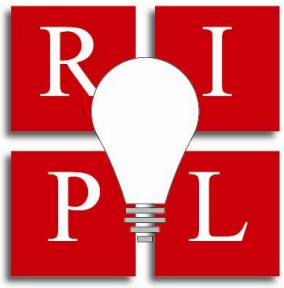
THE JOHN MARSHALL
REVIEW OF INTELLECTUAL PROPERTY LAW



TRADE SECRET LAW: THE ROLE OF INFORMATION GOVERNANCE PROFESSIONALS

WILLIAM LYNCH SCHALLER

ABSTRACT

Trade secrets are rapidly becoming the most important assets of many businesses. Information Governance (IG) professionals can and should play an integral part in managing company trade secrets, but not all companies have IG professionals and not all IG professionals understand the meaning of "trade secrets." This article maps the many facets of trade law and practice that are of potential interest to all IG professionals. It also highlights the different roles IG professionals can play with respect to trade secrets, from cataloging to monitoring to testifying.

Cite as William Lynch Schaller, *Trade Secret Law: The* Role of Information Governance Professionals, 18 J. MARSHALL REV. INTELL. PROP. L. 27 (2018).

TRADE SECRET LAW: THE ROLE OF INFORMATION GOVERNANCE PROFESSIONALS

WILLIAM LYNCH SCHALLER

TRADE SECRET LAW: THE ROLE OF INFORMATION GOVERNANCE PROFESSIONALS

WILLIAM LYNCH SCHALLER* † ©

I. INTRODUCTION

It's hardly an insight that companies today increasingly find their value in intangible assets.[1] Indeed, as attorney and trade secret authority Jim Pooley recently observed, according to a 2015 study by intellectual property merchant bank Ocean Tomo, intangible assets now make up about 84% of public company assets.[2] If you were to ask most people which intangible assets have the greatest value, you might hear patents or trademarks or copyrights. But surprisingly enough, trade secrets are actually the most valuable intellectual property for many firms, especially those engaged in research and development. In fact, Pooley noted, a 2012 study showed large R & D firms considered secrecy twice as important as patents.[3] More recent studies confirm the paramount importance of trade secrets.[4]

Unfortunately, as the importance of trade secrets has mounted, so has the ability to pirate them. Trade secrets, like virtually all other company data, are now digitized. This makes it far easier to store – and steal – vast amounts of such valuable data. Add to this our increasingly mobile workforce, epitomized by worker job-hopping in Silicon Valley, and you have a recipe for heightened trade secret

---

* Partner (Retired), Baker & McKenzie, LLP, Chicago, Illinois. All views herein are mine alone and do not necessarily reflect the views of Baker & McKenzie or its clients; in fact, I am no longer a partner, employee or agent of Baker & McKenzie in any way.

† This article is dedicated to my son, George J. Schaller, currently a Chicago law student. May the law be as good to him as it was to his grandfather and namesake, Judge George J. Schaller; as it has been to his sister, Alexandra J. Schaller of Winston & Strawn; and as it has been to me.

 An earlier version of this paper was delivered as part of Mr. Schaller's presentation at the National Conference on Managing Electronic Records in Chicago, Illinois on May 8, 2018.

[1] George Melloan, *When Assets Are Intangible*, WALL ST. J., Jan. 29, 2018, at A15 (reviewing book by JONATHAN HASKEL & STAIN WESTLAKE, CAPITALISM WITHOUT CAPITAL: THE RISE OF THE INTANGIBLE ECONOMY (Princeton 2017), and the reasons Haskel and Westlake believe intangible assets require us to change the way we think about business in postindustrial economies).

[2] *See* James Pooley, *The Myth of the Trade Secret Troll*, 23 GEO. MASON L. REV. 1045, 1067 (2016) ("As reported by Ocean Tomo, the share of public company value represented by intangible information leapt from 17 percent in 1975 to 68 percent in 1995 to 84 percent today. This means that industry in the span of a single generation has experienced a shift of historic proportions in the kind of property it uses to create value.").

[3] *Id*. "[A] 2012 report from the National Science Foundation and the Census Bureau . . . found that, among 'R&D-intensive' firms—who collectively account for two thirds of U.S. R&D investment—secrecy was deemed important at more than twice the level of patents."

[4] *See, e.g.*, *The Board Ultimatum: Protect and Preserve – The Rising Importance of Safeguarding Trade Secrets*, (June 2017) https://www.bakermckenzie.com/-/media/files/insight/publications/2017/trade-secrets (summarizing survey findings indicating 82% of executives thought their trade secrets were important if not essential to their business, with 60% saying they considered trade secret protection a board-level issue).

misappropriation.[5] And this does not even take into account recent cyberhacking that has resulted in digitized data theft on an epic scale,[6] some of which has included ransomware attacks freezing computers at government and famous firms.[7] Thus,

---

[5] *See* Sharon Weinbar, *The Power of a Fluid Market: Employee Mobility Makes Silicon Valley Flow*, (March 19, 2013) https://www.scalevp.com/blog/the-power-of-fluid-market-employee-mobility-makes-silicon-valley-flow (collecting data showing California leads the nation by a wide margin in venture capital investment, in part because of employee mobility fostered by California's statutory prohibition against employee noncompetition agreements).

[6] *See* Mike Murphy, *New Breach Might Have Exposed Data of Almost Every US Adult*, (June 28, 2018) https://www.msn.com/en-us/money/personalfinance/new-breach-might-have-exposed-data-of-almost-every-us-adult/ar-AAzgx4u ("If confirmed, the [Florida-based Exactis] data leak [containing nearly 340 million individual records] would be one of the largest in history, and far bigger than the Equifax data breach last year that exposed the personal information of about 148 million consumers."); Lily Hay Newman, *Equifax Officially Has No Excuse*, (Sept. 14, 2017) https://www.wired.com/story/equifax-breach-no-excuse (claiming Equifax had two months to fix the web-application vulnerability that resulted in loss of data for 143 million people); Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, (July 9, 2015) https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.e999e9197e6b (reporting on two Office of Personnel Management hacking episodes that compromised not only federal employees and contractors but their families and friends, "a very big deal from a national security perspective and a counterintelligence perspective," according to then-FBI Director James B. Comey); Michael Erman, Noor Zainab Hussain, & Suzanne Barlyn, *Merck Cyberattack May Cost Insurers $275 Million: Versick's PC*, (Oct. 19, 2017) https://www.reuters.com/article/us-merck-co-cyber-insurance/merck-cyber-attack-may-cost-insurers-275-million-verisks-pcs-idUSKBN1CO2NP ("Insurers could pay $275 million to cover the insured portion of drugmaker Merck & Co's loss from a cyber-attack in June, according to a forecast by Verisk Analytics Inc's Property Claim Services (PCS) unit."); Joseph Tanfani, *U.S. Accuses Iran of Hacking Into Universities, Companies*, CHI. TRIB., March 24, 2018, § 1, at 5 (reporting Department of Justice claim that Iran-based hackers used stolen credentials to hack into 320 universities around the world, including 144 in the United States, as well as the United Nations, the Department of Labor, the Federal Energy Regulatory Commission, and the states of Hawaii and Indiana); Kelso L. Anderson, *Data Breach Ruling Potentially Narrows Scope of Privilege and Work-Product Assertions*, A.B.A. LITIG. NEWS, Vol. 43, No.3, at 14 (Spring 2018) (discussing *In re Premera Blue Cross Customer Data Security Breach Litigation* arising out of Blue Cross's public disclosure in 2015 that its computer network was breached, resulting in disclosure of confidential information of 10 million members).

[7] *See* Rob Copeland & Melanie Evans, *LabCorp Works to Counter Cyberattack: Medical Testing Slows After "Ransomeware" Attack; Company Says No Data Was Stolen*, WALL ST. J., July 20, 2018, at B4 (reporting Laboratory Corp. of America is investigating suspicious activity concerning "ransomeware" aimed at one of the company's genetic testing units); Kimberly Hutcherson, *City of Atlanta Still Crippled Six Days After Ransomware Attack*, (March 27, 2018) https://www.msn.com/en-us/news/us/city-of-atlanta-still-crippled-six-days-after-ransomware-attack/ar-BBKMJPY?li=BBnbcA1&%3Bocid=hmlogout (reporting City of Atlanta employees have been authorized to turn their computers and printers back on, for the first time in six days, following a ransomware attack freezing government computers); Gerard Baker, *The Rising Risks of Hacks: With Cyberattacks Increasing in Number and Intensity, Companies Are Learning Just How Vulnerable Their Operations Really Are*, WALL ST. J., March 14, 2018, at R2 ("Even Merck was down for months," said panelist George Kurtz of cybersecurity firm CrowdStrike, referring to Not Petya ransomware freezing of Merck's email system); Keisha M. McClellan & H. Drew McClellan, *Held Hostage: Why Cyber Attacks Against Film and Media Industries Are on the Rise*, A.B.A. LANDSLIDE MAG., Vol. 10, No. 4, at 16, 17 (April 2018) (reporting ransomware attacks on media companies); Ellen Nakashima & Aaron Gregg, *Beware of Malware That Can Kill: Firm Tracks Code Beyond the Mere Malicious*, CHI. TRIB., May 1, 2018, § 2, at 3 (reporting discovery of software "designed to kill humans" by sabotaging a safety system at a petrochemical plant, along the lines of the Stuxnet

while the desire to steal intellectual property may be very old,[8] the means to do it on a national and even international scale are very new – and very dangerous.

Given the increasing importance of trade secrets and the rising risk of theft, Information Governance ("IG") professionals have a tough job. Companies need IG help but either do not know it or do not want to know it.[9] IG costs money and its company-wide benefits are not always apparent to units operating in silos, unaware of one another's policies and practices. Yet in focusing firms on data management, IG professionals can both reduce expenses by lowering data volume and increase revenues by bringing products more quickly to market through better data flow.[10] Within this mix lies the need to maximize and protect the firm's trade secrets – its crown jewels. Are IG leaders leaving them potentially underutilized and possibly unprotected? It seems an honest answer is, unfortunately, "yes."[11]

---

computer worm the U.S. and Israel used against Iran, and discussing industrial control systems protection being offered by firms like Dragos of Maryland and FireEye).

[8] *See* ADRIAN JOHNS, PIRACY: THE INTELLECTUAL PROPERTY WARS FROM GUTENBERG TO GATES (U. Chi. 2009) (book-length history of intellectual property theft across the ages); Lee T. Gesmer, *Protection of Trade Secrets in the Computer Industry*, (Jan. 1, 1990) https://www.gesmer.com/news/protection-of-trade-secrets-in-the-computer-industry ("Industrial espionage and theft of trade secrets go back far in the history of civilization. In ancient China, death by torture was the penalty for revealing the secret of silk making to outsiders.").

[9] *See* Ben DiPietro, *Survey Roundup: The Illusion of Information Governance Control*, WALL ST. J., (Sept. 25, 2015) https://blogs.wsj.com/riskandcompliance/2015/09/25/survey-roundup-the-illusion-of-information-governance-control/ ("Although 75% of business leaders think their organization has information governance under control, a look at global research data by PwC and data security firm Iron Mountain that measures how well businesses manage their information for competitive advantage found only 4% actually are set up for success. The report found 75% of organizations surveyed lacked the necessary skills, technology and corporate culture to exploit their information into a competitive advantage."); Paul P. Tallon, Ronald V. Ramirez & James E. Short, *The Information Artifact in IT Governance: Toward a Theory of Information Governance*, J. MGMT. INFO. SYS., Vol. 30, No. 3, at 141, 150 (2013) ("[T]he Economist Intelligence Unit (EIU) reports that a mere 38 percent of businesses have an information governance strategy in place; fewer than 25 percent consider their information governance strategy to be effective on a host of outcome measures.").

[10] Amanda Ciccatelli, *Why Information Governance Professionals Still Struggle to Secure Buy-In*, (July 11, 2017) https://www.law.com/insidecounsel/2017/07/11/why-information-governance-professionals-still-str/?slreturn=20180023131121 ("For instance, legal, information security, compliance and RIM develop policies and procedures, provide training and employee communication, and are likely investing in IG-related technology, all for slightly different reasons," [Laurie Fischer of HBR Consulting] explained. "Bringing these disciplines together and establishing a holistic framework can facilitate leveraging resources (time, people, money) for IG initiatives."); Paul P. Tallon, Ronald V. Ramirez & James E. Short, *The Information Artifact in IT Governance: Toward a Theory of Information Governance*, J. MGMT. INFO. SYS., Vol. 30, No. 3, at 141, 142 (2013) ("Once adopted, however, information governance can help to boost firm performance. By incorporating these results into an extended theory of IT governance, we note how information governance practices can unlock value from the ever-expanding mountains of data currently held within organizations.").

