemours & Co. v. Kolon Indus.*, 688 F. Supp. 2d 443, 447 (E.D. Va. 2009) (detailing the alleged facts and the initiation of the lawsuit).

¹⁸ Nick Mathiason, *A Lobbying Masterclass: The Inside Story of How Big Business Worked with Lobbyists to Influence the EU in Drawing Up Controversial Trade Secret Proposals*, THE BUREAU OF INVESTIGATIVE JOURNALISM (Apr. 28, 2015), <http://labs.thebureauinvestigates.com/a-lobbying-masterclass/> [<https://perma.cc/27V5-UWG4>] (last visited Mar. 27, 2019).

¹⁹ *EUROPE 2020: A Strategy for Smart, Sustainable and Inclusive Growth*, at 3, COM (2010) 2020 final (Mar. 3, 2010), <http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf> [<https://perma.cc/944X-PRZK>].

²⁰ Mathiason, *supra* note 18.

This led to a *Report on Trade Secrets for the European Commission*,²¹ a follow-on June 2012 conference,²² and public consultations that occurred between December 2012 and March 2013.²³ In April 2013, the European Commission issued another study titled, *Study on Trade Secrets and Confidential Business Information in the Internal Market*,²⁴ followed by two reports commissioned by the Organisation for Economic Cooperation and Development (OECD) in 2013 examining the sufficiency of trade secret law in a cross-section of countries, both within and outside of the EU.²⁵

The foregoing reports and efforts ultimately led the EU to conclude that it would benefit from harmonized trade secret laws to replace the varied trade secret principles of EU-Member states and a draft Trade Secret Directive was developed. From the beginning, the proposed Trade Secret Directive was modeled after U.S. law and, thus, reflected many of the limitations on trade secret protection that are a part of the U.S. law.²⁶ In addition, various non-

²¹ Hogan Lovells Int'l LLP, *Study on Trade Secrets and Parasitic Copying (Look-alikes): Report on Trade Secrets for the European Commission*, at 1, MARKT/2010/20/D (Sept. 23, 2011)

<https://publications.europa.eu/en/publication-detail/-/publication/068c999d-06d2-4c8e-a681-a4ee2eb0e116/language-en/format-PDF/source-97009744#>.

²² *Report European Commission Conference of 29 June 2012 "Trade Secrets: Supporting Innovation, Protecting Know-How"*, at 1, Ref. Ares(2016)97937 (Aug. 1, 2016), [https://ec.europa.eu/docsroom/documents/14836/attachments/1/translations/en/renditions/pdf\[https://perma.cc/3R3Q-8DCP\]](https://ec.europa.eu/docsroom/documents/14836/attachments/1/translations/en/renditions/pdf[https://perma.cc/3R3Q-8DCP]).

²³ Eur. Comm'n Directorate Gen. Internal Mkt. & Serv., *Public Consultation on the Protection Against Misappropriation of Trade Secrets and Confidential Business Information: Summary of Responses*, at 2 (last updated Jan. 3, 2018), [http://ec.europa.eu/DocsRoom/documents/14837/attachments/1/translations/en/renditions/native\[https://perma.cc/NS2X-VM9X\]](http://ec.europa.eu/DocsRoom/documents/14837/attachments/1/translations/en/renditions/native[https://perma.cc/NS2X-VM9X]).

²⁴ Eur. Comm'n, *Study on Trade Secrets and Confidential Business Information in the Internal Market*, EUROPEAN COMMISSION (Dec. 7, 2013), [http://ec.europa.eu/growth/content/study-trade-secrets-and-confidential-business-information-internal-market-0_en\[https://perma.cc/BQ5C-ZZ7P\]](http://ec.europa.eu/growth/content/study-trade-secrets-and-confidential-business-information-internal-market-0_en[https://perma.cc/BQ5C-ZZ7P]). [hereinafter *EC Study*].

²⁵ Mark F. Schultz & Douglas C. Lippoldt, *Approaches to Protection of Undisclosed Information (Trade Secrets): Background Paper*, in OECD TRADE POLICY PAPERS NO. 162 (2014), [https://www.oecd-ilibrary.org/docserver/5jz9z43w0jnw-en.pdf?expires=1554033961&id=id&accname=guest&checksum=298C20AFEC63E00FD871B57FD0E2606F\[https://perma.cc/3R8A-YWSA\]](https://www.oecd-ilibrary.org/docserver/5jz9z43w0jnw-en.pdf?expires=1554033961&id=id&accname=guest&checksum=298C20AFEC63E00FD871B57FD0E2606F[https://perma.cc/3R8A-YWSA]); Douglas C. Lippoldt & Mark F. Schultz, *Uncovering Trade Secrets – An Empirical Assessment of Economic Implications of Protection of Undisclosed Data*, in OECD TRADE POLICY PAPERS NO. 167 (2014), [https://www.oecd-ilibrary.org/docserver/5jxzl5w3j3s6-en.pdf?expires=1554033990&id=id&accname=guest&checksum=FFFE506394DBEA8E86E1A771085E4818\[https://perma.cc/Q72Z-4J4L\]](https://www.oecd-ilibrary.org/docserver/5jxzl5w3j3s6-en.pdf?expires=1554033990&id=id&accname=guest&checksum=FFFE506394DBEA8E86E1A771085E4818[https://perma.cc/Q72Z-4J4L]).

²⁶ Sharon K. Sandeen, *Trade Secret Harmonization and the Search for Balance*, in THE INTERNET AND THE EMERGING IMPORTANCE OF NEW FORMS OF INTELLECTUAL PROPERTY 223 (Susy Frankel & Daniel Gervais eds., 2016).

governmental organizations (NGOs) lobbied for clearer or additional limitations that are reflected in both the Directive's recitals and text.²⁷

In the U.S., the Center for Responsible Enterprise and Trade ("CREATe.org") — a U.S.-based NGO founded in October of 2011 — published a 2012 White Paper on Trade Secret theft.²⁸ Then, in February 2013, Mandiant, a cybersecurity firm, issued a report concerning state-sponsored cyberespionage and trade secret theft.²⁹ One day later, the Executive Office of the President of the United States issued the *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* in which President Obama promised to "coordinate and improve" efforts to protect U.S. innovation, including trade secrets.³⁰ This flurry of activity was apparently the impetus for the creation of a U.S.-based affinity group similar to TSIC known as the Protect Trade Secrets Coalition, which was represented before the U.S. Congress by the law firm of Covington & Burling.³¹

At the same time efforts were underway to sway policymakers and public opinion toward greater harmonization of trade secret law through the issuance of reports and studies, legislation to do just that was introduced in both the U.S.

²⁷ 65 European organizations call on MEPs to revise the Trade Secrets Directive, EUROPEAN FED'N OF JOURNALISTS (Jun. 12, 2015), <https://europeanjournalists.org/blog/2015/06/12/trade-secrets-directive-65-european-organisations-call-on-meps-to-revise-text/> [http://perma.cc/MHN6-NJ7N].

²⁸ See *Trade Secret Theft: Managing the Growing Threat in Supply Chains*, CTR. FOR RESPONSIBLE ENTER. & TRADE (May 1, 2012), <https://create.org/resource/trade-secret-theft-managing-the-growing-threat-in-supply-chains/> [https://perma.cc/7AQD-BYMA].

