

2011

Restoring Transparency to Automated Authority

Frank Pasquale

Brooklyn Law School, frank.pasquale@brooklaw.edu

Follow this and additional works at: <https://brooklynworks.brooklaw.edu/faculty>



Part of the [Banking and Finance Law Commons](#), and the [Business Organizations Law Commons](#)

Recommended Citation

9 J. on Telecomm. & High Tech. L. 235 (2011)

This Article is brought to you for free and open access by BrooklynWorks. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of BrooklynWorks.

RESTORING TRANSPARENCY TO AUTOMATED AUTHORITY

FRANK PASQUALE*

INTRODUCTION.....	235
I. UNHEALTHY SECRETS: PROPRIETARY PRICES AND ELECTRONIC MEDICAL RECORD IMPLEMENTATION	239
II. TRADE SECRECY AS A BUSINESS TOOL IN THE SEARCH INDUSTRY	244
III. CLANDESTINELY COMMENSURATING COMPUTING IN CONSUMER CREDIT SCORING	248
IV. FROM ENRON TO AIG: A DECADE OF UNREPRODUCIBLE FINANCIAL RESULTS.....	250
CONCLUSION.....	252

INTRODUCTION

Governments and firms in capitalist democracies increasingly use automated processes to allocate punishments and rewards.¹ Some of the most dynamic, profitable, and important companies in the information economy provide these assessments. For example, Google orders websites and advertisements; Internet service providers filter spam and aspire to fast-track certain content. In finance, consumer credit scoring determines who gets which loans, and credit-rating agencies can make or break investment offerings. Reputation-scoring in general is becoming a big business: companies now give scores to doctors and lawyers, landlords

* Schering-Plough Professor in Health Care Regulation and Enforcement, Seton Hall Law School; Affiliate Fellow, Yale Information Society Project; Visiting Fellow, Princeton University Center for Information Technology Policy. I wish to thank Paul Ohm, Phil Weiser, Scott Peppet, Harry Surden, Pierre de Vries, Wendy Seltzer, Eric Schmidt, Angela Morrison, Blake Reid, and other organizers of the 2010 Silicon Flatirons conference for inviting me to participate, and to thank the Princeton University Center for Information Technology Policy for hosting a talk where I was able to further develop the ideas in this paper.

1. Felix Stalder, *Autonomy and Control in the Era of Post-Privacy*, 19 OPEN 78, 81-83 (2010) (describing a rise in automated processes using personalized data).

and tenants, restaurants and hotels. The government has used “risk scoring” in law enforcement and anti-terror contexts, and “audit flags” help the IRS find suspect tax returns.² All of these services utilize automated processes to bring some order to vast amounts of information.³

When automated social sorting first arose, it provoked widespread anxiety.⁴ To quell such fears, authorities tended to emphasize the transparency and objectivity of the systems they used. A computer could treat like cases alike, dispassionately. Anyone who doubted that could “look under the hood” and see for themselves how the system operated. Patent law, with its disclosure requirements, promoted such transparency by conditioning intellectual property protection on publicly inspectable written descriptions of claims.⁵

Over time, flaws in this transparency- and objectivity-based approach to legitimating automated authority emerged. Shrewd or malicious individuals who fully understood such systems could game them. Concern over gaming provoked a shift away from transparency as a legitimation strategy; instead, ironclad secrecy has been pursued. The less the spammers, hackers, black-hat search engine optimizers, terrorists, tax cheats, or manipulators know about the shape of a system,

2. Danielle Keats Citron & Frank A. Pasquale III, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. (forthcoming 2011), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1680390 (critiquing opacity of fusion centers’ public-private partnerships).

3. Search engines in particular use algorithmic authority, which “is the decision to regard as authoritative an unmanaged process of extracting value from diverse, untrustworthy sources, without any human standing beside the result saying ‘Trust this because you trust me.’” Clay Shirky, *A Speculative Post on Algorithmic Authority*, CLAY SHIRKY (Nov. 15, 2009, 4:06 PM) <http://www.shirky.com/weblog/2009/11/a-speculative-post-on-the-idea-of-algorithmic-authority>. There are occasional manual interventions to change search results, but the process is overwhelmingly automated via algorithms. Ira Basen, *The Algorithm Method: Programming Our Lives Away*, GLOBE AND MAIL, Nov. 26, 2010, available at <http://www.theglobeandmail.com/news/technology/the-algorithm-method-programming-our-lives-away/article1815869/print/> (“Most [algorithms] are what engineers call “black boxes” – they convert inputs into outputs without revealing how they do it. The good ones are enormously valuable. Google’s is the spine of a business that currently generates about \$28-billion a year in revenues. Its secrets are not for sharing.”).

4. See, e.g., David Lyon, *Surveillance as Social Sorting: Computer Codes and Mobile Bodies*, in *SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK, AND DIGITAL DISCRIMINATION* 13, 13 (David Lyon ed., 2003) (“Abstract data, now including video, biometric, and genetic as well as computerized administrative files, are manipulated to produce profiles and risk categories in a liquid, networked system.”); LANGDON WINNER, *THE WHALE AND THE REACTOR: A SEARCH FOR LIMITS IN AN AGE OF HIGH TECHNOLOGY* 48 (1986) (describing responses to new technology’s impact on social order).

5. Jeanne C. Fromer, *Patent Disclosure*, 94 IOWA L. REV. 539, 541 (2009) (Patent law requires an inventor to “disclose his invention to the public so that science can progress by building on the divulged knowledge.”).

the better. An alternative form of intellectual property has encouraged this strategy: trade secrecy effectively creates a property right in many algorithms whose creators do not want to disclose them in patent applications. Trade secrecy law also makes it all the more important to keep algorithms secret: once they are disclosed, they lose trade secret protection as a matter of law. State secrecy complements trade secrecy law and provides even greater protection in areas where security is critical, such as when national security is at stake.⁶

The move from legitimation-via-transparency to reassurance-via-secrecy has profoundly troubling implications for the foundations of social order in the information age. Few of us understand how our cars work, but we can, in general, judge whether they have safely and comfortably allowed us to drive to our destinations. We cannot so easily judge the validity of a designation of a person as a bad credit risk, or a website as irrelevant. In many cases, outside observers cannot even understand the full array of commercial or political incentives for such designations. Where it prevails, trade secrecy makes it practically impossible to test whether these ratings are correct. The mere act of designating someone as “certain to repay a loan” makes the likelihood of repayment higher, because the highly rated individual will be more likely to get additional credit to “roll over” any troublesome debts. Similarly, a high ranking on search results can become a self-fulfilling prophecy of relevance, as the highest-ranked sites use revenue from visitors to improve the quality of their content.