[11] *See, e.g.*, *The Second Annual Study on the Cybersecurity Risk to Knowledge Assets*, (April 2018) https://www.kilpatricktownsend.com/-/media/Feature/Insights/Gated-Content-PDFs/2018-KTS-Cybersecurity-Study.ashx (reporting Ponemon Institute survey of 634 IT security practitioners indicating that from 2016 to 2017, the likelihood that a company had failed to detect a data breach increased from 74% to 82% and the likelihood company knowledge assets ended up with a competitor increased from 60% to 65%).

Consider the Facebook scandal.[12] The details are still emerging, but it appears Facebook allowed data of 87 million users to fall into the hands of controversial Trump campaign adviser Cambridge Analytica with nothing more than a promise to purge data standing between Facebook and calamity.[13] Could Facebook have taken additional protective measures to prevent misuse of its user data? Some commentators certainly think so. In a recent Wall Street Journal piece,[14] Charles Duan and Shoshana Weissmann argued Facebook could have and should have done more, offering as an example randomizing or modifying data through "differential privacy" algorithms. Even notoriously low-tech attorneys know mere agreements do not suffice;[15] they routinely limit physical access to clients' most sensitive information or make it available only on internet disconnected computers, Duan and Weissmann noted. As a leading collector of data,[16] Facebook's failure to take such precautions has created a firestorm of bad publicity,[17] prompting always-unwanted

---

[12] Bryan Tau & Deepa Seetharaman, *Data Blowback Pummels Facebook*, WALL ST. J., March 20, 2018, at A1 (noting nearly 7% drop in Facebook stock in the aftermath of the Cambridge Analytica revelations, as well as mounting political pressure: "Republican and Democratic lawmakers called for tech-company leaders, including Facebook Chief Executive Mark Zuckerberg, to appear before Congress to explain how they protect user data from being exploited by third-party companies for advertising and other targeting purposes").

[13] *See* Cecilia Kang, *Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users*, (April 4, 2018) https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html (Facebook on Wednesday said the personal information of up to 87 million people, most of them Americans, may have been improperly shared during the 2016 election with Cambridge Analytica, a political consulting firm connected to President Trump.); Deepa Setharaman, *Facebook Struggles Over User Data: Internal Probe Finds Some Developers Are Now Out of Business or Won't Cooperate*, WALL ST. J., June 28, 2018, at B1 ("Facebook Inc.'s internal probe into misuse of user data is hitting fundamental roadblocks: The company can't track where much of the data went after it left the platform or figure out where it is now.").

[14] Charles Duan & Shoshana Weissmann, *How Could Facebook Have Been So Careless?*, WALL ST. J., March 26, 2018, at A21.

[15] *See, e.g.*, Jason Tashea, *Cloudy Ethics: Lawyers Have an Ethical Duty to Safeguard Clients' Confidential Information – a Task That's Become More Complicated as the Cloud Becomes More Ubiquitous*, A.B.A. J., Vol. 104, No. 4, at 30, 31 (April 2018) ("For cybersecurity ethicists, however, an ethical attorney is not just doing one thing; they are in a constant state of evolution and growth to keep pace with threats and best practices."); Timothy Peterson, *Cloudy with a Chance of Waiver: How Cloud Computing Complicates the Attorney-Client Privilege*, 46 J. MARSHALL L. REV. 383, 387-92 (2012) (discussing statutes that do not quite fit cloud computing and the resulting risks to attorney-client confidentiality).

[16] *See* Anick Jesdanun, *Facebook's Limits on Using Data Brokers Won't Stop Tracking: Move Might Earn It PR Points, But It Does Little to Protect Privacy*, CHI. SUN-TIMES, March 30, 2018, at 18 (noting Facebook still tracks browser and device ID visits to third-party sites and apps as well as usage of Facebook's own services through "likes"); Douglas MacMillan, Sarah Krouse & Keach Hagey, *Yahoo, Bucking Industry, Scans Emails for Data to Sell: Web Giant Pushes Harder to Analyze Inboxes for Advertisers*, WALL ST. J., Aug. 29, 2018, at A1 (reporting Yahoo's practice of scanning 200 million Yahoo Mail and AOL Mail inboxes – "the only major U.S. email provider that scans inboxes for marketing purposes" – bucking "a recent Silicon Valley trend toward more data privacy").

[17] *See* Kirsten Grind, *Facebook Suspends Another Data-Harvesting Firm*, WALL ST. J., July 21, 2018, at A1 (reporting suspension of Boston-based Crimson Hexagon, a firm that claims it only pulls publicly available data from Facebook); Mark Thompson, *Facebook's Data Scandal Could Get Even Worse*, (March 20, 2018) https://www.msn.com/en-us/money/technologyinvesting/facebooks-data-scandal-could-get-even-worse/ar-BBKsyFX ("Claims by the New York Times and UK media that Cambridge Analytica tried to influence how Americans voted using information improperly gleaned

regulatory and market scrutiny.[18] While not strictly speaking a trade secret case,[19] it plainly presents the same information-loss dynamics – and possibly the same evidence destruction problems.[20]

---

from 50 million Facebook users has already seriously hurt its brand. The London-based data analysis firm worked on President Donald Trump's campaign. It has denied the claims and says it did not use Facebook data in the 2016 campaign."); Rebecca Ballhaus, *Firm Pitches Entrapment Tactics on Video*, WALL ST. J., March 20, 2018, at A6 ("Executives at Cambridge Analytica, a data firm that worked for President Donald Trump's 2016 campaign, advertised campaign tactics – such as entrapping political opponents with bribes and sex – in a sales pitch captured by undercover journalists at British broadcaster Channel 4." *** [Cambridge chief executive Alexander Nix, caught on the tape, denied the claims, saying he] "was 'playing along' with the conversation and added that the company doesn't engage in 'entrapment, bribes or so-called 'honeytraps.'"); Mae Anderson, *Data Firm at Center of Facebook Privacy Scandal Goes Bankrupt*, CHI. SUN-TIMES, May 3, 2018, at 20 reporting bankruptcy filing of Cambridge Analytica: ("'The siege of media coverage has driven away virtually all of the company's customers and suppliers,' Cambridge Analytics said in a statement.").

[18] *See* John D. McKinnon & Marc Vartabedian, *Big Tech Wants to Shape Privacy Bill*, WALL ST. J., Aug. 7, 2018, at A4 (reporting likelihood of state-law preemption by any federal law that may emerge from the Facebook scandal); Fred Imbert, *Facebook's $120 Billion Stock Route Is Biggest in Market History*, (July 26, 2018) https://www.msn.com/en-us/money/companies/facebooks-dollar120-billion-stock-rout-is-biggest-in-market-history/ar-BBL6ypz (reporting Facebook stock dropped 20%); Georgia Wells, *Probe Into Facebook Adds FBI and SEC*, WALL ST. J., July 3, 2018, at B4 (reporting Facebook's receipt of questions from the FBI and SEC); Deepa Seetharaman & John D. McKinnon, *Zuckerberg and Senators Face Off: Facebook CEO Concedes Missteps as Lawmakers Weigh New Privacy Regulation*, WALL ST. J., April 11, 2018, at A1 ("Senators showed little consensus on what many in the technology industry fear the most – comprehensive legislation to force the protection of user data. But the legislators clearly opened the door to government action further than it had ever been opened before."); Georgia Wells & John D. McKinnon, *Facebook CEO: Lax Privacy a "Huge Mistake,"* WALL ST. J., April 5, 2018, at A1 (quoting Facebook CEO Mark Zuckerberg saying it was "huge mistake" for his company not to focus more on potential abuse of user data); Deepa Seetharaman & Kristen Grind, *Lax Data Policies Haunt Facebook*, WALL ST. J., March 21, 2018, at A1 ("The Federal Trade Commission is investigating whether Facebook violated terms of a 2011 settlement when data of up to 50 million users were transferred to an analytics firm tied to President Donald Trump's campaign, a person familiar with the matter said on Tuesday."); Georgia Wells & John D. McKinnon, *U.S., States Step Up Pressure on Facebook*, WALL ST. J., March 27, 2018, at A1 (reporting multiple Congressional calls for Facebook CEO Mark Zuckerberg to testify, the FTC's inquiries into Facebook's privacy practices, and "37 state attorneys general demanding explanations for its practices").

[19] *See* Hugh McLaughlin, *You're Fired: Pack Everything But Your Social Media Passwords*, 13 NW. J. TECH. & INTELL. PROP. 87, 105-06 (2015) (arguing that social media accounts are not trade secrets); Jasmine McNealy, *Who Owns Your Friends?: Phonedog v. Kravitz and Business Claims of Trade Secret in Social Media Information*, 39 RUTGERS COMPUTER & TECH. L.J. 30 (2013) (discussing Northern District of California *Phonedog* case holding Twitter passwords and follower lists were trade secrets); Barbara Ortutay, *Facebook: Most Users May Have Had Public Data "Scraped,"* (April 5, 2018) https://www.usnews.com/news/business/articles/2018-04-05/facebook-most-users-may-have-had-public-data-scraped ("Facebook's acknowledgement that most of its 2.2 billion members have probably had their personal data scraped by 'malicious actors' is the latest example of the social network's failure to protect its users' data.").

[20] *See* Tom Warren, *Facebook Secretly Deleted Messages Mark Zuckerberg Sent on Messenger: Messages Have Vanished from Recipient's Inboxes*, (April 6, 2018) https://www.theverge.com/2018/4/6/17203114/facebook-mark-zuckerberg-messages-deleted-messenger-inbox ("Facebook has admitted the company has been secretly deleting messages sent on Messenger by founder and CEO Mark Zuckerberg. 'After Sony Pictures' emails were hacked in 2014 we made a number of changes to protect our executives' communications,' says a Facebook spokesperson in a statement to TechCrunch. 'These included limiting the retention period for Mark's

A related problem is theft of someone else's secrets.[21] This most frequently happens through a new employee who imports an ex-employer's secrets into a new employer's database.[22] But it might occur through a firm's competitive intelligence program run amok.[23] Or it might result from a company's innocent acquisition of an infected firm.[24] Or it might arise simply because a firm did not return or did not destroy data after due diligence in a failed deal or at the end of some other business relationship.[25] Have the firm's IG professionals contemplated how they would disinfect their firm after such disasters? Is a "clean room" even possible at that point? Will their failure to act promptly and thoroughly be used later as evidence that they were actually enablers of such wrongdoing? Is ignorance really bliss?

A high-profile example is not hard to find – the recent trade secret theft battle between Google's self-driving car unit Waymo and Uber.[26] The dispute arose when engineer Anthony Levandowski jumped ship from Google/Waymo to start his own firm, Otto, and then shortly thereafter merged it with Uber, becoming in the process the new head of Uber's self-driving car effort.[27] Google/Waymo alleged that in 2015

---

messages in Messenger. We did so in full compliance with our legal obligations to preserve messages.'").

[21] *See* Eric J. Fues & Maximilienne Giannelli, *Title Source Inc. v. House Canary Inc*., (May 29, 2018) https://www.lexology.com/library/detail.aspx?g=838d5c2f-fe30-4469-a92b-235c4528531a (discussing Texas jury verdict of $706 million in favor of startup House Canary on its trade secret counterclaim against Title Source for misappropriating House Canary's appraisal software after their initial business collaboration collapsed).

[22] *See* William Lynch Schaller, *Jumping Ship: Legal Issues Relating to Employee Mobility in High Technology Industries*, 17 LAB. LAW. 25, 88 (2001) (discussing *PMC, Inc. v. Kadisha*, 93 Cal. Rptr.2d 663 (Cal. App. 2000), in which new employer and its officers, directors and principal shareholders faced potential liability as a result of new employee's alleged theft of secrets from his former employer).