²⁹ See, e.g., *APT1: Exposing One of China's Cyber Espionage Units*, MANDIANT, (Feb. 19, 2013), <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf> [http://perma.cc/TT79-FU9W].

³⁰ See *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, EXEC. OFF. OF THE PRESIDENT (2013), https://obamawhitehouse.archives.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf [http://perma.cc/NA3N-5RZG].

³¹ See *Protect Trade Secrets Coalition*, CTR. FOR RESPONSIVE POL., <https://www.opensecrets.org/lobby/clientsum.php?id=F204789&year=2016> [http://perma.cc/PL8G-AF3A] (last visited Oct. 27, 2018) (disclosing that the Protect Trade Secrets Coalition spent \$500,000 in 2014, \$520,000 in 2015, and \$250,000 in 2016). See also Isaac Arnsdorf, *How A Bill (With Virtually No Opposition Still Takes Two Years Before It Almost) Becomes a Law (in 2016)*, POLITICO (May 9, 2016, 2:00 PM), <https://www.politico.com/tipsheets/politico-influence/2016/05/how-a-bill-with-virtually-no-opposition-still-takes-two-years-before-it-almost-becomes-a-law-in-2016-214194#> [http://perma.cc/4RTW-D2V5] (listing nearly 30 lobbyists who worked in favor of the DTSA's passage); Letter from 36 Organizations with an Interest in Trade Secret Protection to Brent J. Fields, Sec'y, Sec. & Exch. Comm'n (Aug. 8, 2016), <https://www.sec.gov/comments/s7-06-16/s70616-352.pdf> [http://perma.cc/586B-RRKT] (prepared with the assistance of Covington & Burling). The founder of CREATe.org formerly worked for Covington & Burling. *CREATe Team*, CTR. FOR RESPONSIBLE ENTER. & TRADE, <https://create.org/about/create-team/> [https://perma.cc/L9LP-WX5B] (last visited May 16, 2019).

and EU. The DTSA traces its origins to a proposal first introduced in the U.S. 112th Congress (2011-2012) in an amendment that Senator Chris Coons of Delaware (the corporate home of DuPont, a proponent of greater protection for trade secrets) offered to a currency manipulation bill.³² The following year, Senator Coons, together with Senators Herb Kohl and Sheldon Whitehouse introduced a standalone bill labeled the Protecting American Trade Secrets and Innovation Act of 2012.³³ There followed similar proposals in both the 113th (2013-2014)³⁴ and 114th Congresses (2015-2016),³⁵ ultimately resulting in enactment of the DTSA on May 11, 2016, less than four weeks before the approval of the Trade Secret Directive.³⁶ In the EU, the first draft of what would become the Trade Secret Directive was proposed in November 2013,³⁷ with the Directive being adopted in June 2016 with a June 9, 2018 transposition deadline.

Although the DTSA is largely duplicative of the UTSA (which has now been adopted as state law by 48 of 50 states), its proponents believed it was necessary to give trade secret law more legitimacy and to enable trade secret owners to more easily bring a trade secret misappropriation claim in U.S. federal courts.³⁸ Prior to the DTSA's adoption, federal lawsuits for trade secret misappropriation could only be filed based upon the diversity jurisdiction of U.S. federal courts because there was no federal private right of action for trade secret misappropriation; after the DTSA's adoption, a federal lawsuit can now be filed based upon federal question jurisdiction. However, the DTSA: (1) does not preempt applicable state law; (2) has a jurisdictional requirement that is not applicable to cases brought under the UTSA; and (3) does not grant federal

³² 157 CONG. REC. S6229-30 (daily ed. Oct. 5, 2011) (statement of Sen. Coons introducing S. Amend. 729, Currency Exchange Rate Oversight Reform Act of 2011, S. 1619, 112th Cong. (2011)).

³³ S. 3389, 112th Cong. (2012).

³⁴ See Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (2014); Trade Secrets Protection Act of 2014, H.R. 5233, 113th Cong. (2014); Private Right of Action Against Theft of Trade Secrets Act of 2013, H.R. 2466, 113th Cong. (2013); Future of American Innovation and Research Act of 2013, S. 1770, 113th Cong. (2013).

³⁵ Defend Trade Secrets Act of 2015, S. 1890, 114th Cong. (2015); Defend Trade Secrets Act of 2015, H.R. 3326, 114th Cong. (2015).

³⁶ Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (2016).

³⁷ *Commission Proposal for a Directive of the European Parliament and of the Council on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure*, COM (2013) 813 final (Nov. 28, 2013), <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0813:FIN:EN:PDF> [https://perma.cc/D7NA-W5XR].

³⁸ See, e.g., R. Mark Halligan, *Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 7 J. MARSHALL REV. INTELL. PROP. L. 656 (2008).

courts exclusive jurisdiction.³⁹ This means that most trade secret cases in the U.S., whether brought in federal or state court, now include claims under both the DTSA and the UTSA and many such cases are still filed in state court. It also means that much of U.S. trade secret law will continue to be governed by state law; the principal difference between the DTSA and UTSA being the *ex parte* civil seizure provision of the DTSA.⁴⁰

Additional U.S. efforts to harmonize trade secret law have been pursued more directly by the USTR through direct appeals to countries (such as China and Japan), the use of FTAs, and the *Special 301 Report* that the USTR issues annually.⁴¹ In fact, the harmonization of trade secret standards was listed as an objective of the USTR in the November 2017, *Summary of Objectives for NAFTA Renegotiations*.⁴²

B. U.S. TRADE SECRET LAW: WHAT IT IS AND IS THOUGHT TO BE

The general contours of U.S. trade secret law are well understood by most trade secret harmonization proponents and are incorporated into the Trade Secret Directive.⁴³ Both the UTSA and DTSA provide specified remedies, including preliminary and permanent injunctive relief, if information, as defined: (1) meets the three requirements of trade secrecy; and (2) has been “misappropriated.”⁴⁴ The definition of a “trade secret” is stated in both positive and negative terms and is limited.⁴⁵ While trade secrets can theoretically include all types of information, including negative information, information that is “generally

³⁹ Sharon K. Sandeen & Christopher B. Seaman, *Toward a Federal Jurisprudence of Trade Secret Law*, 32 BERKELEY TECH. L.J. 829, 849 (2017).

⁴⁰ *See id.* at 901.

⁴¹ The first Special 301 Report to mention trade secrets under the heading “Trade Secrets and Forced Technology Transfer” was issued by the USTR in April 2012. OFF. OF THE U.S. TRADE REPRESENTATIVE, 2012 SPECIAL 301 REPORT 17 (2012), https://ustr.gov/sites/default/files/2012%20Special%20301%20Report_0.pdf [https://perma.cc/5N3N-T8PF]. The lax enforcement of existing trade secret laws and the lack of harmonization with U.S. trade secret law has been a subject of those reports since that date. *See, e.g.*, OFF. OF THE U.S. TRADE REPRESENTATIVE, 2018 SPECIAL 301 REPORT 5 (2018), <https://ustr.gov/sites/default/files/files/Press/Reports/2018%20Special%20301.pdf> [https://perma.cc/NMV7-8YNM].