Therefore, the spread of technology from machinery to social sorting threatens to entrench self-fulfilling prophecies. Those at the top of the heap succeed in large part due to their designation as likely to succeed; those at the bottom may endure cascading disadvantages. This is a particularly troubling outcome if the bases of such designations can never be discovered, let alone adequately challenged and reviewed.

Unfortunately, the law is presently stacking the deck against accountability for automated authorities. Data-gathering companies can engage in a number of legal maneuvers to hide their actions or hamper audits. For example, copyright protection is available for the original selection and arrangement of databases,⁷ and can in turn be technologically reinforced by “anticircumvention measures” endorsed by

6. See, e.g., David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 671 n.198 (2005) (describing a state secrets privilege that can “deprive[] litigants of their right of access to court”); David E. Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257, 260 (2010) (describing situations where citizens “are in the dark about the fact that they are being kept in the dark.”).

7. U.S. COPYRIGHT OFFICE, REPORT ON LEGAL PROTECTION FOR DATABASES (1997), available at <http://www.copyright.gov/reports/dbase.html>.

the Digital Millennium Copyright Act.⁸ The law of trade secrecy allows companies to recover damages from those who wrongfully disclose confidential data and code.⁹ Finally, even where these forms of intellectual property fail to protect given information and tools for processing it, contractual restrictions can effectively “run with data” if one can only access the data by consenting to an end user license agreement. All of these tactics have been used to protect the intellectual property of a number of business interests, and may even spread through academia.¹⁰

Recent public policy battles have sparked renewed attention to the balance between secrecy and disclosure at large corporations. The financial crisis has highlighted undisclosed risks of the largest financial institutions and the confidential Federal Reserve interventions designed to keep the banking system afloat after disruptive events in the fall of 2008. The implementation of electronic health records will raise fascinating and difficult issues about the ownership and use of health data.¹¹ Finally, Google’s growing role in ordering the Web raises fundamental questions about the proper scope of private initiative in organizing and rationing access to knowledge.¹²

In this thought piece, I will first explain why each of these three sectors—health, general purpose search engines, and finance—risks entrenching troubling trends by continuing down the path of excess secrecy and data proprietization. Just as the “fair use” doctrine has deterred the overpropertization of expression, generally recognized fair information practices should include large and powerful data holders’ obligation to surrender some sample of their data to entities entrusted to audit and assess the data holders’ activities.¹³ Objective audits will help

8. Niva Elkin-Koren, *Making Room for Consumers Under the DMCA*, 22 BERKELEY TECH. L.J. 1119, 1120 (2007) (describing how the ability to exercise “physical control over the use of copyrighted works may threaten intellectual freedom and fundamental liberties.”).

9. RESTATEMENT (FIRST) OF TORTS § 757 (1939); David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135, 192 (2007).

10. See, e.g., STEVEN SHAPIN, *THE SCIENTIFIC LIFE: A MORAL HISTORY OF A LATE MODERN VOCATION* 379 N.20 (2008) (listing critiques of the commercialization of the academy).

11. See, e.g., Adele A. Waller & Oscar L. Alcantara, *Ownership of Health Information in the Information Age*, 69 J. AM. HEALTH INFO. MGMT. ASS’N 28, 28-38 (1998); Mark A. Hall & Kevin A. Schulman, *Ownership of Medical Information*, 301 JAMA 1282, 1282-1284 (2009); U.S. DEPT’ OF HEALTH & HUMAN SERVS., OFFICE OF THE NAT’L COORDINATOR FOR HEALTH INFO. TECH., *RECOMMENDED REQUIREMENTS FOR ENHANCING DATA QUALITY IN ELECTRONIC HEALTH RECORD SYSTEMS*, 4-6 (2007).

12. Pamela Samuelson, *Google Book Search and the Future of Books in Cyberspace*, 94 MINN. L. REV. 1308 (2010).

13. In other work, I have explored the related concept of “reciprocal transparency”; the more an entity strives to learn about citizens, the more accountable its decision making should be. Frank Pasquale, *Data and Power: From Individual Consent to Societal Transparency* 3-6

restore confidence in automated authority.

I. UNHEALTHY SECRETS: PROPRIETARY PRICES AND ELECTRONIC MEDICAL RECORD IMPLEMENTATION

Recent controversy over health insurance reform in the U.S. has highlighted the defects of extant markets for medical products and physician and hospital services. Due to public pressure for disclosure, insurers in Massachusetts and California have recently revealed that they pay very different prices for similar services.¹⁴ As health economist Uwe Reinhardt observes, “Only a handful of Americans truly comprehend the complex payment system for U.S. hospitals—mostly those whose job it is to set, negotiate, and study hospital prices.”¹⁵ The rise of a movement advocating “consumer directed health reform” during the Bush administration led to some small steps toward pricing transparency. Yet trade secrecy law still enables obfuscation of critical data.¹⁶ Open government laws are also failing to fully reveal what the public sector is paying for health care. Even Medicare, a government program, has resisted releasing certain payment data.¹⁷

(2010) (unpublished manuscript), available at <http://www.law.yale.edu/documents/pdf/ISP/PasqualeReciprocalTransparency.pdf>; see Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 NW. U. L. REV. 105, 167 (2010) [hereinafter *Beyond Innovation and Competition*] (discussing the power of the French agency CNIL to “require data controllers to ‘ensure data security and confidentiality,’ to ‘accept on-site inspections by the CNIL,’ and to ‘reply to any request for information’”).