[23] *See* Greg Bensinger, *Uber, Waymo Head to Trial*, WALL ST. J., Feb. 5, 2018, at B4 ("The case took an unexpected turn late last year when a 37-page letter from a former Uber security official emerged, alleging the company had formed a covert team dedicated to stealing trade secrets and helping employees dodge regulators' scrutiny. Uber said in court the letter was an extortionist move designed to extract millions of dollars from the company and that many of its allegations were false."); Chloe Cornish & Leslie Hook, *Uber Accused of Running Secret Competitive Intelligence Unit: Judge Says Ride-Hailing Group Withheld Evidence in Waymo Trial*, (Nov. 28, 2017) https://www.ft.com/content/386f07ee-d45e-11e7-a303-9060cb1e5f44 (reporting accusation that Uber was operating a competitive intelligence unit dedicated to stealing trade secrets).

[24] *See* Kel-Keef Enters., Inc. v. Quality Components Corp., 316 Ill. App. 3d 998, (1st Dist. 2000) (litigation arising out of acquisition of a firm tainted by trade secret theft, a theft discussed more fully in *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc*., 925 F.2d 174 (7th Cir. 1991)); Daniel Ilan, Emmanuel Ronco & Jane Rosen, *Data Privacy and Cybersecurity in M & A: A New Era*, A.B.A. LANDSLIDE MAG., Vol. 10, No. 6, at 49 (Aug. 2018) (discussing cybersecurity risks in acquisitions).

[25] *See* Deepa Seetharaman, *Facebook Provokes Storm Over User Data*, WALL ST. J., March 19, 2018, at R1 (reporting dispute between Facebook and outside data firm Cambridge Analytica over whether Cambridge "improperly kept data for years despite saying it had destroyed those records"); Barbara Ortutay, *Facebook Scandal Raises Questions About Privacy Audits*, CHI. TRIB., April 22, 2018, § 2, at 6 (Facebook agreed to outside audits every two years as part of an FTC settlement over its privacy practices; reporting it was unclear whether PriceWaterhouseCoopers caught the Cambridge Analytica matter as part of the FTC audits).

[26] *See* Lawrence D. Burns, *Late to the Driverless Revolution*, WALL ST. J., Aug. 18, 2018, at C1 (offering background story of how self-driving vehicle industry arose and how Google/Waymo and Uber came to compete in it, including Anthony Levandowki's role in their trade secret dispute).

[27] *See* Mike Isaac & Daisuke Wakabayahi, *Uber Fires Former Google Engineer at Heart of Self-Driving Dispute*, (May 30, 2017) https://www.nytimes.com/2017/05/30/technology/uber-anthony-

Levandowski downloaded more than 14,000 files, including files relating to its self-driving car work, and then joined Uber a few weeks later.[28] Uber said Levandowski took the documents as evidence of a $120 million bonus Google/Waymo owed him and claimed Levandowski was supposed to destroy the documents as part of Uber's acquisition of Levandowski's firm, Otto.[29] Uber denied using any such information but ultimately fired Levandowski for failing to cooperate in its internal investigation.[30] Uber nonetheless found itself under a preliminary injunction order barring it from using Google/Waymo's trade secrets, and then the case went to a jury trial on damages – a trial that abruptly ended when Uber agreed to pay Google/Waymo $245 million and further agreed not to use Google/Waymo's technology.[31] In hindsight, hiring Levandowski and then failing to verify and monitor his information sources turned out to be a costly mistake.

Obviously, crises like those confronting Facebook and Uber are well within the wheelhouse of IG professionals. They are tasked with guarding, tracking, storing, managing and destroying company information on a firm-wide basis;[32] they plainly can play a significant role in the protection – and theft – of trade secrets. It is far less evident that IG professionals actually understand the meaning of "trade secret" and their potential role in this field. A few basic points need to be understood.

---

levandowski.html ("Uber agreed to pay $680 million – mostly in company equity – in exchange for the [Levandowski] company's technology and a team of experienced self-driving technology engineers.").

[28] *See* Biz Carson, *The Real Fight Between Uber and Google Over What "May Be the Most Lucrative Business in History" Is Starting*, (May 2, 2017) https://www.businessinsider.com/google-waymo-v-uber-case-explained-2017-5.

[29] *See* Anita Balakrishnan, *Uber Says Its Fight with Waymo Comes Down to One Guy's $120 Million Bonus*, (July 7, 2017) https://www.cnbc.com/2017/07/07/uber-waymo-lawsuit-levandowski-stole-documents-to-secure-bonus-uber-says.html ("Levandowski was paid generously at Google, by a division that is now Alphabet's Waymo. He collected $120 million from Google, despite involvement with at least one start-up that would ultimately compete with his employer, Waymo said. But Uber said on Friday that Levandowski downloaded the documents to compile extensive evidence that he deserved a bonus, and just happened to hang on to them. Indeed, Uber said that Levandowski admitted as much to former Uber CEO Travis Kalanick and that the corresponding files were supposed to be destroyed during Uber's acquisition of Otto.").

[30] *See* Mike Isaac & Daisuke Wakabayahi, *Uber Fires Former Google Engineer at Heart of Self-Driving Dispute*, (May 30, 2017) https://www.nytimes.com/2017/05/30/technology/uber-anthony-levandowski.html ("Uber has pressured Mr. Levandowski to cooperate for months, but after he missed an internal deadline to hand over information, the company fired him.").

[31] Kif Leswing & Rob Price, *Uber and Waymo Have Reached a $245 Million Settlement in Their Massive Legal Fight Over Self-Driving-Car Technology*, (Feb. 9, 2018) https://www.businessinsider.my/uber-settles-with-waymo-in-self-driving-lawsuit-2018-2/ (reporting settlement, including non-use agreement).

[32] *See* Paul P. Tallon, Ronald V. Ramirez & James E. Short, *The Information Artifact in IT Governance: Toward a Theory of Information Governance*, J. MGMT. INFO. SYS., Vol. 30, No. 3, at 141, 142 (2013) ("[W]e define information governance as a collection of capabilities or practices for the creation, capture, valuation, storage, usage, control, access, archival, and deletion of information over its life cycle.").

II. WHAT IS TRADE SECRET LAW?

Trade secret law is part of the larger field called intellectual property ("IP"). Unlike the other major IP fields of patent, copyright and trademark law, trade secret law has no federal registration system. In addition, unlike these other IP fields, trade secret law requires secrecy. Moreover, unlike these other IP fields, trade secrets can lack exclusivity: more than one person or firm can legitimately own the same secret if they develop it through independent means or reverse engineering. Finally, unlike these other IP fields, trade secret law was and remains primarily based upon state law, although the 2016 enactment of the federal Defend Trade Secrets Act ("DTSA") will now move many – but not necessarily all – trade secret cases to federal court.

Each of these distinctions has important implications for IG practitioners. The absence of a government-sponsored repository for trade secrets means firms often do not formally identify their secrets for internal or external purposes until required to do so by a major event like a lawsuit or business sale – a backwards approach, to be sure. This lack of formal cataloging quickly leads to lack of secrecy; if employees do not know it is a trade secret, they will not think to keep it a secret and will not hesitate to steal it. As if this were not complicated enough, 50 states now have 50 distinct legal regimes governing trade secrets, topped off by the independent DTSA – a federal law that explicitly does not overrule or preempt these state laws.[33] The DTSA and most state laws are modelled on the Uniform Trade Secrets Act, as for that matter is the World Trade Organization's TRIPS (Agreement on Trade-Related Aspects of Intellectual Property Rights) trade secret mandate.[34] Not all jurisdictions follow the Uniform Act, however, and some that follow it do so with substantial modifications.[35] Others, like the International Trade Commission and New York, follow separate but similar rules.[36] Thus, what's legal or required in one jurisdiction

---

[33] *See* 18 U.S.C. § 1838 (1996) ("Except as provided in section 1833(b), this chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act)").

[34] *See* Charles H. Camp, Anna R. Margolis & Camellia H. Mokri, *No Way Out: Mandatory Trade Secret Protection Laws in International Arbitration*, (Dec. 2, 2016) http://www.worldfinancialreview.com/?p=12119 ("The language of the Uniform Trade Secrets Act is very similar to the language in TRIPS."); Virtuoso Legal, *What You Need to Know About: Trade Secrets and the EU Trade Secrets Directive*, (June 5, 2018) https://www.lexology.com/library/detail.aspx?g=bd9e35f3-c9ee-4b9f-ae83-3154b0b35cc0 (discussing the 2016 European Union directive to bring European law in line with the Defend Trade Secrets Act in the United States and the Anti-Unfair Competition Law in China).

[35] *See* Sid Leach, *Anything But Uniform: A State-By-State Comparison of the Key Differences in the Uniform Trade Secrets Act*, SNELL & WILMER (Oct. 23, 2015), http://www.swlaw.com/assets/pdf/news/2015/10/23/How%20Uniform%20Is%20the%20Uniform%20Trade%20Secrets%20Act%20-%20by%20Sid%20Leach%20-%20AIPLA%20paper.pdf.

[36] *See* TianRui Grp. Co., Ltd. v. Int'l Trade Comm'n, 661 F.3d 1322, 1327 (Fed. Cir. 2011) ("We hold that a single federal standard, rather than the law of a particular state, should determine what constitutes a misappropriation of trade secrets sufficient to establish an 'unfair method of competition' under section 337."); E.J. Brooks Co. v. Cambridge Sec. Seals, 31 N.Y.3d 441 ("A trade secret is 'any formula, pattern, device or compilation of information which is used in one's business,

may not be in another – a patchwork pattern all too familiar to IG professionals who have wrestled with disparate domestic and foreign data privacy rules.[37] The "biometrics" battles under Illinois law make the point all too clearly.[38]

---

and which gives [one] an opportunity to obtain an advantage over competitors who do not know or use it.'"); Ashland Mgmt. Inc. v. Janien, 82 N.Y.2d 395 (1993) (following Restatement of Torts §757).

[37] *See, e.g.*, Zachary S. Heck, *A Litigator's Primer on European Union and American Privacy Laws and Regulations*, A.B.A. LITIG. MAG., Vol. 44, No. 2, at 59 (2018) (comparing the fundamental human right to privacy in the EU, captured in its General Data Protection Regulation of 2016, with the scattered statutes addressing privacy in America, including HIPAA, the Fair Credit Reporting Act, and the Fair and Accurate Credit Transactions Act); Sam Schechner & Natalia Drozdiak, *U.S. Tech Giants Meet Their Nemesis: EU Antitrust Chief Is De Facto Global Enforcer*, WALL ST. J., April 5, 2018, at A1 (describing Margrethe Vestager's efforts as European Union competition commissioner and European nations' preparation to enforce the EU's "strict new data-protection law" and their increasing interest "in the potential abuse of data and algorithms"); Drew FitzGerald, *Third Parties Know Exactly Where You Are*, WALL ST. J., July 16, 2018, at B4 (discussing controversies over whether cell-phone location tracking violates Section 222 of the Telecommunications Act of 1996); Daniela Hernandez, Zolan Kanno-Youngs & Zusha Elinson, *Use of Database Raises Questions*, WALL ST. J., April 30, 2018, at A6 (reporting use of non-state owned DNA – here familial DNA searching on private company GEDmatch – to catch the alleged Golden State Killer, 72-year-old former police officer Joseph James DeAngelo); Kyle Swenson, *Undercover Cops Grabbed a DJ's Chewing Gum. It Helped Crack a Teacher's 1992 Murder, Police Say*, (June 26, 2018) https://www.washingtonpost.com/news/morning-mix/wp/2018/06/26/undercover-cops-grabbed-a-djs-chewing-gum-it-helped-crack-a-teachers-1992-murder-police-say/?noredirect=on&utm_term=.7c4d33f5c99d (reporting police use of GEDmatch open source database to match DNA profile with 1992 rape and murder victim DNA evidence); Zusha Elinson, *Police Use of Driver Photos Stirs Debate*, WALL ST. J., June 18, 2018, at A2 (reporting Maryland police use of facial recognition software to scan driver license photo database to identify suspect); Colin Lecher, *California Just Passed One of the Toughest Data Privacy Laws in the Country*, (June 28, 2018) https://www.theverge.com/2018/6/28/17509720/california-consumer-privacy-act-legislation-law-vote (discussing new California Consumer Privacy Act of 2018); Devin Coldewey, *Vermont Passes First Law to Crack Down on Data Brokers*, (May 2018) https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers/ ("Data brokers in Vermont will now have to register as such with the state; they must take standard security measures and notify authorities of security breaches (no, they weren't before); and using their data for criminal purposes like fraud is now its own actionable offense.").