⁴² OFF. OF THE U.S. TRADE REPRESENTATIVE, SUMMARY OF OBJECTIVES FOR THE NAFTA RENEGOTIATIONS 9 (Nov. 2017), <https://ustr.gov/sites/default/files/files/Press/Releases/Nov%20Objectives%20Update.pdf> (“Seek provisions governing intellectual property rights that reflect a standard of protection similar to that found in U.S. law, including, but not limited to protections related to trademarks, patents, copyright and related rights (including, as appropriate, exceptions and limitations), undisclosed test or other data, and trade secrets.”).

⁴³ *See* Sharon K. Sandeen, *Implementing the EU Trade Secret Directive, A View from the United States*, EUROPEAN IP REVIEW (2016).

⁴⁴ UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM’N 1985) [hereinafter UTSA].

⁴⁵ *Id.*

known” or “readily ascertainable” cannot be a trade secret.⁴⁶ Moreover, the secrecy of information, alone, does not make it a trade secret.⁴⁷ The subject of the information must also have “independent economic value” that is derived from its secrecy and it must be the subject of efforts that are “reasonable under the circumstances” to maintain its secrecy.⁴⁸ In the U.S., the economic value requirement serves to ensure that the subject information has value generally, but also requires that it would be of value to others.⁴⁹ The reasonable efforts requirement also serves two functions: first, it provides evidence that the putative trade secret owner valued the information before it was allegedly misappropriated (the veracity function); and, second, it provides notice to the individuals and entities that come into contact with the information that it should be handled confidentially (the notice function).⁵⁰

Although the definitions of misappropriation contained in the UTSA and DTSA are convoluted, they generally prohibit the disclosure or use of trade secrets in breach of a duty of confidentiality and the acquisition of trade secrets by “improper means.”⁵¹ Embedded in the definition of misappropriation is the possibility that third parties who are one or more degrees removed from the original act of misappropriation might also be held liable due to their subsequent acquisition, disclosure, or use of the subject information, depending upon their knowledge.⁵² Unlike the Trade Secret Directive, neither the UTSA or the DTSA proscribe a wrong related to importation, although the U.S. International Trade Commission has interpreted its authority to allow it to stop goods containing misappropriated trade secrets from flowing into the U.S.⁵³

Misunderstandings concerning the scope and application of U.S. trade secret law most often arise with respect to the following issues: (1) the identity and parameters of unprotected information, including the meanings of “generally known,” “readily ascertainable,” and “general skill and knowledge,” as well as the scope and meaning of so-called combination trade secrets; (6) the meaning of the reasonable efforts requirement; (3) how duties of confidentiality are created; (4) the requirement of harm, particularly for an award of monetary damages; (5) the fleeting nature of trade secrets; and (6) the application of ancillary limitations on the enforcement of trade secret rights, including freedom of speech and the press.

Each of these issues is explained in more detail in the following subsections, but at this point it is important to emphasize that a characteristic of all the listed issues is that they require knowledge of legal principles that are not contained in

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² *Id.*

⁵³ *Id.* at § 1(2).

the statutory language of the UTSA and DTSA. As further explained below, reference to some of this law may be found in the UTSA and DTSA, particularly the commentary to the UTSA, but often it can only be found in relevant case decisions and other statutes. Thus, those who do not take the time to find and understand this non-statutory body of U.S. trade secret law are apt to misunderstand and misapply U.S. trade secret law. Additionally, because U.S. trade secret law was significantly changed by the UTSA, case decisions that predate the adoption of the UTSA by each state may be wholly irrelevant.

1. *The identity and parameters of unprotected information*

Many people make the mistake of thinking that all confidential business information qualifies for trade secret protection and are uncomfortable with the notion that someone could take (they would say “steal”) confidential information from a business and not be held liable for trade secret misappropriation. A recent example is the media coverage surrounding Waymo’s (a Google company) lawsuit against Uber in which it alleged that Uber had received over 140,000 proprietary files originally misappropriated by a former employee of Waymo.⁵⁴ Most media accounts emphasized the “theft” of the files,⁵⁵ but as the case proceeded the presiding Judge ruled that many of the allegedly misappropriated documents were not trade secrets.⁵⁶ One reason for this disconnect is the rhetorical and sensationalistic value of claims of trade secret theft, but it is also due to the incorrect assumption that trade secrets or, more broadly, information, are property in the same way that a hammer is property. Although trade secrets are treated like property in the U.S. in many contexts — *e.g.*, they can be sold, licensed, and taxed — they are a form of intangible property rights the metes and bounds of which are defined by the law that created them.

The principles of law that often lead people astray concerning the scope of U.S. trade secret protection relate to the concomitant definition of unprotected information. As already noted, the definition of a trade secret does not include information that is “generally known” or “readily ascertainable,” but it is likely that many people do not know what these terms actually mean. The term

⁵⁴ Waymo LLC v. Uber Technologies, Inc., 870 F.3d 1350 (Fed. Cir. 2017).

⁵⁵ See, *e.g.*, Charles Duhigg, *Did Uber Steal Google’s Intellectual Property?*, THE NEW YORKER (Oct. 15, 2018), <https://www.newyorker.com/magazine/2018/10/22/did-uber-steal-googles-intellectual-property> [<https://perma.cc/R5MM-XAKZ>].

⁵⁶ See Waymo LLC v. Uber Techs., Inc., No. C 17-00939 WHA, 2017 WL 2123560, at *8 (N.D. Cal. May 15, 2017) (“That being said, Waymo has shown at least serious questions going to the merits concerning whether *some* information within the 14,000-plus downloaded files has been used by defendants and qualifies for trade secret protection.”) (emphasis in the original); Sarah Jeong, *I’m not so sure Waymo’s going to win against Uber*, THE VERGE (Feb. 8, 2018, 6:39 PM) <https://www.theverge.com/2018/2/8/16993208/waymo-v-uber-trial-trade-secrets-lidar> [<https://perma.cc/K47S-CKVF>] (“Waymo originally asserted that over a hundred trade secrets had been misappropriated by Uber — that’s been narrowed down to eight.”).

“generally known” does not just refer to information that is “known by the general public;” more broadly, it refers to information that is generally known among those who can benefit from it.⁵⁷ Thus, while most members of the public may not know how to drill an oil well, information about oil well drilling that is known in that industry is considered “generally known” for trade secret purposes. Information that is “readily ascertainable” is not generally known but is “knowable” by reference to publicly available information. How easily and where this information can be found is the critical question, with U.S. court often applying a definition that is similar to the definition of “prior art” under patent law.⁵⁸

Two other principles of U.S. trade secret law (that are admittedly more obscure) also limit the scope of protectable trade secret information. The first is the concept of “general skill and knowledge.” For important public policy reasons largely borrowed from English common law, the U.S. has long recognized the public interest in the development and growth of its citizens, including through work experience.⁵⁹ Thus, employees can learn and grow on the job, eventually taking their new-found skills and knowledge with them to future jobs.⁶⁰ The key, of course, is determining what constitutes “general” skill and knowledge versus the “special” skill and knowledge that might be the legitimate trade secrets of the employer. Proper application of the reasonable efforts requirement helps as those efforts should define what the employer claims as a trade secret, but often the analysis comes down to a question of the relative equities. A practical reality that harmonization advocates often miss with respect to this issue is that courts are unlikely to classify information as a trade secret if employers do not make a claim to it, particularly if the information was created by the employee. Issues of trade secret ownership can also arise.