14. Lucette Lagnado, *California Hospitals Open Books, Showing Huge Price Differences*, WALL ST. J., Dec. 27, 2004, at A1; Frank Pasquale, *Partners in Power*, CONCURRING OPINIONS (Jan. 3, 2009, 09:00 PM), http://www.concurringopinions.com/archives/2009/01/partners_in_pow_1.html (“[I]n procedures including coronary bypass, CT-scan of the chest, MRI of the brain, and ultrasound, [the expensive hospitals] appear to offer no quality edge—just far higher prices.”).

15. Uwe E. Reinhardt, *The Pricing of U.S. Hospital Services: Chaos Behind a Veil of Secrecy*, 25 HEALTH AFFAIRS 57, 57-58 (2006).

16. *Id.* at 62 (“[A]ctual dollar payments [paid by insurers to hospitals] have traditionally been kept as strict, proprietary trade secrets by both the hospitals and the insurers. Recently Aetna announced that it will make public the actual payment rates it has negotiated with physicians in the Cincinnati area. That this small, tentative step toward transparency made national news speaks volumes about the state of price-transparency in U.S. health care. It remains to be seen whether that first step will trigger a larger industrywide move toward removing, at long last, the veil that has been draped for so long over the actual prices paid in the U.S. health system.”); see also Annemarie Bridy, *Trade Secret Prices and High-Tech Devices: How Medical Device Manufacturers Are Seeking to Sustain Profits by Propertizing Prices*, 17 TEX. INTELL. PROP. L.J. 187, 188 (2009) (discussing recent claims by the medical device manufacturer Guidant/Boston Scientific that the actual prices its hospital customers pay for implantable devices, including cardiac pacemakers and defibrillators, are protectable as trade secrets under the Uniform Trade Secrets Act).

17. See *Consumer's Checkbook Loses Appeal in Medicare Data Case*, FINDLAW COMMON LAW (Feb. 2, 2009), <http://commonlaw.findlaw.com/2009/02/consumers-checkbook-loses->

Classic economic theory directly relates the competitiveness of a market to the degree of information available about the products and services exchanged in it. However, health care is one of many areas where intermediaries consider information gathering either a commodifiable service in itself, or an aspect of their own competitive strategy. A corporate giant like IMS Health can charge hundreds of thousands of dollars for datasets, setting up a divide between researchers who have access to critical information about, for example, pharmaceutical prescribing patterns, and those who do not. Pharmaceutical companies also push to keep exclusive access to their own data—even when serious public health concerns arise about their products.

Health policy scholars have long demonstrated how difficult it is to develop a “market” in health care.¹⁸ There is a “triple layer of agency” between care and patients whose *physicians’* recommendations are often constrained by an *insurer* which is chosen by the patient’s *employer or government*. Many other western countries have tried to address these agency problems by establishing authoritative centers to gather

appeal-in-medicare-data-case.html. On the other hand, it must be acknowledged that Medicare releases a great deal of information at low costs, which might be ten to twenty times more expensive in the hands of a company like IMS Health. See Mark Schoofs & Maurice Tamman, *In Medicare’s Data Trove, Clues to Curing Cost Crisis*, WALL ST. J., Oct. 26, 2010, at A1 (“Federal investigators use the database to find fraud; academic researchers mine it to compare the cost and utilization of various services; and consultants make a business out of analyzing the data for a wide variety of health-care companies.”); Kristin Madison, *Defragmenting Health Care Delivery Through Quality Reporting*, in THE FRAGMENTATION OF U.S. HEALTH CARE: CAUSES AND SOLUTIONS 87 (Einer Elhauge ed., 2010). I have called for more data development as a goal of health care policy in a recent essay on specialty hospitals. Frank Pasquale, *Ending the Specialty Hospital Wars: A Plea for Information-Forcing Regulatory Design*, in THE FRAGMENTATION OF U.S. HEALTH CARE: CAUSES AND SOLUTIONS, *supra* at 235.

18. Donald R. Cohodes, *Where You Stand Depends on Where You Sit: Musings on the Regulation/Competition Dialogue*, 7 J. HEALTH POL. POL’Y & L. 54, 56 (1982) (“Medical care has a number of characteristics that distinguish it from most other products . . . [1] Medical care services are not purchased from any desire for such services in themselves . . . [but instead the] demand . . . is derived from the ‘demand’ for good health. . . [2] Medical care is only one determinant of health status, and for most people at most times it is not even a very important determinant. . . [3] The need for medical care is unpredictable, requiring expenditures that are irregular and of uncertain magnitude. . . [4] The need for medical care is often immediate, allowing little time for shopping around and seeking advice or alternatives. . . [5] Consumers are usually ignorant of their medical care needs. They cannot possibly obtain the knowledge and training to diagnose their own medical care needs . . . [And 6,] [p]hysicians, though highly trained and better able to diagnose needs and prescribed treatment, also are often uncertain about the appropriate services to provide.”). FIRE industries (finance, insurance, and real estate) share some of these qualities, making whatever transparency can be provided all the more important. *But see* Omri Ben-Shahar, Frank & Bernice J. Greenberg Professor of Law, Univ. of Chicago Law Sch., Ronald H. Coase Lecture in Law & Economics: Myths of Consumer Protection: Information, Litigation, and Access (Feb. 17, 2009), <http://www.law.uchicago.edu/node/426> (arguing that disclosure fails to improve consumer decision making in a variety of fields).

information (such as the National Institute for Clinical Excellence in Britain).¹⁹

Recent U.S. moves follow these steps in some small ways.²⁰ Transparency has been on the agenda of reformers, and provisions leveraging new federal powers over private health insurers require them to release key data.²¹ The recently passed health insurance reform legislation requires each state exchange to force “health plans seeking certification as qualified health plans to submit to the Exchange . . . and make available to the public, accurate and timely disclosure” of a wide variety of important information.²² The bill responds to the demands of health policy experts like Karen Pollitz, who has repeatedly pointed out the need for “rules to ensure that insurance products are understandable and marketing practices are transparent and above board.”²³

Unfortunately, other developments in health information technology threaten to undermine policies of openness. According to Phillip Longman, the \$20 billion allocated in the American Recovery and Reinvestment Act (the “ARRA,” also known as the “stimulus”) to subsidize health information technology could be directed to proprietary systems that prevent widespread study and utilization of health records.²⁴ Longman asserts that the “largest and most successful example of digital

19. Frank Pasquale, *Rationing Health Care, British Style*, CONCURRING OPINIONS (Dec. 3, 2008, 4:14 PM), http://www.concurringopinions.com/archives/2008/12/rationing_health.html (“Britain’s National Institute for Health and Clinical Excellence (NICE) is at the cutting edge of an evidence-based movement aimed at reducing health care costs and getting value for money.”).