[38] Michael G. Morgan, Kristen E. Michaels, Christopher M. Murphy, Mark E. Schreiber & Lynette Ryan Acre, *To Scan or Not to Scan: Surge in Lawsuits Under Illinois Biometrics Law*, (Nov. 8, 2017) https://www.natlawreview.com/article/to-scan-or-not-to-scan-surge-lawsuits-under-illinois-biometrics-law ("The Illinois Biometric Information Privacy Act (BIPA) is having its moment. At least 32 class action lawsuits have been filed by Illinois residents in state court in the past two months challenging the collection, use and storage of biometric data by companies in the state."); Ally Mariotti, *Illinois May Change Law Protecting Biometric Data*, CHI. TRIB., April 11, 2018, § 2, at 1 (reporting Illinois bill that would allow employers "to collect biometric information on their employees if it is used exclusively for employment, human resources or identification, as well as safety, security or fraud prevention"); Matthew Hector, *Amendments to Weaken BIPA Effectively Dead: Amendments Adding Exemptions to the Incidental Collection of Biometric Data Stall in State Senate*, 106 ILL. B. J. 21 (2018) (according to the Illinois Chamber of Commerce, "roughly 90 percent of the cases for alleged violations of the [Illinois] biometric law are for employment purposes"); Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317 *leave to appeal granted*, No. 123186 (Ill. Sup. Ct. May 30, 2018) (plaintiff, who sued Six Flags under the Illinois Biometric Information Privacy Act for fingerprinting plaintiff without first obtaining written consent, suffered no injury and therefore lacked standing to be an "aggrieved" person under the BIPA).

III. WHAT CONSTITUTES A TRADE SECRET?

The federal DTSA, like its state law counterparts, defines "trade secret" as information (1) that derives its economic value from its relative secrecy and (2) that is subject to reasonable secrecy measures.[39] If this definition seems broad, that's because it is. Indeed, trade secrets have been called "one of the most elusive and difficult concepts in the law to define."[40]

In part, this elusiveness stems from the sheer breadth of trade secret law. It protects both technical and non-technical data, meaning chemical processes and customer lists can both be trade secrets, as can machines and plans. Neither novelty in the patent sense nor originality in the copyright sense is necessary for trade secret status. In fact, combinations of well-known information can rise to the level of trade secrets if the combinations themselves are not generally known in the industry or profession. Economic value can mean anything from cost savings, to pricing prowess, to process improvements; requiring economic value precludes protection for information not generally known to the public but clearly understood in a particular industry.[41] Even information about what *doesn't* work can constitute a trade secret.[42]

From the IG professional's standpoint, the secrecy requirement is far more likely to be of concern than the specific subject matter being protected. Who should have access, when and for what purpose are key questions with varying answers across an organization.[43] Scientists, for example, might want group-wide access to foster research and development in their department, yet the law department might want access restricted on a "need to know" basis so "secrecy" can be easily shown in the event of a dispute. The IT department, in turn, might roll out solutions that allow tracking of all data but ready use of none. Outsiders – such as customers, vendors and suppliers – may have altogether different needs and secrecy practices.[44]

---

[39] *See* 18 U.S.C. § 1839(3) (2016); 14 U.L.A. § 1(4) (1985).

[40] Learning Curve Toys, Inc. v. PlayWood Toys, Inc., 342 F.3d 714, 723 (7th Cir. 2003).

[41] *See* George S. May Int'l v. Int'l Profit Assoc., 256 Ill. App. 3d 779, (1st Dist. 1993) (discussing "economic value" requirement under the Illinois Trade Secrets Act); Sharon 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, 524-26 (2010) (examining the history of the "economic value" requirement).

[42] *See* Michael Rosen, *The Role of "Negative Trade Secrets" in the Uber-Waymo Litigation*, (Feb. 21, 2018) http://www.aei.org/publication/the-role-of-negative-trade-secrets-in-the-uber-waymo-settlement/ ("According to Waymo, Levandowski's disclosure to Uber of self-driving approaches that proved *un*successful was every bit as damaging to Waymo as his alleged revelation of helpful tips.").

[43] *See* Brian E. Finch, *Safety From Hackers – and Trial Lawyers*, WALL ST. J., Feb. 26, 2018, at A17 (discussing need to amend the Safety Act – formally known as the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002 – to have Department of Homeland Security "safe/well-constructed/regularly updated/effective" certification for security products or services, thereby triggering limited liability protection, to broadly cover "cyber incidents," as opposed to just "terrorism"); Jason Tashea, *MGM Resorts Uses an Obscure Law to Sue Las Vegas Mass Shooting Victims*, (July 17, 2018) http://www.abajournal.com/news/article/mgm_resorts_uses_an_obscure_law_to_sue_las_vegas_mass_shooting_victims/ (reporting MGM's invocation of Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 to shield it from liability arising out of the Las Vegas mass shootings – the first such case in the 15 years since the SAFETY ACT was passed – on the theory that MGM hired Contemporary Services Corporation, a third-party security vendor with SAFETY Act certification).

[44] *See* Keisha M. McClellan & H. Drew McClellan, *Held Hostage: Why Cyber Attacks Against Film and Media Industries Are on the Rise*, A.B.A. LANDSLIDE MAG., Vol. 10, No. 4, at 16, 17 (April

Centralized governance may be the goal, but a standard one-size-fits-all policy may not make sense for many firms. After all, "[o]ver-governance could limit information-led innovation, motivating users to work around policies and to take unnecessary risks with their information."[45]

The critical consideration to remember is that trade secret law requires relative secrecy, not absolute secrecy.[46] If *total* secrecy were demanded, no one could see or use the secrets and then the secrets would have no economic value to the firm. On the other hand, failure to take *any* secrecy measures will usually prove fatal,[47] at least absent proof that the law or industry custom and practice required recipients to maintain secrecy.[48] The moral of the story is clear: "one who claims a trade secret must exercise eternal vigilance in protecting its confidentiality."[49]

IV. WHAT ARE REASONABLE SECRECY MEASURES?

Someday companies and courts may no longer care about secrecy measures. Everything will be ultra-encrypted via blockchain or some comparable technology.[50] Until then, there is plenty to worry about.[51]

2018) ("Technological advances enable media companies to achieve more output with less production expense, but such efficiencies create new access points for would-be hackers" – especially digitized products subject to lax security measures at vendors serving the media companies); Ellen Nakashima & Paul Sonne, *Chinese Swipe Data from Navy Contractor: Sub Warfare Plans Part of Breaches, U.S. Officials Say*, CHI. TRIB., June 9, 2010, § 1, at 5 ("The data stolen was of a highly sensitive nature despite being housed on the contractor's unclassified network. The officials said the [stolen] material, when aggregated, would be considered classified, a fact that raises concerns about the Navy's ability to oversee contractors tasked with developing cutting-edge weapons.").

[45] *See* Paul P. Tallon, Ronald V. Ramirez & James E. Short, *The Information Artifact in IT Governance: Toward a Theory of Information Governance*, J. MGMT. INFO. SYS., Vol. 30, No. 3, at 141, 167, 168 (2013) ("The inflection point at which the effects of information governance start to decline and potentially become negative is an open question, but one that may become increasingly important as the strategic importance of information becomes more widely accepted.").

[46] *See* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 177 (7th Cir. 1991).

[47] *See* Fail-Safe, LLC. V. A.O. Smith, Corp., 674 F.3d 889, 893 (7th Cir. 2012) (party seeking to develop a pump motor for pool suction entrapment prevention technology failed to secure confidentiality agreement from counterparty).

[48] *See* Hicklin Eng'g, LC v. Bartell, 439 F.3d 346, 350 (7th Cir. 2006) (an implied understanding to abide by trade norms of secrecy can suffice for trade secret purposes).

[49] RTE Corp. v. Coatings, Inc., 84 Wis. 2d 105 (1978).

[50] *See, e.g.*, Reade Ryan & Mayme Donohue, *Securities on Blockchain*, 73 BUS. LAW. 85, 87 (2018) ("Blockchain is a type of distributed ledger, comprised of digital records of transactions or assets, accessible to and trusted by all participants running the same protocol. A protocol for this purpose is a set of rules governing the format of messages that are exchanged between the participants. The fundamental innovation of blockchain is that it creates a means of establishing and maintaining consensus among the participants in a transaction without the need for either an established trust relationship or a central intermediary."); Inayat Chaudhry, *The Patentabilty of Blockchain Technology and the Future of Innovation*, A.B.A. LANDSLIDE MAG., Vol. 10, No. 4, at 21, 22 (April 2018) ("When someone requests a transaction using blockchain technology, it is broadcast to a peer-to-peer network consisting of computers, known as nodes, which employs algorithms to validate the transaction and the user's status. Once the transaction has been verified, it is combined with other transactions to create a new block of data for the ledger that is then added to the existing blockchain, and the transaction is considered complete."); SEC v. Recoin Group Found., LLC, No. 17 Civ. 05725 (E.D.N.Y. Sept. 29, 2017) (Cmplt., p. 7, n.2) ("A blockchain is a type of

When it comes to secrecy measures, size matters. For large companies, courts often demand extensive secrecy measures; smaller companies sometimes are held to a lower standard.[52] Most companies end up in between: confidentiality agreements, computer passwords, secrecy legends on screens and documents, and "need to know" access. Some go further, deploying encryption, network monitoring, antivirus programs and "whitelisting" applications blocking unauthorized programs.[53] Many of these measures are straightforward and uncontroversial in principle, as Vicki Cundiff explained at length in a thoughtful article,[54] but they can become complex and contested in practice.[55]

The practical difficulties of this issue were examined at length by recently-retired Judge Richard Posner in a well-known 1991 opinion for the Seventh Circuit

---

distributed ledger, or peer-to-peer database spread across a network, that records all transactions in the network in theoretically unchangeable, digitally recorded data packages called blocks. Each block contains a batch of records of transactions, including a timestamp and a reference to the previous block, linking the blocks together in a chain. The system relies on cryptographic techniques for secure recording of transactions. A blockchain can be shared and accessed by anyone with appropriate permissions.") available at https://www.sec.gov/litigation/complaints/2017/comp-pr2017-185.pdf.

[51] *See, e.g.*, Robert McMillan, *Cracking the iPhone's Passcode: An Atlanta Startup's $15,000 Device Helps Police Unlock Apple's Privacy Safeguards*, WALL ST. J., June 15, 2015, at B4 (reporting Grayshift LLC's new device, called a "Graykey," could "break into an iPhone and download nearly all of the data available on the device").

[52] *See* William Lynch Schaller, *Growing Pains: Intellectual Property Considerations for Illinois Small Businesses Seeking to Expand*, 35 LOY. U. CHI. L.J. 845, 858 (2004) (citing cases showing "courts frequently excuse small businesses from [secrecy] measures they might require of larger companies").

[53] *See* Hanley Chew, Tyler Newby & Sarah Lightstone, *Takeaways from the 11th Circuit's Reversal of the FTC's Data Security Order Against LabMD*, (July 3, 2018) https://www.fenwick.com/publications/Pages/Takeaways-From-the-11th-Circuits-Reversal-of-the-FTCs-Data-Security-Order-Against-LabMD.aspx (listing these steps as part of authors' discussion of the Eleventh Circuit's opinion reversing the FTC's vague cease and desist order in *LabMd, Inc. v. FTC*, 891 F.3d 1286 (11th Cir. 2018)); Paige M. Boshell, *The LabMD Case and the Evolving Concept of "Reasonable Security,"* (July 16, 2018) https://businesslawtoday.org/2018/07/labmd-case-evolving-concept-reasonable-security/ (reviewing *LabMd, Inc. v. FTC*, the FTC's 2015 *Start with Security* guide, the FTC's 2017 *Stick with Security* blogs, and other regulatory approaches to cybersecurity published by the National Institute of Standards and Technology, the Federal Financial Institutions Examination Council, and the states of New York, Massachusetts and Alabama); Craig A. Newman, *The FTC's Abusive Cyber Enforcement*, WALL ST. J., July 25, 2018, at A19 (detailing cybersecurity firm Tiversa's questionable trolling activities – including its offer of remediation services to fix LabMD's cybersecurity for payment and its threat to turn over LabMD's file to the FTC – that led to FTC's prosecution of LabMD, and discussing Eleventh Circuit's rejection of the FTC's "indeterminable standard of reasonableness" for data-security programs).

[54] *See* Victoria Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, 49 IDEA: INTELL. PROP. L. REV. 359, 364-65 (2008) (offering comprehensive discussion of digital information protection, including "programmable access cards, computer firewalls, password protections [such as frequent changes and multiple levels], digital watermarks, and secure intranets").