The final (and second obscure) definitional principle relates to the previous three: trade secrets in the U.S. cannot be created by contract.⁶¹ Rather, trade secrets have an independent legal existence as previously defined. Thus, the mere fact that a person or company agrees to keep specified information confidential does not mean that information constitutes trade secrets; secrecy is only one of three requirements for trade secret protection. The rub, however, is that (as further explained in the next subsection) written nondisclosure agreements (NDAs) are frequently at issue in trade secret litigation, possibly

⁵⁷ UTSA, *supra* note 44, at § 1.

⁵⁸ UTSA, *supra* note 44, at § 1, cmt. (“Information is readily ascertainable if it is available in trade journals, reference books, or published materials. Often, the nature of a product lends itself to being readily copied as soon as it is available on the market.”)

⁵⁹ See William L. Letwin, *The English Common Law Concerning Monopolies*, 21 U. Chi. L. Rev. 355 (1954); see also, e.g., *Hamilton Mfg. Co. v. Tubbs Mfg. Co.*, 216 F. 401, 406 (C.C.W.D. Mich. 1908).

⁶⁰ See Camilla A. Hrdy, *The General Knowledge, Skill, and Experience Paradox*, 60 B.C. L. REV. (forthcoming).

⁶¹ UTSA, *supra* note 44, at § 1.

leading individuals uneducated about the nuances of U.S. trade secret law to believe that NDAs can define the scope of trade secret protection. While NDAs are useful as a means to specify what a business claims as a trade secret and as evidence of the required reasonable efforts, they are not definitive on what information actually qualifies as a trade secret. Further adding to this area of misunderstanding is the fact that (provided the subject information is not generally known or readily ascertainable and does not consist of general skill and knowledge) NDAs can be used to create a *contractual* duty of confidentiality for information not qualifying as a trade secret. In such cases, however, the NDA creates a potential breach of contract claim against parties to the contract; it does not turn non-trade secret information into a trade secret and cannot be the basis of a claim against those who are not in privity of contract.

The definition of a trade secret that is contained in the Trade Secret Directive is consistent with the foregoing legal principles and does not appear to give EU-Member countries much flexibility to expand or narrow the definition of a trade secret.⁶² However, it is possible that EU-Member countries may define information that is “generally known,” “readily ascertainable” and “general skill and knowledge” differently than in the U.S., depending upon the values of each country. Additionally, the definition of “combination trade secrets” (involving a possible “unique” or “improved” combination of known information) will need to be defined; under U.S. law, this is a messy and largely unsettled issue.⁶³ Although, unlike U.S. law, Article 2.4 of the Trade Secret Directive contains a statutory definition of combination trade secrets, it is not particularly helpful in explaining how generally known or readily ascertainable information must be combined or altered to be protectable.⁶⁴ Also, except for Article 1.3(a), it is not clear to what extent the Directive will allow non-trade secret information to be protected either by contract or based upon other theories of law. Where the UTSA explicitly precludes all claims for relief (except breach of contract claims) for the alleged misappropriation of “competitively significant secret information,”⁶⁵ the Trade Secret Directive does not contain a similar provision and does not explicitly require EU-Member states to rescind laws that previously provided protection for confidential or secret business information.

2. *The meaning of the reasonable efforts requirement*

A common point of consternation voiced by trade secret owners concerns how countries and their courts define the “reasonable efforts” requirement of trade secret law. Understandably, trade secret owners want the bar set low when determining “reasonable efforts” so that more information can be protected as a trade secret with less efforts. When countries and courts focus on the veracity

⁶² EU Trade Secret Directive, *supra* note 3, at art. 2.

⁶³ Tait Graves & Alexander Macgillivray, *Combination Trade Secrets and the Logic of Intellectual Property*, 20 SANTA CLARA COMPUT. & HIGH TECH. L.J. 261, 261 (2004).

⁶⁴ EU Trade Secret Directive, *supra* note 3, at art. 2.4.

⁶⁵ UTSA, *supra* note 44, at § 7, cmt.

and notice functions of the reasonable efforts requirement, however, the bar is often set higher and businesses become frustrated that the information they classify as trade secrets are not treated as such. This is the current state of the law in the U.S., with some courts finding that a company's protective efforts are reasonable when other courts do not.⁶⁶ The existence of differences of opinion relates principally to the fact that the requirement is highly contextual and subjective, but it is also due to the difficulties and costs of keeping information "relatively secret" while still engaging in robust (and often international) commerce. In this regard, reasonable efforts are often needed both internally, with respect to a business' own operations and externally with respect to the operations of a business' suppliers, vendors, and licensees. Sometimes, companies do a reasonable job protecting internal information, but not external information, thereby resulting in findings of a lack of reasonable efforts.⁶⁷

Another reality is that businesses tend to abhor attempts to make the reasonable efforts requirement more objective, preferring application of a fluid and amorphous definition that gives businesses a chance to prove the existence of trade secrets in cases where they have instituted few protective measures. This was reflected, for instance, in complaints concerning objective factors instituted by Japan for the purpose of both helping Japanese companies protect their trade secrets and assisting Japanese courts in applying the reasonable efforts requirement. It is also reflected in the criticism of countries that require express confidentiality agreements because such a requirement is seen as foreclosing other efforts that should be deemed reasonable enough. Moreover, if businesses had their way it seems that the reasonable efforts standard would change depending upon the egregiousness of the defendant's actions; the more egregious they are, the less protective efforts that should be required.

Unfortunately, there is nothing in the UTSA, DTSA, or U.S. case law that can provide EU-Member countries much guidance on this critical issue. As a result, all EU-Member countries are vulnerable to criticism by companies and the USTR if they believe they apply the reasonable efforts requirement too stringently. On the other hand, if the reasonable efforts requirement is applied too liberally, countries are bound to be criticized by NGOs for protecting information that should be deemed to have entered the public domain. There may, however, be a middle ground that can be developed. At a high level, there does seem to be a difference between the efforts that should be required for information that is voluntarily shared with another, like an employee or vendor.

At a minimum, the recipient of the information should be informed of the information that is claimed as a trade secret (the notice function of the requirement) and best practices suggest that an express or implied-in-fact confidentiality agreement should be required. Information that is unlawfully

⁶⁶ Sharon K. Sandeen and Elizabeth A. Rowe, *TRADE SECRET LAW CASES AND MATERIALS* ch. 5 (2017) (discussing cases).

⁶⁷ Elizabeth A. Rowe, *Contributory Negligence, Technology, and Trade Secrets*, 17 *GEO. MASON L. REV.* 1, 11, n.75 (2009) (citing cases).

acquired by another might be the subject of a lesser reasonable efforts requirement, although as a practical matter, no business should put itself in the position of making such an argument. Moreover, a public policy argument may be made (consistent with the security of data more generally) that companies should be required to engage in reasonable self-help measures to prevent computer hacking and other forms of information theft.

3. *Establishing duties of confidentiality.*

The historical origins of U.S. trade secret law reveal that trade secret misappropriation is an act of unfair competition that usually arises from the breach of a duty of confidence; its classification as a quasi-property right (or intellectual property right) came later.⁶⁸ The “acquisition by improper means” prong of trade secret misappropriation is of even more recent vintage and by comparison has not developed as much, or as well, as the breach of confidence variety.⁶⁹ This is due to the fact that the majority of trade secret claims in the U.S. concern present or former employees and not the acts of foreign espionage and intrigue that are frequently cited as justifying trade secret harmonization efforts.⁷⁰ With this background, it is easy to see how trade secret harmonization advocates might conclude that a country is not complying with its obligations. The creation of duties of confidentiality is governed by legal principles that typically exist separate and apart from trade secret law.⁷¹ Adopting a “harmonized” trade secret law does nothing to harmonize the law that results in the creation of duties of confidentiality.