20. Chris Fleming, *New Health Affairs Issue: Comparative Effectiveness Research*, HEALTH AFFAIRS BLOG (Oct. 5, 2010, 7:36 AM), <http://healthaffairs.org/blog/2010/10/05/new-health-affairs-issue-comparative-effectiveness-research> (“A national push on comparative effectiveness research is under way as a result of federal stimulus and health reform legislation.”).

21. Patient Protection and Affordable Care Act § 10104(f)(2), 42 U.S.C.A. § 18031(e)(3)(A) (West 2010). This data includes “(i) Claims payment policies and practices[;] (ii) Periodic financial disclosures[;] (iii) Data on enrollment[;] (iv) Data on disenrollment[;] (v) Data on the number of claims that are denied[;] (vi) Data on rating practices[;] (vii) Information on cost-sharing and payments with respect to any out-of-network coverage[;] (viii) Information on enrollee and participant rights under this title[;] (ix) Other information as determined appropriate by the Secretary.” *Id.*

22. *Id.*

23. *Making Health Care Work for American Families: Ensuring Affordable Coverage: Hearing Before the Subcomm. On Health of the H. Comm. On Energy and Commerce*, 111th Cong. 5 (2009) (statement of Karen Pollitz, Research Professor, Georgetown University Health Policy Institute); see also Matthew Holt *Letters to Health-Care Santa: Free Our Data*, EZRA KLEIN (Dec. 23, 2009, 3:00 PM ET), http://voices.washingtonpost.com/ezra-klein/2009/12/letters_to_health-care_santa_f_1.html (“We need health care organizations to be transparent in their practices and for patients to have full access to their data as a matter of course. One little amendment in conference could get us there.”).

24. Phillip Longman, *Code Red: How Software Companies Could Screw Up Obama’s Health Care Reform*, WASH. MONTHLY, July/Aug. 2009, at 19.

medicine is an open-source program called VistA,” and contrasts it with proprietary systems “written by software developers who are far removed from the realities of practicing medicine.”²⁵ Longman worries that several proprietary systems increase the chance of medical error due to restrictive licensing agreements which prohibit users from revealing system problems.²⁶

In an increasingly polarized health policy landscape, a rare consensus has emerged around the need to deploy electronic medical records (“EMRs”). Computational innovation may improve health care by creating stores of data vastly superior to those used by traditional medical research. But before patients and providers “buy in,” they need to know that medical privacy will be respected. Counterintuitively, trade secrecy protections for companies that compile data may ultimately undermine patients’ privacy interests.

Many current discussions of EMRs erroneously conflate commercial rationales for trade secrecy with patient privacy rationales for data security. Secrecy supports “security via obscurity” strategies that can ultimately compromise both patient privacy and the types of medical research EMRs should be stimulating. For example, strong trade secrecy protections may prevent patients from even finding out about data breach-prone storage methods. If employers’ uses of EMRs cannot be scrutinized, they may be more likely to “develop complex scoring algorithms based on [EMRs] to determine which individuals are likely to be high-risk and high-cost workers.”²⁷ That use of data could shatter already fragile trust in electronic health records systems.

Data lock-ups may also create scale-driven business models that unduly tether medical research to ownership of large reservoirs of data. As Longman notes, “Electronic medical records [should] produce a large collection of digitized data that can be easily mined by managers and researchers (without their having access to the patients’ identities, which are privacy protected) to discover what drugs, procedures, and devices work and which are ineffective or even dangerous.”²⁸ Legal scholars have examined the trade-offs between data portability, standardization, privacy, and innovation in EMRs. One key to policy success in the EMR field will be distinguishing between raw data (which should be both

25. *Id.* at 21, 22.

26. *Id.* at 23. (“Perversely, license agreements usually bar users of proprietary health IT systems from reporting dangerous bugs to other health care facilities. In open-source systems, users learn from each other’s mistakes; in proprietary ones, they’re not even allowed to mention them.”).

27. Sharona Hoffman, *Employing E-Health: The Impact of Electronic Health Records on the Workplace*, 19 KAN. J.L. & PUB. POL’Y 409, 422 (2010).

28. Longman, *supra* note 24, at 23.

portable and, when properly anonymized, subject to academic research)²⁹ and its interpretation and organization (which are more justifiably considered the intellectual property of a particular firm).³⁰ EMR software vendors can exploit a combination of trade secrecy law and licensing agreements to “lock up” data in proprietary formats. If vendors of EMR systems retain excessive control over patient data, many important forms of research may be unduly limited.³¹ Scientists are already worried about this trend of closed computation in the modeling of drug trials.³² For a better sense of the dangers of such a trend, we need only examine its impact in the realm of search engines and credit scoring.

29. Marc A. Rodwin, *The Case for Public Ownership of Patient Data*, 302 JAMA 86, 88 (2009). For a good discussion of laws regarding anonymization procedures, see Barbara Evans, *Ethical and Privacy Issues in Pharmacogenomic Research*, in PHARMACOGENOMICS: APPLICATIONS TO PATIENT CARE (Howard L. McLeod et al. eds., 2d ed. 2009).

30. For the benefits of such data analysis, see David M. Eddy, *Evidence-Based Medicine: A Unified Approach*, 24 HEALTH AFF. 9, 9-17 (2005); Walter F. Stewart et al., *Bridging the Inferential Gap: The Electronic Health Record and Clinical Evidence*, 26 HEALTH AFF. W181 (2007).