[55] *See, e.g.*, Matthew Steinberg, *Can We Talk NDAs?: Provisions Can Raise Concerns, Legal Problems*, CHI. TRIB., Feb. 5, 2018, § 2, at 1 (discussing questions surrounding nondisclosure agreements outside the context of trade secrets or other proprietary information, including covering up workplace problems); Brian D. Hall, *The Impact of Wearable Technology on Trade Secret Protection and E-Discovery*, 33 A.B.A. J. LAB. & EMP. L. 79 (2018) (discussing security measures applicable to new devices like live video broadcasting, smart glasses and concealed recording devices).

Court of Appeals, *Rockwell Graphic Systems, Inc. v. DEV Industries, Inc*.[56] Plaintiff Rockwell manufactured printing presses and replacement parts and in some instances subcontracted out parts manufacturing to independent machine shops that the parties called "vendors." To do their job, vendors needed Rockwell's "piece part drawings" showing materials, dimensions, tolerances and manufacturing methods; otherwise vendors could not make the parts. Rival press manufacturer DEV, headed by a former Rockwell employee named Fleck, recruited another Rockwell employee named Peloso. Trade secret theft allegations followed, and DEV defended in part on the ground that Rockwell had failed to take adequate secrecy measures. The district court accepted DEV's "inadequate secrecy measures" argument and granted summary judgment in favor of DEV.

The Court of Appeals reversed, holding that a trial was needed to determine whether Rockwell's secrecy efforts were reasonable. Speaking through Judge Posner, the Seventh Circuit described Rockwell's secrecy measures in some detail:

> Rockwell keeps all its engineering drawings, including both piece part and assembly drawings, in a vault. Access not only to the vault, but also to the building in which it is located, is limited to authorized employees who display identification. These are mainly engineers, of whom Rockwell employs 200. They are required to sign agreements not to disseminate the drawings, or disclose their contents, other than as authorized by the company. An authorized employee who needs a drawing must sign it out from the vault and return it when he has finished with it. But he is permitted to make copies, which he is to destroy when he no longer needs them in his work. The only outsiders allowed to see piece part drawings are the vendors (who are given copies, not originals). They too are required to sign confidentiality agreements, and in addition each drawing is stamped with a legend stating that it contains proprietary material. Vendors, like Rockwell's own engineers, are allowed to make copies for internal working purposes, and although the confidentiality agreement that they sign requires the vendor to return the drawing when the order has been filled, Rockwell does not enforce this requirement. The rationale for not enforcing it is that the vendor will need the drawing if Rockwell reorders the part. Rockwell even permits unsuccessful bidders for a piece part contract to keep the drawings, on the theory that the high bidder this round may be the low bidder the next. But it does consider the ethical standards of a machine shop before making it a vendor, and so far as appears no shop has ever abused the confidence reposed in it.
>
> The mere fact that Rockwell gave piece part drawings to vendors — that is, disclosed its trade secrets to "a limited number of outsiders for a particular purpose" — did not forfeit trade secret protection. *A.H. Emery Co. v. Marcan Products Corp*., 389 F.2d 11, 16 (2d Cir.1968). On the contrary, such disclosure, which is often necessary to the efficient exploitation of a trade secret, imposes a duty of confidentiality on the part of the person to whom the disclosure is made. *Jones v. Ulrich*, 342 Ill.App. 16, 25-26, 95

[56] 925 F.2d 174 (7th Cir. 1991).

> N.E.2d 113, 117 (1950); *Crocan Corp. v. Sheller-Globe Corp.*, 385 F.Supp. 251, 253 (N.D. Ill. 1974). But with 200 engineers checking out piece part drawings and making copies of them to work from, and numerous vendors receiving copies of piece part drawings and copying them, tens of thousands of copies of these drawings are floating around outside Rockwell's vault, and many of these outside the company altogether. Although the magistrate and the district judge based their conclusion that Rockwell had not made adequate efforts to maintain secrecy in part at least on the irrelevant fact that it took no measures at all to keep its assembly drawings secret, DEV in defending the judgment that it obtained in the district court argues that Rockwell failed to take adequate measures to keep even the piece part drawings secret. Not only did Rockwell not limit copying of those drawings or insist that copies be returned; it did not segregate the piece part drawings from the assembly drawings and institute more secure procedures for the former. So Rockwell could have done more to maintain the confidentiality of its piece part drawings than it did, and we must decide whether its failure to do more was so plain a breach of the obligation of a trade secret owner to make reasonable efforts to maintain secrecy as to justify the entry of summary judgment for the defendants.[57]

The Court of Appeals also tied Rockwell's secrecy efforts to the economic value of the secrets themselves. After sketching what can loosely be called the "tort" and "property" approaches to trade secrets,[58] Judge Posner observed:

> Under the first approach, at least if narrowly interpreted so that it does not merge with the second, the plaintiff must prove that the defendant obtained the plaintiff's trade secret by a wrongful act, illustrated here by the alleged acts of Fleck and Peloso in removing piece part drawings from Rockwell's premises without authorization, in violation of their employment contracts and confidentiality agreements, and using them in competition with Rockwell. Rockwell is unable to prove directly that the 100 piece part drawings it got from DEV in discovery were stolen by Fleck and Peloso or obtained by other improper means. But if it can show that the probability that DEV could have obtained them otherwise — that is, without engaging in wrongdoing — is slight, then it will have taken a giant step toward proving what it must prove in order to recover under the first theory of trade secret protection. The greater the precautions that Rockwell took to maintain the secrecy of the piece part drawings, the lower the probability that DEV obtained them properly and the higher the probability that it obtained them through a wrongful act; the owner had taken pains to prevent them from being obtained otherwise.

---

[57] *Id.* at 177-78.

[58] *See* Charles T. Graves, *Trade Secrets as Property: Theory and Consequences*, 15 J. INTELL. PROP. L. 39, 45-57 (2007) (a property conception of trade secrets forces courts to define claim limits and avoid over-inclusive claims, thereby promoting employee mobility and startups).

> Under the second theory of trade secret protection, the owner's precautions still have evidentiary significance, but now primarily as evidence that the secret has real value. For the precise means by which the defendant acquired it is less important under the second theory, though not completely unimportant; remember that even the second theory allows the unmasking of a trade secret by some means, such as reverse engineering. If Rockwell expended only paltry resources on preventing its piece part drawings from falling into the hands of competitors such as DEV, why should the law, whose machinery is far from costless, bother to provide Rockwell with a remedy? The information contained in the drawings cannot have been worth much if Rockwell did not think it worthwhile to make serious efforts to keep the information secret.[59]

As a 1991 case, *Rockwell* was decided before the widespread use of computers and digital data. Even so, the secrecy measures it described – primarily confidentiality agreements, confidentiality legends and "need to know" access – remain standard strategies for most firms over 25 years later. If hundreds or even thousands of people need to see secrets to do their jobs, sharing such information with an understanding of confidentiality does not automatically destroy trade secret status, as *Rockwell* and many other cases hold.[60]

The problem in *Rockwell* was not too much access; it was too little retrieval. As in the Facebook scandal, the plaintiff in *Rockwell* failed to make affirmative efforts to secure return of its information once authorized users no longer needed it.[61] Such failure raises the likelihood that trade secret protection will be lost in later litigation. On this point consider the Illinois Appellate Court's illustrative 1993 holding in *George S. May International v. International Profit Associates*:

> It is undisputed that the field and survey service manuals, which contained the bulk of May's system and formulas, were routinely disseminated to thousands of incoming trainees before any confidentiality agreements were executed by May, and without regard to the extent of these individuals' commitment to May. Certain of May's allegedly confidential forms were apparently also given to or discussed with prospective clients. Although May purported to have sign-out policies and penalties for unreturned manuals, it is unclear how or whether these policies were enforced, given the vast number of people with daily access to the material. Finally and more importantly, although May marked its manuals with broad admonitions regarding trade secrets, it never identified

---

[59] *Id.* at 178-79.

[60] *See, e.g.*, ISC-Bunker Ramo Corp. v. Altech, Inc., 765 F. Supp. 1310 (N.D. Ill. 1990) (access by hundreds of employees to plaintiff's computer service manuals did not necessarily destroy secrecy of those manuals).

[61] *See also* Douglas MacMillan, *App Developers Gain Access to Millions of Gmail Inboxes*, WALL ST. J., July 3, 2018, at A1, A6 ("The latitude outside developers have in handling user data shows how even as Google and other tech giants have touted efforts to tighten privacy, they have left the door open to others with different oversight practices.").

> these secrets for its personnel despite the fact that the manuals also contained much material that May believed to be commonly-known.[62]

Rockwell and *George S. May International* highlight the problems IG practitioners face when designing systems dealing with mass circulation of confidential data. It's not that it can't be done; it just has to be done carefully. The discussions in these cases dovetail with secrecy recommendations former Microsoft executive and lawyer Pamela Passman recently published in the World Intellectual Property Organization's magazine.[63] One of her most important suggestions is establishing an information protection team.

The Wall Street Journal, in its May 30, 2018 edition, recently offered an entire section of interest to those following this field. The most significant, for present purposes, were the lead article, *What Keeps CIOs Up at Night?*,[64] and the one immediately following it, *How Firms Can Create a Cybersafe Culture*.[65] In the first the authors interviewed multiple CIOs who expressed their concerns on such diverse subjects as employees logging into corporate systems remotely, limiting access to networks on a need-to-know basis called "zero trust," multifactor identification (biometrics like fingerprint and facial recognition tools),[66] evaluating and monitoring

---

[62] George S. May Int'l v. Int'l Profit Assocs.', 256 Ill. App. 3d 779, (1st Dist. 1993).

[63] *See* Pamela Passman, *Eight Steps to Secure Trade Secrets*, (February 2016) http://www.wipo.int/wipo_magazine/en/2016/01/article_0006.html (outlining multiple measures, including document protection policies, electronic security controls, and employee training). There are, of course, many refinements to these as well as additional security measures. *See, e.g.*, Joel D. Bush II & John M. Moye, *Protecting Your Trade Secrets: Best Practices for Securing Information with New and Departing Employees*, (Aug. 11, 2015) https://www.acc.com/legalresources/quickcounsel/protecting-your-trade-secrets.cfm (recommending "copy protection and embedded code to trace copies," a "global tip line," restrictions on "bring your own device" technology, and exit interviews); Adam K. Levin, *Somebody's Watching You: Predictive Behavior Profiling Helps Companies Determine Which Employees May Be Security Threats*, CHI. TRIB., April 23, 2018, § 2, at 3 ("Similar online employee surveillance [predictive behavior profiling/data mining] is creeping into other industries as companies seek to strengthen overall network security, with an eye in particular on avoiding unauthorized access to systems, protecting proprietary information and trade secrets as well as creating better overall cyber hygiene."); Mark Epstein, *How to Keep Online Speech Free*, WALL ST. J., April 30, 2018, at A15 (noting Mark Zuckerberg's recent Congressional testimony in which he said "Facebook will soon employ artificial intelligence to identify and delete 'hate speech.' Yet he struggled to define the term.").

[64] Jeff Stone, Kim S. Nash & Adam Janofsky, *What Keeps CIOs Up at Night?*, WALL ST. J., May 30, 2018, at R1.

[65] Stuart Madnick, *How Firms Can Create a Cybersafe Culture*, WALL ST. J., May 30, 2018, at R4.