Even in the U.S., the law concerning the creation of duties of confidentiality is not harmonized because it is primarily based upon state law and there are 50 different states with different sets of law, including statutes that may create duties of confidentiality “as a matter of law.” In the absence of a statute, the

⁶⁸ Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 316 (2008) (“The doctrine of trade secrets evolved out of a series of related common law torts: breach of confidence, breach of confidential relationship, common law misappropriation, unfair competition, unjust enrichment, and torts related to trespass or unauthorized access to a plaintiff’s property”).

⁶⁹ See Sharon K. Sandeen, *Out of Thin Air: Trade Secrets, Cybersecurity, and the Wrongful Acquisition Tort*, 19 MINN. J.L. SCI. & TECH. 373, 375-77 (2018) [hereinafter Sandeen, *Out of Thin Air*].

⁷⁰ David S. Levine & Christopher B. Seaman, *The DTSA at One: An Empirical Study of the First Year of Litigation Under the Defend Trade Secrets Act*, 53 WAKE FOREST L. REV. 105, 112 (2018) (“While cyberespionage often results in headline-grabbing stories, previous studies have shown that the bulk of trade secret litigation involves more mundane misconduct—a rogue employee who departs with trade secret information and joins a competitor or launches a new company. . . . In short, instances of hacking and other intrusions, while high profile and often devastating to their victims, remain low compared to bread-and-butter departing employee claims.”).

⁷¹ Sandeen, *supra* note 66, ch. 7.

principal ways that duties of confidentiality are established under U.S. law are: (1) by an express contract, either written or oral; (2) by a contract that is implied-in-fact; (3) as a matter of law which, in the absence of a statute would be based upon case law such as that related to common law fiduciary duties; and (4) based upon so-called “quasi-contracts,” although use of that equitable theory has been precluded by section 7 of the UTSA.⁷² But even when an applicable duty of confidentiality exists, there is also the question of its scope. For instance, employers in U.S. trade secret cases frequently invoke the common law “duty of loyalty” in an attempt to establish a duty of confidentiality, but as the *Restatement of Employment Law* explains, a duty of confidentiality is not imposed on all employees and, where it exists, does not extend to the protection of non-trade secret or non-confidential information.⁷³ Without the establishment of an enforceable duty of confidentiality, the only trade secret claim that is available under U.S. law is for the acquisition of trade secrets by improper means,⁷⁴ but such a claim is often limited by the requirement of harm.⁷⁵

Because of the foregoing it is advisable for trade secret owners to create duties of confidentiality by contract, preferably documented in a writing. But despite this well-known advice, some trade secret harmonization advocates have criticized the trade secret laws of countries that require express confidentiality agreements. Such a requirement, however, is not far removed from applicable U.S. law that frequently requires the existence of either an express or implied-in-fact contracts.⁷⁶ Thus, the more critical question is: In the absence of an express contract or a duty of confidentiality imposed as a matter of law, how easy should it be to establish a duty of confidentiality with respect to trade secrets? Some commentators in the U.S. have argued that the mere sharing of information under circumstances where the recipient of the information should know that confidentiality was expected is enough,⁷⁷ but such a low threshold seems inconsistent with the reasonable efforts requirement of the UTSA and DTSA and the law governing the establishment of implied contractual duties.

The ways by which duties of confidentiality are formed is an issue that all EU-Member countries should consider; the UTSA, the TRIPS Agreement, the

⁷² See, e.g., *Reeves v. Alyeska Pipeline Serv. Co.*, 926 P. 2d 1130, 1135 (Alaska 1996); UTSA, *supra* note 44, at § 7.

⁷³ RESTATEMENT OF EMP’T LAW, § 8.01 (AM. LAW INST. 2015) (explaining that the duty of loyalty only extends to trade secrets for employees that are not in a position of trust and confidence).

⁷⁴ UTSA, *supra* note 44, at §2.

⁷⁵ See *supra* Section B.4.

⁷⁶ See Deepa Varadarajan, *The Trade Secret-Contract Interface*, 103 IOWA L. REV. 1543, 1556 (2018).

⁷⁷ *Food Mktg. Inst. v. Argus Leader Media*, No. 18-481, 2019 WL 2570624, at *6 (U.S. June 24, 2019) (noting that traditional definitions of “confidential” use the term in two senses; one requiring that it only be closely held, and the other requiring assurances of confidentiality).

DTSA, and the Trade Secret Directive are silent on the issue.⁷⁸ It appears that the Trade Secret Directive both broadens and limits the scope of confidentiality agreements as compared to U.S. law. First, at least when compared to those in the U.S. who believe it is possible for duties of confidentiality to be created through the mere sharing of confidential information with knowledge or reason to know of the desire for confidentiality,⁷⁹ Article 4.3(b) of the Directive seems to require more; namely, a confidentiality agreement or a duty of confidentiality (presumably imposed by law).⁸⁰ However, Article 4.3(c) may not require a duty of confidentiality at all, but only “breach of a contractual or any other duty to limit the use of the trade secrets.”⁸¹

4. *The requirement of harm*

Anyone who has studied U.S. tort law knows that all tort claims include an element of harm.⁸² While the various torts define the requisite harm differently, and statutes such as the UTSA and DTSA may broaden the applicable measures of harm, some provable harm remains an essential requirement.⁸³ What trips up some U.S. trade secret harmonization advocates is failing to realize that the harm requirement can result in an unsuccessful trade secret case, even where strong evidence of the misappropriation of trade secrets is presented.⁸⁴ Thus, when they complain that a country is not enforcing trade secret law, they might not realize that the result of a given case may be because no cognizable harm was proven. This may seem unfair, but it is also an argument that U.S. businesses that have suffered data breaches usually assert to avoid liability.⁸⁵ Moreover, eliminating the requirement of cognizable harm would alter a centuries-old principle of tort law.

Fortunately for trade secret owners, the UTSA and DTSA changed the common law in two ways that make it easier for them to obtain relief, even when proof of harm is non-existent or sketchy. First, both statutes allow for the grant of preliminary and permanent injunctive relief to prevent the “actual and *threatened* misappropriation of trade secrets.”⁸⁶ This is a useful expansion of the common law in at least two scenarios: (1) where the defendant rightfully acquired trade secret information pursuant to a duty of confidentiality and there is evidence that he intends to breach his duty of confidentiality and disclose or use the trade secrets; and (2) where the defendant improperly acquires the

⁷⁸ See generally EU Trade Secret Directive, *supra* note 3; TRIPS Agreement, *supra* note 9; UTSA, *supra* note 44.

⁷⁹ *Food Mktg. Inst.*, 2019 WL 2570624, at *6, *7.

⁸⁰ See EU Trade Secret Directive, *supra* note 3, at art. 4.3(b).

⁸¹ *Id.* at art. 4.3(c).

⁸² See, e.g., RESTATEMENT (SECOND) OF TORTS § 7 (AM. LAW INST. 1965).