31. *Id.* (“Unfortunately, billions of taxpayers’ dollars are about to be poured into expensive, inadequate proprietary software, thanks to a provision in the stimulus package. The bill offers medical facilities as much as \$64,000 per physician if they make ‘meaningful use’ of ‘certified’ health IT in the next year and a half, and punishes them with cuts to their Medicare reimbursements if they don’t do so by 2015. Obviously, doctors and health administrators are under pressure to act soon. But what is the meaning of ‘meaningful use’? And who determines which products qualify? These questions are currently the subject of bitter political wrangling. . . . Not only are [the Certification Commission for Healthcare Information Technology’s] standards notoriously lax, the group is also largely funded and staffed by the very industry whose products it is supposed to certify. Giving it the authority over the field of health IT is like letting a group controlled by Big Pharma determine which drugs are safe for the market.”). Meaningful use standards are now being developed by Health and Human Services, and preliminary indications suggest they may be responding to concerns like those expressed by Longman. See Jordan T. Cohen, *CMS and HHS Release New Proposed Rules Governing Health IT – Part 1: Overview of Proposed Rule on “Meaningful Use,”* HEALTH REFORM WATCH (Jan. 3, 2010), <http://www.healthreformwatch.com/2010/01/03/cms-and-hhs-release-new-proposed-rules-governing-health-it---part-1-overview-of-proposed-rule-on-meaningful-use>.”

32. Jennifer Kahn, *Modeling Human Drug Trials—Without the Humans*, WIRED, Dec. 2009, at 156, 157, 194 (“In early 2004 . . . the American Diabetes Association asked a physician and mathematician named David Eddy to run his own . . . trial [on atorvastatin]. He would do it, though, without human test subjects, instead using a computer model he had designed called Archimedes. The program was a kind of SimHealth: a vast compendium of medical knowledge drawn from epidemiological data, clinical trials, and physician interviews, which Eddy had laboriously translated into differential equations over the past decade. . . . Eddy’s secretive habits are . . . troubling, according to David Nathan, director of the Diabetes Center at Massachusetts General Hospital. ‘If you listen to David, he has 10,000 variables and differential equations describing everything from blood sugar to office furniture But it’s never quite clear what they are or how they interact. All the calculations happen inside a black box. And that’s a problem because there’s no way to tell whether the model’s underlying assumptions are right.’”).

II. TRADE SECRECY AS A BUSINESS TOOL IN THE SEARCH INDUSTRY

Trade secrecy law has focused on promoting “commercial ethics” in markets. One of its central goals is to avoid wasteful or unfair competition. For example, rather than triple-locking every vault or biometrically assessing the credentials of all who seek access, a trade-secret owner can bind employees, customers, and others not to misappropriate or disclose valuable processes and products. A legal entitlement to trade secrecy cuts down the costs that would be incurred by zealous pursuit of “real secrecy.”

Along with these benefits, trade secrecy has many costs.³³ Secrecy can impede incremental innovation, while the patent system’s disclosure requirements promote it.³⁴ A smaller group of scholars has addressed the negative consequences of trade secrecy for society; for example, a firm might prevent health and safety regulators from adequately investigating its practices or products by using trade secrecy protections to deflect investigations.³⁵ In the digital realm, another set of situations indicates how excess trade secrecy can undermine the public good: namely, the competitions sparked by search engine ranking.³⁶ Opaque methods of ranking and rating online entities make it difficult for those who feel

33. SUZANNE SCOTCHMER, INNOVATION AND INCENTIVES 81 (2004) (“Unlike all other forms of intellectual property, trade-secret law allows owners to suppress knowledge.”). In rare cases, copyright may do the same, given the “secure deposit” exception to copyright’s deposit requirement.

34. While widespread disclosure destroys the property value of a trade secret, it is a prerequisite for patent protection. The legitimate reasons for search engines’ general emphasis on keeping ranking algorithms confidential throw some light on the divergent rationales for adopting patent or trade secrecy protection for any given instance of intellectual property. While Google’s foundational technology in search (the PageRank method) is patented, its continual tweaking of search is usually not. Keeping the search algorithm private is the key to defeating gamers who might propagate link farms or other disfavored methods to gain salience in search results.

35. Levine, *supra* note 9, at 170-77; Mary L. Lyndon, *Information Economics and Chemical Toxicity: Designing Laws to Produce and Use Data*, 87 MICH. L. REV. 1795, 1855-56 (1989).

36. *Viacom Int’l Inc. v. YouTube Inc.*, 253 F.R.D. 256 (S.D.N.Y. 2008); Joe Nocera, *Stuck in Google’s Doghouse*, N.Y. TIMES, Sept. 13, 2008, at C1 (“In the summer of 2006 . . . Google pulled the rug out from under [web business owner Dan Savage, who had come to rely on its referrals to his page, Sourcedtool]. . . . When Mr. Savage asked Google executives what the problem was, he was told that Sourcedtool’s ‘landing page quality’ was low. Google had recently changed the algorithm for choosing advertisements for prominent positions on Google search pages, and Mr. Savage’s site had been identified as one that didn’t meet the algorithm’s new standards. . . . Although the company never told Mr. Savage what, precisely, was wrong with his landing page quality, it offered some suggestions for improvement, including running fewer AdSense ads and manually typing in the addresses and phone numbers of the 600,000 companies in his directory, even though their Web sites were just a click away. At a cost of several hundred thousand dollars, he made some of the changes Google suggested. No improvement.”).

(and quite possibly are) wronged to press their case.

Google's secrecy about its website-ranking algorithm has provoked investigations in Europe.³⁷ The *New York Times* editorial page recently called for similar scrutiny in the U.S.³⁸ The stakes are high for those who want to be found online. Search engines are referees in the millions of contests for attention that take place on the Web each day. There are dozens of entities that want to be the top result in response to a query such as "sneakers," "best Thai restaurant," or "florist." For consultants, a top or twentieth-ranked result can be the difference between lucrative gigs and obscurity.