[66] *See, e.g.*, Jay Greene, *Microsoft Official Cites "Sobering" Use of Technology*, WALL ST. J., July 14, 2018, at B3 (quoting Microsoft president and chief legal officer Brad Smith as saying government's use of facial-recognition software is "sobering"); Madalyn Velisaris, *New Bill Raises Privacy Concerns*, (June 19, 2018) https://dailyillini.com/news/2018/06/19/new-bill-raises-employment-privacy-concerns/ (reporting both houses of the Illinois General Assembly have passed Senate Bill 2907, amending the Criminal Identification Act, that allows employers "to get real-time notifications when a [fingerprinted employee] breaks the law anywhere in the United States," as opposed to the one-time snapshots previously available from government agencies); Zolan Kanno-Youngs & Robert McMillan, *Controversial Facial System Identifies Suspect*, WALL ST. J., June 30, 2018, at A3 (county official "fed a photograph of the [Capital Gazette mass shooting] suspect into the Maryland Image Repository System, a database of mug shots and driver's license photos" – facial recognition software similar to that used by 31 states); Tiffany Lee, *Biometrics and Disability*

security systems of vendors and other third parties, SEC disclosures on internal risks concerning cyber exposure and security,[67] and tying top executive pay to cybersecurity goals. The second article focused on helpful hints concerning the number one risk: employees. Much like Passman's paper, this second article spoke of team leadership, employee training, filters to fend off suspicious emails, active reminders, and accountability through measurement – "if you cannot measure it, you cannot manage it." If these Wall Street Journal articles are not enough, excellent background papers examining related problems can be found in recent issues of the DePaul Law Review and the Sedona Conference Journal.[68]

In short, secrecy measures need to be established and then followed. This is particularly true when it comes to documenting access to and the return or destruction of data. Proper attention to data management on the front end may avoid public humiliation on the back end.[69]

V. HOW DO YOU IDENTIFY TRADE SECRETS?

Another common theme in both *Rockwell* and *George S. May International* concerned trade secret identification, as the preceding passages reflect. If trade secrets could be registered and recorded like patents, copyrights and trademarks, trade secret identification would not be much of an issue. Property registration, epitomized by real estate recording systems, fosters economic growth by precluding or at least limiting ownership and boundary disputes. Hernando de Soto offers illuminating real estate examples of this phenomena in his wonderful book, *The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else*,[70] not least President Abraham Lincoln's signing of the Homestead Act in 1862.[71] As de Soto noted in a more recent Wall Street Journal piece he co-authored with

---

Rights: Legal Compliance in Biometric Identification Programs, 2016 U. ILL. J.L. TECH. & POL'Y 209, 212-17 (2016) (describing federal and state biometric programs).

[67] *See* Jennifer C. Archie & Serrin A. Turner, *5 Key Takeaways on Cybersecurity*, (June 1, 2018) https://www.lexology.com/library/detail.aspx?g=4f161971-50ab-4403-a983-1bfddd8edc14 (reviewing SEC guidance and recommending five steps: (1) disclosing the board's role in managing cybersecurity; (2) including disclosure review in incident response procedures; (3) mitigating insider trading risk after cybersecurity incidents; (4) disclosing promptly material incidents; and (5) avoiding generic disclosures).

[68] See Stephan Landsman, et al., *Symposium: Privacy, Data Theft and Corporate Responsibility*, 66 DEPAUL L. REV. 311, 313-604 (2017) (offering 11 articles on aspects of data theft responsibility); Sedona Conference Working Group on Data Security and Privacy Liability, *The Sedona Conference Data Privacy Primer*, 19 SEDONA CONF. J. 273, 419-31 (2018) (discussing workplace privacy issues relating to company equipment and email, "bring your own device" policies, social media usage, passwords and other login information, and content monitoring).

[69] Edward A. Morse, Vasant Raval & John R. Wingender, Jr., *SEC Cybersecurity Guidelines: Insights into the Utility of Risk Factor Disclosures for Investors*, 73 BUS. LAW. 1 (2018) (discussing cybersecurity concerns for purposes of public company disclosures).

[70] HERNANDO DE SOTO, THE MYSTERY OF CAPITAL: WHY CAPITALISM TRIUMPHS IN THE WEST AND FAILS EVERYWHERE ELSE 111 (2000).

[71] *Id.* at 155.

former Senator Phil Gramm: "It's a simple yet startling fact: The road to economic development runs through the county clerk's office at the local courthouse."[72]

To IG professionals, Gramm and de Soto's prescription for modernizing property registration – blockchain – cannot come as a surprise.[73] Gramm and de Soto love its recordkeeping capacity, its accessibility to millions of users, and its ease of updating.[74] Banks love it too and are busy patenting it.[75] Could blockchain be adapted in some fashion to record and update trade secrets, perhaps in a publicly-controlled but restricted-access registry?[76] Would secrets eventually be compromised despite their owners' best efforts?[77]

Alas, we will have to wait to find out because, as noted, at present no central registry for trade secrets exists. This presents several serious problems. One is

---

[72] Phil Gramm & Hernando de Soto, *How Blockchain Can End Poverty*, WALL ST. J., Jan. 26, 2018, at A15.

[73] *See* Frank Fazzio, *Blockchain for Information Governance: The IG Use Case*, (March 12, 2018) https://www.zasio.com/blockchain-for-information-governance-the-ig-use-case/ ("Information Governance (IG) and records management are a natural fit for blockchain technology because these fields value data based on its authenticity, integrity, and reliability. However, any potential blockchain application would need to be flexible enough to meet the needs of enterprise users. In addition to managing records through their lifecycle, a blockchain solution for IG would need to be economically feasible and integrate with normal business operations and existing systems. It would also need to be secure against cyber threats, particularly in light of recent major heists at Japanese cryptocurrency exchanges Mt. Gox and Coincheck.").

[74] Gramm & de Soto, *supra* note 72. ("If Blockchain technology can empower public and private efforts to register property rights on a single computer platform, we can share the blessings of private-property registration with the whole world.").

[75] *See* Inayat Chaudhry, *The Patentability of Blockchain Technology and the Future of Innovation*, A.B.A. LANDSLIDE MAG., Vol. 10, No.4, at 21, 24 (April 2018) ("The most notable patent filers in the blockchain technology space have been banks" – including Goldman Sachs, Bank of America and Mastercard); Thomas Franklin & Brian Olion, *IP Issues Surrounding Blockchain Technology Implementation*, L.WK. COLO., Vol. 16, No. 20 (May 14, 2018) ("Last year alone more than 1,248 blockchain-based patent applications were filed across China, the EU, Japan, South Korea and the U.S., a huge jump over the prior four years. This explosive growth shows that entities realize the value of patenting blockchain technology."); Gurneet Singh, *Are Internet-Implemented Applications of Blockchain Technology Patent-Eligible in the United States?*, 17 CHI.-KENT J. INTELL. PROP. 356, 376 (2018) ("The federal case law narrows the scope of § 101, and permits patent-eligibility of some, not all, aspects of internet-implemented applications of block-chain technology.").

[76] *See* ADRIAN JOHNS, PIRACY: THE INTELLECTUAL PROPERTY WARS FROM GUTENBERG TO GATES 216-20 (2009) (describing the Enlightenment's "universal library" movement, with roots "extending back to the Library of Alexandria and forward to utopian visions of the Internet," and the late Georgian-era "legal deposit" rule requiring "copies of each book published in Britain … to be turned over to select libraries" – a rule that "rested [in Britain] on the ancient universities and the principle of deposit, which dated back to 1610"); Nir Kshetri, *Blockchain Could Be the Security Answer. Maybe*, WALL ST. J., May 30, 2018, at R7 (describing "private key" and "public key" access to blockchain system but noting possible problem with identity and access management relying on passwords "exchanged and stored on insecure systems").

[77] Steven Johnson, *Beyond the Bitcoin Bubble*, (Jan. 16, 2018) https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html ("If there's one thing we've learned from the recent history of the internet, it's that seemingly esoteric decisions about software architecture can unleash profound global forces once the technology moves into wider circulation."); AP, *Bitcoin Tumbles to 4-Month Low of $6370 After Hacking Report*, CHI. SUN-TIMES, June 14, 2018, at 20 (reporting hackers stole $37 million – nearly one-third – of South Korean digital currency exchange Coinrail's virtual currency).

"overclaiming," whether in transactions or in litigation. As it happens, Judge Posner addressed this, too, in *Rockwell*:

> Perhaps thinking of the doctrine of patent misuse (on which see *USM Corp. v. SPS Technologies, Inc.*, 694 F.2d 505, 510-12 (7th Cir.1982), and cases cited there), DEV suggests that if a firm claims trade secret protection for information that is not really secret, the firm forfeits trade secret protection of information that is secret. There is no such doctrine — even the patent misuse doctrine does not decree forfeiture of the patent as the sanction for misuse — and it would make no sense. This is not only because there are any number of innocent explanations for Rockwell's action in "overclaiming" trade secret protection (if that is what it was doing) — such as an excess of caution, uncertainty as to the scope of trade secret protection, concern that clerical personnel will not always be able to distinguish between assembly and piece part drawings at a glance, and the sheer economy of a uniform policy — but also because it would place the owner of trade secrets on the razor's edge. If he stamped "confidential" on every document in sight, he would run afoul of what we are calling (without endorsing) the misuse doctrine. But if he did not stamp confidential on every document he would lay himself open to an accusation that he was sloppy about maintaining secrecy — and in fact DEV's main argument is that Rockwell was impermissibly sloppy in its efforts to keep the piece part drawings secret.[78]

Judge Posner was certainly right that either underclaiming or overclaiming trade secrets places the owner "on the razor's edge," but his forgiving attitude on overclaiming might not be as representative of judicial thought today as it was in 1991. Judges today are beginning to question trade secret assertions, particularly when they operate to restrict employee mobility or to otherwise stifle competition. A recent California case, *Cypress Semiconductor Corp. v. Maxim Integrated Products*,[79] for example, approved a bad faith fee award of $180,000 against plaintiff Cypress for using baseless trade secret litigation to restrain a competitor's employee raiding efforts. The court's decision rested in part on Cypress' inability and unwillingness to identify its secrets with particularity at the outset of the case, as required under California law. Cypress' choice to voluntarily dismiss its own case did not preclude the $180,000 award, the California Court of Appeal held.

Although California has a statute requiring plaintiff to identify its trade secrets before pursuing discovery against defendant, most states do not. The new DTSA also is silent on this issue. As a result, parties jockey for tactical advantage in these cases. Plaintiff contends it needs to know what defendant stole before plaintiff can identify its relevant secrets, an argument with some force when plaintiff has thousands of secrets and defendant has perhaps stolen only one or two. Defendant, in turn, maintains that it needs to know exactly what it is charged with stealing so it can prepare an adequate defense. Defendant also claims that unless plaintiff is forced to go first with identification, plaintiff will shape its secrets to fit what

---

[78] *Rockwell*, 925 F.2d at 176-77.

[79] 236 Cal. App. 4th 243 (2015).

defendant happens to have in its possession. Judicial approaches to this problem vary, with some judges requiring early and specific identification by plaintiff, some allowing identification amendments by plaintiff for good cause, and some ordering simultaneous disclosure by plaintiff and defendant.[80]

A related litigation issue concerns courts: identification of secrets is needed to make injunction orders sufficiently specific to place the defendant on notice as to what he or she cannot do. Indeed, Rule 65 of the Federal Rules of Civil Procedure demands such specificity, as the Seventh Circuit Court of Appeals held in *Patriot Homes, Inc. v. Forest River Housing, Inc*.[81] The district court there granted a preliminary injunction prohibiting defendant Sterling from "[u]sing, copying, disclosing, converting, appropriating, retaining, selling, transferring, or otherwise exploiting Patriot's copyrights, confidential information, trade secrets, or computer files."[82] The district court's order also required Sterling to "[c]ertify that copied data and materials of Patriot's property, confidential information and trade secrets on computer files and removable media (CDs, DVDs, tapes, etc.) have been deleted or rendered unusable."[83] The Court of Appeals vacated the preliminary injunction as too vague from a trade secret identification standpoint:

> The preliminary injunction entered by the district court uses a collection of verbs to prohibit Sterling from engaging in certain conduct, but ultimately it fails to detail what the conduct is, i.e., the substance of the "trade secret" or "confidential information" to which the verbs refer. While the law prohibits using another's trade secrets, *American Can Co. v. Mansukhani*, 742 F.2d 314, 328 (7th Cir.1984), it is not clear from the injunction order what the trade secret or confidential information is in this case. Patriot claims that its trade secret is the "playbook" for constructing modular homes consisting of its blueprints, engineering calculations, quality control manuals, and other documents. But it does not deny that much of this information was readily available when Sterling submitted FOIA requests because at that time Patriot had not asked the states to keep the information confidential.[84]

Identification might seem primarily to be a litigation conundrum, but it arises in transactional settings as well. One is overbroad employment or commercial agreements that use generic trade secret descriptions. These invite disputes about what is and is not covered, and some courts will not enforce them.[85] For example, in

---

[80] *See* William Lynch Schaller, *Secrets of the Trade: Tactical and Legal Considerations from the Trade Secret Plaintiff's Perspective*, 29 U. TEX. REV. LITIG. 730, 798-806 (2010) (collecting cases).

[81] 512 F.3d 412 (7th Cir. 2008).