⁸³ See, e.g., *id.* See also UTSA, *supra* note 44, at §§ 1(2), 2 (a).

⁸⁴ Sandeen, *Out of Thin Air*, *supra* note 69, at 380-81.

⁸⁵ Sandeen, *Out of Thin Air*, *supra* note 69, at 400.

⁸⁶ 18 U.S.C. § 1836(b)(3)(A)(i) (2012); UTSA, *supra* note 44, at § 2.

subject trade secrets and thereafter threatens to disclose or use them. A related concern, largely unresolved in the U.S., is whether injunctive relief should be granted as a matter of course once trade secret misappropriation is proven or whether such relief should only be granted after considering the equities, including the public interest.

Second, both the UTSA and the DTSA have expanded the applicable measure of damages beyond what was allowed under U.S. common law to include (in addition to a measure of damages based upon plaintiff's provable losses) measures of damages based upon: (1) defendant's unjust enrichment; or (2) a reasonable royalty.⁸⁷ However, there is no monetary remedy available in the U.S. when trade secrets, although acquired by improper means, are not subsequently disclosed or used.⁸⁸ This is because trade secret misappropriation in the U.S. is not a trespassory tort entitling a plaintiff to an award of nominal damages and expanded theories of harm for wrongful acquisition have been slow to develop.

The EU Trade Secret Directive specifies remedies similar to those available under U.S. law, but with some notable and potentially problematic differences.⁸⁹ Articles 10 through 13 specify the conditions under which provisional and corrective injunctions can be granted, including a list of considerations that largely mirror the equitable and temporal considerations of U.S. law.⁹⁰ Article 13.3 allows the "person liable" to request an order of "pecuniary compensation" in lieu of the injunction allowed under Article 12 if specified conditions are met.⁹¹ Principal among them is the requirement that the "person liable" be a third party that "neither knew nor ought, under the circumstances, to have known that the trade secret was obtained from another who was using or disclosing the trade secret unlawfully."⁹² Under U.S. law, by contrast, no liability would attach to a third party unless they knew or had reason to know of the earlier misappropriation, effectively providing protection to bona fide purchasers and licensees of misappropriated trade secrets.⁹³

With respect to monetary relief, Article 14.1 of the Directive states that the trade secret holder is entitled to "damages appropriate to the actual prejudice suffered as a result of the unlawful acquisition, use or disclosure of the trade secrets."⁹⁴ Additionally, Article 14.2 indicates that both the trade secret holder's lost profits and the infringers unfair profits may be appropriate measures of

⁸⁷ 18 U.S.C. § 1836(b)(3)(B) (2012); UTSA, *supra* note 44, at § 3(a).

⁸⁸ *See id.* (requiring awards to be based on actual loss, unjust enrichment, and harm from unauthorized disclosure).

⁸⁹ *See* EU Trade Secret Directive, *supra* note 3, at arts. 10-14.

⁹⁰ *See id.* at arts. 10-13.

⁹¹ *Id.* at art. 13.3.

⁹² *Id.* at art. 13.3(a).

⁹³ *See* UTSA, *supra* note 44, at §1(2)(ii)(B).

⁹⁴ EU Trade Secret Directive, *supra* note 3, at art. 14.1.

damages.⁹⁵ Without stating directly whether unlawful appropriation is a trespassory claim, the Directive also allows for a measure of damages based upon “moral prejudice,”⁹⁶ which may allow for monetary recovery in cases where trade secrets are unlawfully acquired but not subsequently disclosed or used. If so, this provides the potential for monetary recovery in the EU where it does not exist in the U.S., except in rare cases where U.S. courts have taken an expansive view of trade secret harms.⁹⁷ A related question for the EU is what kind of activities constitute “unlawful acquisition”?

5. *The fleeting nature of trade secrets*

Another reality of U.S. trade secret law that often leads to misunderstanding involves the fleeting nature of trade secret rights; in particular, that trade secrecy can be lost due to no fault of the putative trade secret owner or an alleged misappropriator. This can happen because trade secret protection in the U.S., unlike patent and copyright protection, does not grant term-specified exclusive rights and because loss of secrecy results in the loss of trade secret rights.⁹⁸ In fact, the U.S. Supreme Court has recognized that trade secret law would interfere too much with the purposes of U.S. patent law if it was not leaky like a “sieve.”⁹⁹ This is one reason, U.S. trade secret law has long recognized that the acts of reverse engineering and independent development are “proper means” of acquiring trade secret information.¹⁰⁰ The analog to this rule is that if someone properly acquires information through reverse engineering or independent development and then makes that information “generally known” or “readily ascertainable,” their act of disclosure destroys the trade secrecy of the same information held by all others, even if that information continues to be treated confidentially by some.¹⁰¹ Consequently, the trade secret status of information often changes.

In the U.S., if information loses its status as a trade secret before the date of the alleged trade secret misappropriation, then any resulting trade secret case should be dismissed. If the information loses its status as a trade secret after the date of the alleged misappropriation, then available remedies should be affected. For instance, monetary damages and injunctive relief would be calculated for at least the applicable “lead time advantage” (that is the advantage that the defendant gained over potential third party competitors), but otherwise would not be available once the subject information ceases to be a trade secret.¹⁰²

⁹⁵ See *id.* at art. 14.2.

⁹⁶ *Id.*

⁹⁷ Sandeen, *Out of Thin Air*, *supra* note 69, at 377-78.

⁹⁸ See generally 18 U.S.C. § 1836 (2012); UTSA, *supra* note 44.

⁹⁹ *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 490 (1974).

¹⁰⁰ UTSA, *supra* note 44, at §1, cmt.

¹⁰¹ *Id.* at §2, cmt. (illustrating that result of a party reverse engineering a trade secret).

¹⁰² *Id.* at §§ 2-3, cmts.

The remedies provisions of the Trade Secret Directive are modeled after U.S. law and include the limitations on the scope of monetary and injunctive relief that are described above,¹⁰³ but the EU needs to work out the details. In this regard, procedural hurdles and the lack of robust discovery processes in other countries are often a source of consternation for U.S. trade secret owners. While the U.S.-led trade secret harmonization efforts have attempted to address some of these issues, a practical reality is that sometimes they cannot be addressed unless the entire legal system of a country is modified or special processes for trade secret cases are established. Moreover, in countries that have also enacted criminal laws to prohibit trade secret misappropriation, the prosecution of civil trade secret claims may be affected either positively or negatively; positively, because a criminal investigation may reveal important information about a case, but negatively because prosecution of the civil case may be delayed pending the conclusion of the criminal investigation.

6. *Ancillary limitations on the enforcement of trade secret rights*

In theory, at least, every type of intellectual property law balances the protection of intellectual property rights against other values, most notably the value of free competition.¹⁰⁴ As previously noted, both the UTSA and DTSA include several express limitations on the scope of trade secret protection, but it is important to recognize that other limitations exist in ancillary bodies of U.S. law.¹⁰⁵ This includes: (1) federal and state laws governing restraints on trade, including the enforceability of nondisclosure and noncompete agreements;¹⁰⁶ (2) common law rules and state and federal statutes governing the ownership and use of employee-created inventions and information;¹⁰⁷ (3) other employee rights, including the public's interest in employee mobility;¹⁰⁸ (4) the interrelationship of trade secret, patent, and copyright law, specifically whether trade secret protection should be discouraged in favor of patent and copyright protection, where applicable;¹⁰⁹ (5) the government's access to and use of trade secret information for regulatory purposes;¹¹⁰ and (6) the broader public interest,

¹⁰³ EU Trade Secret Directive, *supra* note 3, at arts. 11.3(b), 13.2 (referencing art. 2.1 to describe when information is no longer a trade secret).