It may seem odd to characterize search results as a competition; they are often thought of as a neutral map of the Web. However, the growing "search engine optimization" industry reveals the pressures that individuals and corporations experience as they struggle for salience in results associated with certain queries.³⁹ The primacy of dominant search engines make them *de facto* sovereigns over important swaths of social life.⁴⁰ Both government agencies and public interest groups have begun investigating the possibility that they are acting inconsistently with relevant law or their stated missions.⁴¹ But these challenges and investigations may never end conclusively given the secrecy at the core of the companies' operations.⁴²

For example, John Battelle tells the story of the owner of

37. Richard Waters, *Unrest Over Google's Secret Formula*, FIN. TIMES, July 12, 2010, at 22 ("Prompted by three complaints, the European Commission this year began an informal investigation, the first time that regulators have pried into the inner workings of the technology that lies at the heart of Google.").

38. Editorial, *The Google Algorithm*, N.Y. TIMES, July 15, 2010, at A30 ("[T]he potential impact of Google's algorithm on the Internet economy is such that it is worth exploring ways to ensure that the editorial policy guiding Google's tweaks is solely intended to improve the quality of the results and not to help Google's other businesses.").

39. Frank Pasquale, *The Troubling Trend Toward Trade Secrecy in Rankings and Ratings*, in THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH (Rochelle C. Dreyfuss & Katherine J. Strandburg, eds., forthcoming 2011).

40. DAVID STARK, THE SENSE OF DISSONANCE: ACCOUNTS OF WORTH IN ECONOMIC LIFE 1 (2009) ("Search is the watchword of the information age. Among the many new information technologies that are reshaping work and daily life, perhaps none are more empowering than the new technologies of search. . . . Whereas the steam engine, the electrical turbine, the internal combustion engine, and the jet engine propelled the industrial economy, search engines power the information economy.").

41. Waters, *supra* note 37.

42. Growing personalization also undermines efforts to understand how the algorithm works. In late 2009, Google changed its algorithms so that even users not signed in to its services would see "personalized results." As customization advances, only the search engineers know who is seeing what results. See Frank Pasquale, *The Decline of Media Studies (and Privacy) in a Search Engine Society*, CONCURRING OPINIONS (July 10, 2010, 7:11 PM), <http://www.concurringopinions.com/archives/2010/07/the-decline-of-media-studies-and-privacy-in-a-search-engine-society.html>.

2bigfeet.com (a seller of large-sized men's shoes), whose site was knocked off the first page of Google's results for terms like "big shoes" by a sudden algorithm shift in November of 2003, right before the Christmas shopping season.⁴³ Site owner Neil Moncrief attempted to contact Google several times, but said he "never got a response."⁴⁴ Google claimed that Moncrief may have hired a search engine optimizer who ran afoul of its rules but it would not say precisely what those rules were.⁴⁵ Like the IRS's unwillingness to disclose all of its "audit flags," the company did not want to permit manipulators to gain too great an understanding of how it detected their tactics. Search engine algorithms are enormously complex, and sometimes embody artificial intelligence that even their inventors have a difficult time fully understanding.⁴⁶ Such cyberdrift might be even more disturbing than deliberately manipulated results.⁴⁷

Theoretically, plaintiffs could guess at what was being done by search engines in particular cases, and subsequently algorithms could be disclosed only to a court under a protective order.⁴⁸ But even in that best-

43. JOHN BATTELLE, *THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE* 154-59 (2005).

44. *Id.* at 157.

45. *Id.*

46. The difference between explanation and understanding is key here. See Georg HENRIK VON WRIGHT, *EXPLANATION AND UNDERSTANDING* (Cornell paperbacks 2004) (distinguishing natural and human sciences); Chris Anderson, *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, WIRED, June 23, 2008, at 108-09 ("At the petabyte scale, information is not a matter of simple three- and four-dimensional taxonomy and order but of dimensionally agnostic statistics. It calls for an entirely different approach, one that requires us to lose the tether of data as something that can be visualized in its totality. It forces us to view data mathematically first and establish a context for it later. . . . Google's founding philosophy is that we don't know why this page is better than that one: If the statistics of incoming links say it is, that's good enough. No semantic or causal analysis is required. That's why Google can translate languages without actually 'knowing' them (given equal corpus data, Google can translate Klingon into Farsi as easily as it can translate French into German).").

47. Jaron Lanier, *One Half of a Manifesto*, EDGE (Sept. 25, 2000), <http://www.edge.org/documents/archive/edge74.html> ("There is a real chance that . . . the ideology of cybernetic totalist intellectuals will be amplified from novelty into a force that could cause suffering for millions of people."); JARON LANIER, *YOU ARE NOT A GADGET* 15 (2010) (article expressing concern over situations where "every element in the system—every computer, every person, every bit—comes to depend on relentlessly detailed adherence to a common standard, a common point of exchange.").

48. Protective orders may be issued in the discovery process "for good cause [in] order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." FED. R. CIV. P. 26(c)(1). Rule 26(c)(1)(G) specifies the issuance of a protective order to structure the discovery of trade secrets: orders may be issued "requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way." For a general discussion of trade secrets and protective orders, see 1 MELVIN F. JAGER, *TRADE SECRETS LAW* § 5:33 (updated in Sept. 2008).

case scenario, it is hard to imagine a court with the institutional competence to understand whether a given set of results has been manipulated. A more systematic institutional response is needed here—perhaps a trusted advisory committee within the Federal Trade Commission could help courts and agencies adjudicate coming controversies over search engine practices.⁴⁹ Qualified transparency here would promote the development of what Christopher Kelty calls a “recursive public”—one that is “vitally concerned with the material and practical maintenance and modification of the technical, legal, practical, and conceptual means of its own existence as a public.”⁵⁰

Neither markets nor common law are likely to hold search engines accountable under present circumstances. Oftentimes these intermediaries operate at the hub of multi-sided markets. For example, in a given situation where a Google user is searching for flowers nearby, Google’s search engine might block one florist for what it deems illicit “search engine manipulation” (as defined by a trade-secret-protected algorithm), but still deliver several relevant results. The searcher is unlikely ever to know of the blockage, and advertisers that benefit from increased patronage may be pleased by it. Though early search engine prototypes that rested entirely on paid ads were quickly routed by more objective sources of information, few are likely to detect or mind subtle manipulation now. Given the trend toward dynamically personalized search results, it is hard to imagine how monitoring could effectively detect untoward conduct here. The blocked florist could detect that it was blocked on its own computer, but would be unlikely to access a large enough sample of search results to prove unfair treatment.⁵¹

Reputations are created or destroyed, highlighted or obscured, by search engines. Traditional restrictions on data and information flows—be they in the form of privacy or intellectual property laws—inadequately constrain these important intermediaries. In considering the balance of power between search engines and those whom their actions affect, scholars have focused on either strengthening or weakening extant doctrines of copyright, trademark, contract, antitrust, and privacy law.