[82] *Id*. at 414.

[83] *Id*.

[84] *Id*. at 415.

[85] *Compare* IDX Sys. Corp. v. Epic Sys. Corp., 285 F.2d 581, 586 (7th Cir. 2002) (criticizing argument that overbroad nondisclosure agreements are void), *with* Am. Family Mut. Ins. Co. v. Roth, 485 F.3d 930, 933 (7th Cir. 2007) (contract that forbids disclosure of customer information is enforceable—"but only if the contractual prohibition is reasonable in time and scope, and, specifically, only if its duration is limited") (applying Wisconsin law, but citing Illinois cases for support)), *and* Fleetwood Packaging v. Hein, No. 14 C 9670, 2015 WL 6164957 (N.D. Ill. Oct. 20, 2015) (refusing to enforce overbroad nondisclosure agreement).

AssuredPartners, Inc. v. Schmitt the Illinois Appellate Court refused to enforce a confidentiality agreement that purported to cover all information relating to the "business or affairs of the Company."[86] A second transactional context is failure to comply with agreements that require a party to identify its trade secrets when it discloses them for some purpose, such as during deal due diligence. Failure to follow the governing contract is a recipe for loss of secrecy.[87]

How can IG professionals help? They can insist on careful cataloging of trade secrets as their firm develops and refines them – "record as you go," so to speak. They can also insist on strict compliance with identification conditions called for in company agreements – i.e., if the contract requires it, label them as trade secrets before handing them over to outsiders. At the very least, IG practitioners can request indirect identification by asking that "trade secret" or "confidential information" legends be placed on computer screens and documents to put others on notice of the company's trade secret assertion. They might even go so far as to encourage the firm to periodically purge trade secrets once they are found in the public domain or once their shelf life has expired.

VI. WHAT CONSTITUTES MISAPPROPRIATION?

The concept of misappropriation has some subtle features that may surprise casual observers. IG professionals need to understand them if they are going to be part of the information protection team. They may also want to know them to avoid personal liability for someone else's wrongdoing.

Allegations of unauthorized acquisition, use or disclosure of trade secrets form the heart of all trade secret theft cases.[88] In some instances the proof is direct: an employee or other insider gets caught on camera copying documents as part of a scam. This occurred in a well-known case involving a Coca-Cola executive secretary, Joya Williams, who stole marketing campaign secrets and tried to sell them to rival Pepsi.[89] She did not know Pepsi called Coca-Cola to warn of the conspiracy. Coca-Cola then called the FBI and installed cameras that recorded her engaging in theft.[90] Williams received an eight-year sentence for her flagrant misconduct.

---

[86] 44 N.E.3d 463 (1st Dist. 2015).

[87] *See, e.g.*, Nilssen v. Motorola, Inc., 963 F. Supp. 664, 680-82 (N.D. Ill. 1997) (failure to follow contractual protocol for designating secrets waived secrecy protection).

[88] *See* Seng-Tiong Ho v. Taflove, 648 F.3d 489, 503 (7th Cir. 2011) ("A claim of trade secret misappropriation, then, requires that the information have a status of secrecy and that a confidential relationship be breached."); Drew Harwell, *Former Employee Sued by Tesla Says He Was a Whistleblower, Alarmed by Company Practices and Elon Musk*, (July 2018) https://www.washingtonpost.com/news/the-switch/wp/2018/06/20/tesla-sues-former-employee-as-elon-musk-signals-hunt-for-saboteurs/?utm_term=.b579366f323a (reporting on *Tesla, Inc. v. Tripp*, No. 2:18 cv 01088 (D. Nev. June 20, 2018), in which Tesla alleged former employee Martin Tripp hacked into the company's computers to steal trade secrets).

[89] *See* U. S. v. Williams, 526 F.3d 1312 (11th Cir. 2008) (affirming Williams' eight-year prison sentence).

[90] *Id.* at 1317 ("On June 12, 2006, Coca-Cola security installed additional cameras near Williams' work area. Footage from the cameras showed Williams at her desk going through multiple files looking for documents. After locating them, Williams placed the papers into her personal bag. In some cases, Williams stuffed papers into a plastic bag before placing them in her

But it is not necessary to get caught on Candid Camera. More often the proof is circumstantial, along the lines of Judge Posner's observations in *Rockwell*:

> Rockwell is unable to prove directly that the 100 piece part drawings it got from DEV in discovery were stolen by Fleck and Peloso or obtained by other improper means. But if it can show that the probability that DEV could have obtained them otherwise — that is, without engaging in wrongdoing — is slight, then it will have taken a giant step toward proving what it must prove in order to recover under the first theory of trade secret protection.[91]

A third misappropriation theory is more elusive and hence more dangerous: inevitable disclosure. In some circumstances, the theory runs, an employee cannot avoid drawing on a former employer's trade secrets in working for a new employer in a similar position[92] – becoming, in effect, "the man (or woman) who knew too much." The doctrine has been around in some form for at least 100 years,[93] but trade secrets owners began relying on it more frequently in the late 1980s and early 1990s.[94] It became well accepted nationwide in the wake of the Seventh Circuit Court of Appeals' 1995 decision endorsing it in *PepsiCo, Inc. Redmond*,[95] with the prominent exception of California.[96] While the DTSA appears to forbid inevitable disclosure claims under that federal statute,[97] as Ken Vanko and Dave Bohrer have pointed out,[98] the DTSA also expressly preserves all state law claims[99] – suggesting that

---

bag. Williams was also observed holding a new Coca-Cola product sample before placing it into her personal bag.").

[91] *Rockwell*, 925 F.2d at 178-79.

[92] *See* C & F Packing Co., Inc. v. IBP, Inc., No. 93 C 1601, 1998 WL 1147139, 8-9 (N.D. Ill. Mar. 16, 1998) (quoting deposition testimony of former C & F Packing employee McDaniel in denying defense summary judgement motion in "inherent disclosure" case: "Q: Did you draw on your experience at C & F with the Italian sausage toppings to help solve problems at IBP? A: I tried to keep things separate. Whether I did it unknowingly or not, I cannot say.").

[93] *See* William Lynch Schaller, *Trade Secret Inevitable Disclosure: Substantive, Procedural and Practical Implications of an Evolving Doctrine*, 86 J. PAT. & TRADEMARK OFF. SOC'Y 336 (2004) (reviewing history of the inevitable disclosure doctrine).

[94] *See, e.g.*, Norand Corp. v. Parkin, 785 F. Supp. 1353 (N.D. Iowa 1990) (issuing inevitable disclosure restraining order against marketing employee who jumped ship from bar coding scanning firm Norand to rival Symbol Technologies).

[95] 54 F.3d 12612 (7th Cir. 1995).

[96] *See, e.g.*, Whyte v. Schlage Lock Co., 101 Cal.4th 1443 (2002).

[97] *See* 18 U.S.C. § 1836(b)(3)(A)(i)(I) & (II) (a DTSA injunction shall not "prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows" or "otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business").

[98] *See* Kenneth J. Vanko, *Revisiting the Seventh Circuit's Decision in PepsiCo: Inevitable Disclosure Injunctions in the Wake of the Federal Defend Trade Secrets Act of 2016*, CIR. RIDER, at 46, 50 (April 2017) (arguing the DTSA limits inevitable disclosure claims under federal law, but not under Illinois state law); David Bohrer, *Threatened Misappropriation of Trade Secrets: Making a Federal (DTSA) Case Out of It*, 33 SANTA CLARA COMPUTER & HIGH TECH. L.J. 506, 527-28 (2017) (reviewing language and legislative history reflecting DTSA's rejection of "inevitable disclosure" doctrine).

state law claims for inevitable disclosure can be joined with federal law claims under the DTSA. In general, injunctive relief is the remedy sought and received in most such cases, as exemplified by the five-moth injunction approved in *PepsiCo*. However, as a practical matter the inevitable disclosure rule can be more dangerous because it pries open the defendant firm's files and sometimes reveals actual theft or other wrongdoing far greater than plaintiff initially imagined.[100]

The nuances of direct, circumstantial and inevitable disclosure evidence of misappropriation may not matter so much when an IG professional is working for plaintiff; how the firm as victim proves theft is mainly a company matter. But these distinctions might matter greatly if the IG professional is working for the accused firm. Vicarious liability claims, like civil conspiracy or aiding and abetting, could be alleged against the IG professional individually if he or she knew of and assisted the thief. This might arise, for instance, if an employer discovers a new employee stole a former employer's secrets and orders the information protection team – including the IG professional – to destroy all evidence of the theft, or worse, allows the accused employee himself to destroy it, as Uber apparently did with Levandowski.

Such a housecleaning might seem appropriate at first blush, but can the IG professional or any other member of the team really know what is and is not a secret of the former employer? Does the team realize that trade secret law governs not only the stolen secrets but also anything "derived" from them as well?[101] What are the metes and bounds of the problem the team is now facing? Shouldn't the team instead preserve all evidence and have the firm's general counsel call the former employer for permission to destroy such evidence or to offer to return it, as Pepsi did in the Coca-Cola case?[102] If these simple steps are unsatisfactory, the two firms could develop a

---

[99] *See* 18 U.S.C. § 1838 ("Except as provided in section 1833(b), this chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act)").

[100] *See* William Lynch Schaller, *Corporate Opportunities and the Third Party "Refusal to Deal" Defense: Policy and Practice Lessons from Illinois*, 47 J. MARSHALL L. REV. 1 (2013) (discussing sweeping implications of fiduciary duty law); William Lynch Schaller, *Corporate Opportunities and Corporate Competition in Illinois: A Comparative Discussion of Fiduciary Duties*, 46 J. MARSHALL L. REV. 1, 1-2 (2012) ("Illinois courts have long understood how vulnerable firms are to fiduciary disloyalty, and they frequently call upon noncompetition agreements and trade secret law to remedy it. *** [But] corporate opportunity and corporate competition claims are actually far more powerful than their restrictive covenant and trade secret counterparts, as these fiduciary duty theories do not require proof of an agreement, evidence of secrecy measures, or other factual and legal clutter that tends to derail contract and trade secret charges.").

[101] *See* Mangren Research & Dep't Corp. v. Nat'l Chem. Co., Inc., 87 F.3d 937, 944 (7th Cir. 1996) ("[I]f trade secret law were not flexible enough to encompass modified or even new products that are substantially derived from the trade secret of another, the protections that law provides would be hollow indeed."); Sokol Crystal Prods., Inc. v. DSC Commc'ns. Corp., 15 F.3d 1427, 1430-31 (7th Cir. 1994) (discussing "derived from" trade secret standard); *In re* Innovative Constr. Sys., Inc., 793 F.2d 875, 887 (7th Cir. 1986) ("[T]he user of another's trade secret is liable even if he uses it with modifications or improvements upon it effected by his own efforts, so long as the substance of the process used by the actor is derived from the other's secret.").

[102] *See* BEN W. HEINEMAN, JR., THE INSIDE COUNSEL REVOLUTION: RESOLVING THE PARTNER-GUARDIAN TENSION, at 52 (2016) (discussing an instance in the early 1990s in which General Electric (i) discovered, investigated and then reported fraud and misappropriation of government

joint protocol on how to resolve the issue, perhaps by bringing in a neutral third-party to collect and inspect the data.[103] Surely this controlled process is preferable to indeterminate and interminable litigation[104] – litigation that will be intrusive by any measure and may even commence with a search and seizure order under the DTSA or state law.[105]

VII. WHEN IS MISAPPROPRIATION A CRIME?

The preceding discussion of conspiracy, aiding and abetting and evidence destruction may alarm any sentient IG practitioner. And well it should; prosecuting trade secret theft is a top priority for the Department of Justice. The Obama Administration made this clear, and the Trump Administration promises more of the same.[106] Consider the Obama Administration's 2013 policy statement:

> The Department of Justice has made the investigation and prosecution of corporate and state sponsored trade secret theft a top priority. The Department of Justice and the FBI will continue to prioritize these investigations and prosecutions and focus law enforcement efforts on

---

funds at its Israeli unit, (ii) terminated or disciplined scores of employees, (iii) instituted system reforms, and (iv) paid penalties and fines).

[103] *See* Victoria Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, 49 IDEA: INTELL. PROP. L. REV. 359, 361-62 (2008) (discussing forensic analytics, including identification of stolen electronic documents through digital watermarks).