¹⁰⁴ RESTATEMENT (THIRD) OF UNFAIR COMPETITION, *supra* note 61, at § 1.

¹⁰⁵ See discussion *supra* Section B.1.

¹⁰⁶ See, e.g., 15 U.S.C. § 1 (2012) (making restraint of trade or commerce illegal).

¹⁰⁷ See, e.g., 17 U.S.C. § 201(b) (2012) (ownership of copyrights for works made for hire).

¹⁰⁸ See, e.g., *Whyte v. Schlage Lock Co.*, 101 Cal. App. 4th 1443, 1461 (2002) (noting that, "[t]he decisions rejecting the inevitable disclosure doctrine correctly balance competing public policies of employee mobility and protection of trade secrets.").

¹⁰⁹ See *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 475-78, 490 (1974) (discussing the interconnection between trade secrets and patent law and that inventors are often more inclined to seek patent protection if possible).

¹¹⁰ See generally Elizabeth A. Rowe, *Striking A Balance: When Should Trade-Secret Law Shield Disclosures to the Government?*, 96 IOWA L. REV. 791 (2011) [hereinafter Rowe,

including with respect to government transparency, freedom of speech and the press, and whistleblowing activities.¹¹¹

There is a complex body of state and federal law in the U.S. on all the foregoing issues that cannot be fully explained in this article. Because of this complexity, and given the facially broad language of the UTSA and DTSA and the fact that a lot of the law that limits the scope and application of U.S. trade secret law is not directly expressed in those statutes, it is easy for government officials and harmonization advocates to miss those limitations. But neither the U.S., nor any other country can easily erase nor ignore applicable ancillary areas of law when doing so would undermine core principles, including human rights. Moreover, due to the lobbying efforts of both the proponents and opponents of the DTSA, specific references to two of these limitations are now included in the language of the DTSA.¹¹² First, a new “whistleblower immunity” that applies to all U.S. trade secret misappropriation claims, civil and criminal and state and federal, has been added.¹¹³ Second, a provision of the remedies section explicitly states that no injunction can issue except in accordance with applicable state law, which involves a range of approaches including California’s longstanding restrictions on the enforcement of noncompete agreements.¹¹⁴

While U.S. law requires an examination of different sources of law to fully understand the limits that are placed upon the meaning and application of trade secret law, the Trade Secret Directive specifically lists numerous limitations both in its recitals and in the text of the Directive itself.¹¹⁵ This includes:

1. Repeated statements that trade secret law should be applied in a manner that does not hinder employee mobility and preserves existing laws with respect to restrictions on competition;
2. Explicit recognition of the right of public officials to collect trade secret information and allow or require the disclosure of relevant information to the public;
3. A listing of information that cannot be protected as a trade secret, including trivial information and the experience and skills gained by employees in the normal course of their employment;

Striking a Balance] (discussing “the elaborate regulatory scheme of agency rules and regulations” relating to trade secrets disclosed to the government).

¹¹¹ See generally Pamela Samuelson, Principles for Resolving Conflicts Between Trade Secrets and the First Amendment, 58 HASTINGS L.J. 777 (2007).

¹¹² See, e.g., Peter S. Menell, *The Defend Trade Secrets Act Whistleblower Immunity Provision: A Legislative History*, 1 BUS. ENTREPRENEURSHIP & TAX L. REV. 398, 407 (2017) (describing Professor Menell’s efforts in promoting a whistleblower provisions for the DTSA); Sharon K. Sandeen & Christopher B. Seaman, *Toward A Federal Jurisprudence of Trade Secret Law*, 32 BERKELEY TECH. L.J. 829, 858, n.170 (2017) (describing Professor Sandeen’s letter to Senator Dianne Feinstein regarding California’s abhorrence of restrictive covenants.)

¹¹³ 18 U.S.C. § 1833(b) (2012).

¹¹⁴ 18 U.S.C. § 1836(b)(3)(A)(i)(II) (2012).

¹¹⁵ See generally EU Trade Secret Directive, *supra* note 3.

4. A listing of types of behaviors that do not constitute misappropriation, including independent development, reverse engineering, and other “honest commercial practices;
5. A statement that the protection of trade secrets shall not extend to whistleblowing activity;
6. Recognition that trade secret law should not be used to restrict freedom of expression or the rights of the press to engage in investigative journalism and protect their journalistic sources; and
7. The need of EU-Member countries to consider the interrelationship of the Trade Secret Directive and other directives and regulations, including the GDPR.

Two of the issues listed in the first paragraph of this section that are not addressed in the Trade Secret Directive and that remain for the EU to determine concern the ownership of trade secrets and the interrelationship between trade secret, patent, and copyright laws; both are issues that can significantly impact the success of trade secret claims.

C. EXPANDED PROTECTIONS UNDER THE TRADE SECRET DIRECTIVE

While the Trade Secret Directive includes a long list of limitations, both in its recitals and in its text, it also appears to broaden trade secret protection in several ways beyond what is currently required in the U.S. For instance, as already mentioned, the Directive provides for monetary recovery measured by “moral prejudice” for the unlawful acquisition of trade secrets, apparently, even if the subject trade secrets were not subsequently disclosed or used.¹¹⁶ Relatedly, the Directive defines the unlawful acquisition of trade secrets to not only include conduct “contrary to honest commercial practices” (as in the U.S.), but also the “unauthorised access to, appropriation of, or copying of any documents . . . containing the trade secret or from which the trade secret can be deduced.”¹¹⁷ Similar proscriptions under U.S. law have raised a host of issues that will need to be resolved by the EU. For instance, some have raised concerns regarding the meaning and scope of “unauthorized access” under the U.S. Computer Fraud and Abuse Act (CFAA),¹¹⁸ specifically, as to whether online terms of use agreements or other terms that were not negotiated or read can define the parameters of “authorization.”¹¹⁹ Similarly, section 301 of the Copyright Act of 1976 raises the question of whether trade secret misappropriation claims involving acts of copying information are preempted by U.S. copyright law.¹²⁰ Without appropriate definitions and limits, the Directive may be used against

¹¹⁶ *Id.* at art. 14.2.

¹¹⁷ EU Trade Secret Directive, *supra* note 3, at art. 4.2.

¹¹⁸ 18 U.S.C. § 1030 (2012)

¹¹⁹ *See, e.g.,* United States v. Nosal, 676 F.3d 854 (9th Cir. 2012); Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372, 394-400 (2018).

¹²⁰ 17 U.S.C. § 301 (2012).

persons who either unwittingly or for beneficial purposes exceed authorized access to information or engage in “fair use” of copyrightable content.