49. See *Beyond Innovation and Competition*, *supra* note 13, at 160 (proposing public and private institutions for promoting qualified transparency to enhance accountability while protecting intellectual property).

50. CHRISTOPHER M. KELTY, *TWO BITS: THE CULTURAL SIGNIFICANCE OF FREE SOFTWARE* 3 (2008).

51. As customization advances, only the search engineers know who is seeing what results. See Pasquale, *supra* note 42; but see Benjamin Edelman, *Hard-Coding Bias in Google “Algorithmic” Search Results* (Nov. 15, 2010), <http://www.benedelman.org/hardcoding> (making a case that “Google’s use of hard-coding and other adjustments to search results gives Google an important advantage in any sector that requires or benefits from substantial algorithmic search traffic,” by analyzing various Web results).

However, a critical mass of doctrine in these fields (along with established patterns of consumer behavior and the advent of cloud computing) has freed up so much information that the law needs to be concerned not only with information aggregation, but also with rankings and evaluations that flow from it. We should be troubled when trade secrecy obscures the basis of these rankings.

III. CLANDESTINELY COMMENSURATING COMPUTING IN CONSUMER CREDIT SCORING

New York Times business reporter Joe Nocera recently noted that while a “credit score is derived after an information-gathering process that is anything but rigorous,” it “has become the only thing that matters anymore to the banks and other institutions that underwrite mortgages.”⁵² Credit bureaus have also engaged in secret ranking and scoring practices that jeopardize individual reputations.⁵³ They routinely convert information into a single score purporting to assess the creditworthiness of applicants for loans. Though a credit score is computed via proprietary algorithms protected as trade secrets, it is widely treated as a fair and objective evaluation of an individual’s creditworthiness.⁵⁴ Revelation of such secrets can amount to a “taking,” requiring government compensation for disclosure mandated by regulators.⁵⁵

After the subprime debacle, the social importance of credit scoring

52. Joe Nocera, *Credit Score is the Tyrant in Lending*, N.Y. TIMES, July 24, 2010, at B1.

53. Martha Poon, *From New Deal Institutions to Capital Markets: Commercial Consumer Risk Scores and the Making of Subprime Mortgage Finance*, 34 ACCT., ORG., & SOC’Y 654, 658 (2009) (“The strength of the bureau scores as risk management aids is that they give competitive lending firms equal access to general snapshots of the consumer that are continuously recalculated as new data is amassed from participating lenders. Such scores are by no means produced from an ‘ideal’ data set. They are parasitic and pragmatic constructions that make the most of information that is readily available at the bureaus as a resource for manufacturing pre-packaged analytic products. These black-boxed statistical figures are in large part ‘behavioural scores’. They do not seek to qualify static qualities of the person so much as they constitute a temporally responsive picture of consumer risk that is useful for tracking a person’s ongoing relationship to credit.”).

54. Liz Pulliam Weston, *Eight Secret Scores That Lenders Keep*, MSN MONEY, <http://articles.moneycentral.msn.com/Banking/YourCreditRating/8SecretCreditScoresThatLendersKeep.aspx?page=all> (last updated Mar. 17, 2009) (describing “complex and largely secret scoring systems”).

55. Mandated disclosure destroys a trade secret, which can trigger obligations for compensation. Robert K. Hur, *Takings, Trade Secrets, and Tobacco: Mountain or Molehill?*, 53 STAN. L. REV. 447, 489 (2000) (“[T]he common law’s definition of trade secrets supports, and the [Supreme] Court expressly approved, the intuitively appealing picture of a trade secret’s destruction being a per se taking, regardless of the economic impact on the underlying knowledge.”).

(and its use by predatory lenders) has become more obvious than ever.⁵⁶ Nevertheless, the industry remains highly opaque, with scored individuals unable to determine the consequences of late payments, changes in location, or other decisions.⁵⁷ At least one report has alleged that credit scoring has negative, disparate impacts on minorities and low income neighborhoods.⁵⁸ Use of credit scores has been regulated by forty-eight states.⁵⁹ The National Fair Housing Alliance has criticized them for possibly “disadvantag[ing] protected classes,” arguing that the “[i]ndustry’s [l]ack of [t]ransparency [c]reates [f]air [h]ousing [c]oncerns.”⁶⁰

The scores themselves may be self-fulfilling prophecies, creating the financial distress they claim merely to indicate.⁶¹ An individual’s financial situation should determine the score, but the causation may be the reverse: the very act of designating certain persons or institutions likely failures increases the likelihood of failure. If a scorer determines that one missed \$10 payment for a woman with two children earning \$30,000 per year lowers her credit score by 200 points, she will be more likely to default because her low score means that she will be paying much more in interest for any financing she can obtain. Since the scores are black boxes, we have no assurance that scorers try to eliminate such

56. Poon, *supra* note 53, at 654 (“[O]nce modified by specific GSE interpretations the calculative properties generated by these credit bureau scores reconfigured mortgage finance into two parts: the conventional, risk-adverse, GSE conforming ‘prime’ and an infrastructurally distinct, risk-avaricious, investment grade ‘subprime.’”).

57. FRANK M. FITZGERALD, OFFICE OF FIN. & INS. SERV., THE USE OF INSURANCE CREDIT SCORING IN AUTOMOBILE AND HOME OWNERS INSURANCE 24 (2002) (discussing the “lack of adequate, detailed information that is made readily available to consumers that allows them to determine if their insurance credit score and resulting insurance premium is accurate”).

58. BIRNY BIRNBAUM, INSURER’S USE OF CREDIT SCORING FOR HOMEOWNER’S INSURANCE IN OHIO: A REPORT TO THE OHIO CIVIL RIGHTS COMMISSION 2 (2003) (“Based upon all the available information, it is our opinion that insurers’ use of insurance credit scoring for underwriting, rating, marketing and/or payment plan eligibility very likely has a disparate impact on poor and minority populations in Ohio.”).