[104] *See, e.g.*, Motorola Sols., Inc. v. Hytera Commc'n. Corp., 314 F.Supp.3d 931, 933-34 (N.D. Ill. 2018) (Cole, M.J.) (recounting the court's earlier invitation to have the parties agree on a forensic computer imaging protocol that would not run afoul of Chinese law; noting over 7500 pages of court filings followed on a "preliminary" discovery fight over imaging of seven employee computers in China just on the threshold issue of whether Motorola's trade secret claim was timely filed; stressing that Motorola had already received 700,000 documents comprising over 3 million pages; likening the fight to the Punic Wars; and then quoting Winston Churchill: "Now this is not the end. It is not even the beginning of the end.").

[105] *See* 18 U.S.C. § 1836(b)(2) (setting forth detailed rules for search and seizures in DTSA cases); Am. Can Co. v. Mansukhani, 742 F.2d 314 (7th Cir. 1984) (discussing Rule 65 ex parte temporary restraining orders authorizing search and seizures in trade secret cases long before the DTSA); Michael T. Renaud, Bret Cohen & Nick Armington, *The DTSA and Civil Seizure Under Federal Rule of Civil Procedure 65*, (Jan. 30, 2017) https://www.mintz.com/insights-center/viewpoints/2017-01-dtsa-and-civil-seizure-under-federal-rule-civil-procedure-65 (discussing interplay between DTSA civil seizure and Rule 65 injunctive relief).

[106] *See* Barak Cohen, Christopher K. Veatch & John Barkley Sample IV, *Criminal Trade Secret Prosecutions Under Trump – One Year Later*, (June 14, 2018) https://www.perkinscoie.com/en/news-insights/criminal-trade-secret-prosecutions-under-trump-one-year-later.html (noting nine new trade secret theft criminal cases under the Trump Administration were all against foreign nationals or those assisting them, but speculating that "changing priorities, including a focus on violent crime and immigration matters, may negatively impact the DOJ's resources for and commitment to future trade secret prosecutions in the foreseeable future"); Barak Cohen & Chelsea Curfman, *How Will Criminal Trade Secret Prosecutions Fare Under President Trump?,* (Jan. 4, 2017) https://www.perkinscoie.com/en/news-insights/how-will-criminal-trade-secret-prosecutions-fare-under-president.html ("While the answer is uncertain, statements by the President-elect and his U.S. Attorney General nominee, Jeff Sessions, suggest that the Trump administration may be equally, if not more, likely to encourage prosecution of suspected trade secret theft, particularly when foreign nationals and national security are involved.").

> combating trade secret theft. The FBI is also expanding its efforts to fight computer intrusions that involve the theft of trade secrets by individual, corporate, and nation-state cyber hackers. The Department of Homeland Security component law enforcement agencies will continue to work cooperatively with the Department of Justice when its investigations uncover evidence of trade secret theft.[107]

Prosecution of Chinese firm Sinovel Wind Group provides an example.[108] Once a major customer of wind turbine software maker AMSC, Sinovel decided to steal AMSC's software that regulated the flow of electricity from wind turbines to electrical grids. To this end, Sinovel hired away a key engineer working in AMSC's Austrian subsidiary and had him download software code before leaving. He then passed the secret code to Sinovel, which thereafter refused to pay AMSC $800 million for products Sinovel had contracted to buy. A jury convicted Sinovel and several Sinovel executives of trade secret theft in a verdict rendered in January 2018, and the court thereafter ordered a substantial fine and restitution.[109]

For present purposes, there are two important things to remember: (i) trade secret cases almost always involve crimes and (ii) any number of criminal law theories can ensnare unwary IG professionals who end up working with a thief. Among these are substantive crimes like conspiracy to steal trade secrets and aiding and abetting trade secret theft, as might happen if an IG professional knowingly assists a thief. But equally worrisome are process crimes like obstruction of justice, lying to federal agents, witness tampering, subornation of perjury, and perjury. Any of these might arise if evidence of stolen secrets is hidden or destroyed, if FBI agents are told lies, or if suspicious conversations with the thief take place.

Uber ran into a variant of this problem in its dispute with Google/Waymo: ex-employee Richard Jacobs alleged Uber tried to cover its tracks by using a secret messaging system, an allegation Uber claimed was part of Jacobs' attempt to extort Uber.[110] Uber ran into another variant of it when Judge Alsup in the Google/Waymo

---

[107] *See Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, https://www.justice.gov/criminal-ccips/file/938321/download (Feb. 2013), at 11; Aruna Viswanatha, *U.S. Accuses Chinese Operative of Stealing Trade Secrets*, WALL ST. J., Oct. 11, 2018, at A1 (reporting indictment and arrest of Yanjun Xu – said to be the first Chinese national the United States has publicly identified as a Chinese government intelligence officer engaged in trade secret theft – for allegedly targeting a General Electric Aviation employee in a Chinese effort to steal information about composite material General Electric Aviation uses in manufacturing fan blades and fan-blade encasements).

[108] Department of Justice Press Release, *Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of AMSC Trade Secrets: Theft of Trade Secrets Allegedly Cheated AMSC of More Than $800 Million*, (June 27, 2013) https://www.justice.gov/opa/pr/sinovel-corporation-and-three-individuals-charged-wisconsin-theft-amsc-trade-secrets.

[109] *See* Department of Justice Press Release, *Court Imposes Maximum Fine on Sinovel Wind Group for Theft of Trade Secrets*, (July 6, 2018) https://www.justice.gov/opa/pr/court-imposes-maximum-fine-sinovel-wind-group-theft-trade-secrets (reporting fine of $1.5 million, restitution of nearly $58 million, and other relief).

[110] *See* Paayal Zaveri & Deirdre Bosa, *Uber: Ex-Employee's Claim That We Hid Trade Secret Theft Was an Effort to Extort Money*, (Nov. 29, 2017) https://www.cnbc.com/2017/11/29/uber-ex-employee-was-trying-to-extort-money.html ("Angela Padilla, deputy general counsel at the company, said in court testimony that the allegation from ex-employee Richard Jacobs that the company took steps to cover its tracks when stealing trade secrets from Alphabet's Waymo was not true. She

litigation referred the matter to the United States Attorney for criminal investigation and prosecution.[111] These developments underscore the dangerous interplay between civil and criminal litigation in trade secret cases. Indeed, sometimes civil cases uncover powerful evidence of which previously-reluctant prosecutors may have been unaware, thereby heightening the risk prosecutors will bring charges. This happened in the well-known trade secret litigation DuPont brought against Kolon Industries for theft of DuPont's Kevlar trade secrets, resulting in $360 million in fines and restitution.[112]

VIII. WOULD YOU LIKE TO TESTIFY?

IG practitioners can contribute to trade secret protection and defense of claims in all of the areas outlined above. But there is one particular task they can perform better than most: testifying about the company's information governance policies and procedures.

As one of the few employees with comprehensive knowledge of the company's information governance practices, an IG professional can be designated as a witness to speak for (and bind) the company under Rule 30(b)(6) of the Federal Rules of Civil Procedure. Or the IG practitioner might be offered as just a narrative witnesses to explain how the firm stores, monitors, retrieves and destroys data. The need for such testimony can arise during discovery and certainly can arise during trial, where a jury might be assisted in understanding a firm's information practices by a knowledgeable witness who can also tell a story.

An illustrative case worth examining is *Illinois Tool Works, Inc. v. Metro Mark Products, Ltd*.[113] ITW sued Metro Mark for trade secret theft after two ITW employees jumped ship to Metro Mark. The court issued an evidence preservation order at the outset and the parties eventually had a dispute over the completeness of Metro Mark's discovery response concerning invoices. This dispute ultimately turned on information maintained on a Packard Bell computer – a computer Metro Mark record keeper Thomas Heinzel claimed had been repeatedly damaged through

---

added that Jacob's claims were an effort to extort money from the company. The evidence in question is a letter from Jacobs' attorney alleging that Uber advised employees to use ephemeral messaging systems, like Wickr, and non-attributable devices to hide their tracks to protect the company from potential litigation.").

[111] *See* Tom Krisher, *Judge Refers Uber Theft Allegations to U.S. Attorney*, (May 12, 2017) https://www.detroitnews.com/story/business/autos/mobility/2017/05/12/uber-waymo/101606274/.

[112] *See* Lindsay Dunsmuir, *Kolon Industries Pleads Guilty in DuPont Kevlar Trade Secrets Case*, (April 30, 2015) https://www.reuters.com/article/us-dupont-kolon-lawsuit/kolon-industries-pleads-guilty-in-dupont-kevlar-trade-secrets-case-idUSKBN0NL2B220150430 (reporting Kolon's guilty plea to conspiracy to steal trade secrets, Kolon's agreement to pay $275 million in restitution and $85 million in criminal fines, and Kolon's confidential settlement with DuPont resolving a $919 million jury award and 20-year worldwide injunction that had both been reversed on appeal); *Federal Prosecution of Trade Secret Theft*, (Jan. 2014) https://www.quinnemanuel.com/the-firm/news-events/article-january-2014-federal-prosecution-of-trade-secret-theft/ ("The Department of Justice had initiated and ceased investigating the offense before DuPont filed suit, but partly on the basis of evidence DuPont discovered in the civil case – including documents that federal authorities would have otherwise had to obtain through time-consuming coordination with the foreign government – federal prosecutors sought and obtained an indictment of the foreign firm and the executives.").

[113] 43 F. Supp. 2d 951 (N.D. Ill. 1999).

various accidents. As Heinzel was one of the ex-ITW employees who departed to Metro Mark, his records were of particular interest, as were his shifting explanations for the condition of his computer. Miraculously, forensic experts located a treasure trove of new documents on the Packard Bell computer, contrary to Heinzel's assurances that all documents had already been produced. The court sanctioned Metro Mark for obstructing discovery, to no one's surprise.

Federal and state judicial reports teem with cases like *Illinois Tool Works*.[114] While some concern intentional destruction or secreting of evidence, many more simply involve incoherent or changing stories about how information was collected, stored and retrieved. In a trade secret theft case like *Illinois Tool Works*, a comprehensive and cogent explanation of information governance practices can spell the difference between victory and defeat.

IX. CONCLUSION

If one puts aside the ransomware cases, trade secret theft always involves misguided notions about competition. Trade secret theft is not competition; it is unfair competition. By the same token, as Judge Posner reminded in another Uber case, "'[p]roperty' does not include a right to be free from competition."[115] Thus, trade secret law seeks to balance property and competition interests.[116]

In striking this balance, trade secret law insists upon proof of theft. Independent development and reverse engineering do not constitute theft, and for this reason hiring a rival's employee or consultant or disassembling a rival's product are usually legitimate forms of competition. But once a competitor knows or has reason to know that a rival's secrets are being disclosed or used, competition becomes wrongdoing. In fact, it often becomes a crime. And the authorities are only too willing to prosecute it.

Trade secret misappropriation, when viewed in this light, becomes a serious business indeed. Like moths to a flame, IG professionals are drawn to these cases by virtue of their job: handling information. Understanding the rules of the game is imperative for IG practitioners who want to protect their companies. But it is equally imperative for IG practitioners who want to protect themselves.

---

[114] *See, e.g.,* Arthur Andersen LLP v. U. S., 544 U.S. 696 (2005) (reversing accounting firm Arthur Andersen's conviction for obstruction of justice in connection with the collapse of Enron; Andersen managers' instructions to employees to delete Enron-related files were in accordance with the firm's document retention policy and hence were not knowingly corrupt); MPCT Sols. Corp. v. Methe, 1999 U.S. Dist. LEXIS 10703 (N.D. Ill. July 2, 1999) (granting sanctions against defendant for violating court order requiring preservation of computer evidence); Peal v. Lee, 403 Ill. App. 3d 197, 454 (1st Dist. 2010) (affirming dismissal as sanction for plaintiff's deliberate deletion of "thousands of files from his personal computer, using multiple programs with names like File Shredder and Privacy Eraser Pro"); Liebert Corp. v. Mazur, 357 Ill. App. 3d 265 (1st Dist. 2005) (discussing computer evidence destruction and forensic recovery efforts).

[115] Int'l Transp. Trade Ass'n v. City of Chi., 839 F.3d 594, 596 (7th Cir. 2016).

[116] *See* PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 1268 (7th Cir. 1995) ("Trade secret law serves to protect 'standards of commercial morality' and 'encourage[ ] invention and innovation' while maintaining 'the public interest in having free and open competition in the manufacture and sale of unpatented goods.'")