An underlying principle of all information law, including copyright law and trade secret law, is that much of the information that businesses use and collect daily should be free for others to use, particularly with respect to information that is generally known and readily ascertainable.¹²¹ If the term “protected information” is defined too broadly, businesses may find themselves embroiled in disruptive and costly litigation concerning the alleged theft of information. From a societal point of view, information that does not meet the limited definition of a trade secret may serve to generate new ideas and inventions and to operate businesses effectively and efficiently. Thus, U.S. law has long recognized that it is not good public policy to tie-up information too much, particularly when there is a public interest in the information.¹²² This is one reason why trade secrets must have an independent legal existence and cannot be created by contract. Allowing companies to define what constitutes “authorized access” and then enabling a lawsuit for “unauthorized access” can conflict with these important principles, particularly if the requirement of a legitimate trade secret is ignored or minimized. Moreover, if the alleged wrongful acts involve the copying of information that is protected by copyright law, shouldn’t the defenses that are normally applied in copyright cases be available? Article 3.1(d) of the Trade Secret Directive may allow for such defenses as other “honest” means of acquiring trade secrets, but the parameters are not clear.¹²³ Undoubtedly, other EU law will be cited as defining what constitutes honest means of acquiring information.¹²⁴

Another way the Trade Secret Directive appears to have broadened trade secret law beyond what is recognized in the U.S. is by creating an entirely new wrong not specified in either the UTSA or DTSA.¹²⁵ Article 4.5 of the Directive makes the “production, offering or placing on the market of infringing goods, or the importation, export or storage of infringing goods” an unlawful use of the subject trade secrets provided the alleged infringer has the requisite knowledge or reason to know of an earlier infringement.¹²⁶ “Infringing goods” is defined to include “goods, the design, characteristics, functioning, production process or

¹²¹ RESTATEMENT (THIRD) OF UNFAIR COMPETITION, § 39 (AM. LAW INST. 2019) (“The subject matter and scope of trade secret protection is necessarily limited by the public and private interest in access to valuable information. The freedom to compete in the marketplace includes, in the absence of patent, copyright, or trademark protection (see §§ 16 and 17), the freedom to copy the goods, methods, processes, and ideas of others.”).

¹²² *Id.*

¹²³ EU Trade Secret Directive, *supra* note 3, art. 3.1(d).

¹²⁴ See Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs, art. 6, 2009 O.J. (L 111) 16 (allowing for the reproduction and translation of computer code for specified purposes).

¹²⁵ EU Trade Secret Directive, *supra* note 3, art. 4.5.

¹²⁶ *Id.*

marketing of which significantly benefits from trade secrets unlawfully acquired, used or disclosed.”¹²⁷ While an important aspect of U.S. trade secret law extends potential liability to third parties (particularly those not in privity of a contract), the circumstances under which such liability can be imposed is limited.¹²⁸ Typically, in the U.S., the third party, while not involved in the initial acts of misappropriation, is not too far removed from them.¹²⁹ This is because, to be held responsible for trade secret misappropriation, they must know or have reason to know of the existence of trade secrets and of the misappropriation.¹³⁰ The only exception concerns companies that import allegedly infringing goods into the U.S. and are made the subject of an action before the U.S. International Trade Commission (ITC).¹³¹

While Article 4.5 of the Trade Secret Directive is undoubtedly designed to create an ITC-like remedy to prevent the unfettered distribution of infringing goods throughout the EU, it could be interpreted to extend beyond mere importers to include retailers and consumers.¹³² Of course, the requisite knowledge requirement could limit the reach of third party claims, but it will depend upon how that requirement is interpreted and applied. Two critical questions are: (1) How and when must the requisite knowledge be acquired?; and (2) Did the alleged infringer detrimentally rely upon its acquisition of the alleged trade secrets before knowledge was acquired? Should, for instance, the delivery of a cease and desist order by the trade secret holder be enough to provide the requisite knowledge?

On its face, the Trade Secret Directive does not limit potential third party liability to people and companies that have not changed their position. Thus, it is possible for goods to be seized and services to be shut down once an otherwise innocent business is informed that the goods and services it is selling are tainted with the trade secrets of another. It is also not clear what is meant by the term “significantly benefits.”¹³³ This raises concerns that trade secret claims may be used to preclude the free movement of goods and services when the allegedly misappropriated trade secrets comprise only a portion of the goods and services.¹³⁴

Finally, the Trade Secret Directive may be broader than U.S. law as a result of its failure to specify a uniform statute of limitations, except to state that the applicable limitations period shall not exceed six years.¹³⁵ This contrasts with the majority rule in the U.S. that imposes a three-year statute of limitations as

¹²⁷ EU Trade Secret Directive, *supra* note 3, art. 2.4.

¹²⁸ See UTSA, *supra* note 44, at §1 (2), definition of misappropriation.

¹²⁹ *Id.*

¹³⁰ *Id.*

¹³¹ See *TianRui Grp. Co. v. Int’l Trade Comm’n*, 661 F.3d 1322, 1326 (Fed. Cir. 2011).

¹³² EU Trade Secret Directive, *supra* note 3, art. 4.5.

¹³³ *Id.* at art. 2.4.

¹³⁴ *Id.*

¹³⁵ *Id.* at art. 8.

measured from the time that the trade secret misappropriation was or could have been discovered.¹³⁶ The drafters of the UTSA saw this rule as an important limitation on the scope of trade secret protection that was consistent with the reasonable efforts requirement of trade secrecy — in theory, if efforts to protect trade secrets are reasonable, the misappropriation will be quickly discovered.¹³⁷ On the other-hand, the discovery rule provision of the UTSA's statute of limitations allows for some flexibility with respect to when the statute of limitations period begins to run. Without a more limited statute of limitations and application of the so-called discovery rule, it is possible that EU Member countries will adopt widely-different limitation periods. This may lead to forum shopping in cases where the subject goods and services are widely distributed throughout the EU.

CONCLUSION

As with any legislation, there are both pros and cons to the Trade Secret Directive. On balance, it is a positive development for the same reason that the 1979 adoption of the UTSA was an important development in the U.S. At a minimum, it should lead to greater understanding of both the meaning and limits of trade secret protection, including the definitions of a trade secret and the acts of misappropriation. It also broadens and clarifies the available remedies, allowing for greater and more timely enforcement of trade secret rights in the EU. Thus, trade secret owners can be relatively certain that information that meets the three requirements of trade secrecy (secrecy, commercial value, and reasonable steps to maintain secrecy) can be protected through resort to EU judicial authorities that have power to grant and enforce injunctive relief.

While some NGOs in the EU opposed the Trade Secret Directive, including those that expressed concern about how it might curtail whistleblowing activity and government transparency, as I have written elsewhere,¹³⁸ when properly applied, U.S. trade secret principles limit the scope and nature of trade secret rights. Thus, seeing and applying the Directive as a reflection of U.S. law should address many of the concerns that were raised. While both the direct and ancillary limits that are placed upon the scope of trade secret protection in the U.S. may be disliked by businesses that own trade secrets, they are welcomed by businesses that are accused of trade secret misappropriation. That is why balance in trade secret law and policy is needed. The Trade Secret Directive clearly evinces a desire for balance and is remarkable for the explicit limitations it places on the scope of trade secret rights. Because of these limitations, it is predicted that the EU Directive will cause everyone to look more closely at whether and how those same limitations are applied in the U.S., hopefully leading to better trade secret balance on both sides of the Atlantic.

¹³⁶ UTSA, *supra* note 44, at § 6.

¹³⁷ *Id.* at § 6, cmt.

¹³⁸ SANDEEN, *The Limits of Trade Secret Law*, *supra* note 6, at 537.