59. NAMIC ONLINE, NAMIC’S STATE LAWS AND LEGISLATIVE TRENDS: STATE LAWS GOVERNING INSURANCE SCORING PRACTICES (2004), <http://www.namic.org/reports/credithistory/credithistory.asp>; see, e.g., HAW. REV. STAT. ANN. § 431:10C-207 (West 2010) (“No insurer shall base any standard or rating plan, in whole or in part, directly or indirectly, upon a person’s race, creed, ethnic extraction, age, sex, length of driving experience, credit bureau rating, marital status, or physical handicap.”).

60. *Future of Housing Finance: The Role of Private Mortgage Insurance Before the Subcomm. on Capital Markets, Insurance and Government Sponsored Enterprises of the H. Comm. on Fin. Servs.*, 111th Cong. 6 (2010) (testimony of Deborah Goldberg); see also BIRNBAUM, *supra* note 58, at 2 (“data and information strongly suggest insurers’ use of credit has a disparate impact on poor and minority populations”).

61. Robert Berner & Chad Terhune, *Linking Credit Scores to Hospital Care*, BUSINESSWEEK, Dec. 1, 2008, at 80.

endogeneity, or whether they profit from such self-fulfilling prophecies.

IV. FROM ENRON TO AIG: A DECADE OF UNREPRODUCIBLE FINANCIAL RESULTS

While ordinary consumers are vulnerable to unaccountable x-rays of their financial status, those at the top of the finance sector have used opaque instruments to obscure the real bases of profits and bonuses. Margaret Atwood's one-sentence description of the origins of the subprime crisis highlights how opaque financial instruments created unknown risks for investors and governments. In her Massey Lectures, the Canadian novelist wrote that "[This] scheme . . . boils down to the fact that some large financial institutions peddled mortgages to people who could not possibly pay the monthly rates and then put this snake-oil debt into cardboard boxes with impressive labels on them and sold them to institutions and hedge funds that thought they were worth something."⁶² As similar black boxes, ranging from off-balance-sheet "special purpose vehicles" to "over the counter" derivatives, continue to imperil the global economy, there will be increasing pressure for the financial industry to adopt more principles of openness.

Murky relationships between leading bankers and regulators tend to shield important transactions—and implicit governmental backing of them—from public scrutiny.⁶³ Banks that are "too big to fail" tend to engage in transactions that are too sensitive to disclose. They also amass the political leverage necessary to deflect demands for openness from regulators and journalists.⁶⁴

Many Washington regulators are swamped by information; for example, "A Senate study in 2002 found that the SEC had managed to fully review just 16 percent of the nearly 15,000 annual reports that

62. MARGARET ATWOOD, *PAYBACK: DEBT AND THE SHADOW SIDE OF WEALTH* 8 (2008).

63. See, e.g., Complaint for Declaratory & Injunctive Relief at 1, *Bloomberg L.P. v. Bd. of Governors of the Fed. Reserve Sys.*, 649 F. Supp. 2d 262 (S.D.N.Y. 2009) (No. 08 Civ. 9595) (alleging that key Fed programs "make [no] reference to any public disclosure of the posted collateral or of the Fed's methods in valuing it" with respect to key lending programs); see Greg Kaufmann, *Friedmanism at the Fed*, *THE NATION*, Mar. 15, 2010, at 18, 20 ("Despite demands from Congress and the media, neither the Fed nor AIG disclosed the names of the banks or the amount of money each had received through the bailout until March 15, 2009, when AIG finally did so.").

64. Kevin Drum, *Capital City*, *MOTHER JONES*, Jan./Feb. 2010, available at <http://motherjones.com/print/31351> (during the 2008 election cycle, "The defense lobby . . . contributed \$24 million to individuals and PACs The farm lobby? [It contributed] \$65 million. Health care [firms contributed] . . . \$167 million. And the finance lobby? They're No. 1, . . . [having] contributed an astonishing \$475 million during the 2008 election cycle."). Drum concludes that "the finance lobby is, still, simply too big to fight." *Id.*

companies submitted in the previous fiscal year; the recently disgraced Enron hadn't been reviewed in a decade."⁶⁵ Daniel Roth claims that better access to financial information would give "everyone the tools to track, analyze, and publicize financial machinations."⁶⁶ As part of such a data infrastructure, Professors Viral Acharya and Robert Engle argue that "[d]erivative [t]rades [s]hould [a]ll [b]e [t]ransparent."⁶⁷ Acharya and Engle criticized derivatives regulation for not going far enough to address these issues. The Dodd-Frank Act also fails to provide for adequate disclosure of OTC derivatives.⁶⁸

Secrecy is a troubling linchpin of contemporary finance capital, even though the size and interconnectedness of large financial institutions has increased the fragility of the credit system as a whole. Information about important transactions should be available to regulators instantly.⁶⁹ The larger a financial institution is, the more information it should be required to share about its business practices, and the faster it should be required to disclose them.⁷⁰ Real-time reporting of all transactions to

65. Daniel Roth, *Road Map for Financial Recovery: Radical Transparency Now!*, WIRED, Mar. 2009, at 80, 82.

66. *Id.* at 83.

67. Viral V. Acharya & Robert Engle, *Derivatives Trades Should All Be Transparent*, WALL ST. J., May 15, 2009, at A13 ("Most financial contracts are arrangements between two parties to deliver goods or cash in amounts and at times that depend upon uncertain future events. By their nature, they entail risk, but one kind of risk — 'counterparty risk' — can be difficult to evaluate, because the information needed to evaluate it is generally not public. Put simply, a party to a financial contract might sign a second, similar financial contract with someone else — increasing the risk that it may be unable to meet its obligations on the first contract. So the actual risk on one deal depends on what other deals are being done. But in over-the-counter (OTC) markets — in which parties trade privately with each other rather than through a centralized exchange — it is not at all transparent what other deals are being done. This makes it likely that some institutions will build up excessively large positions in OTC derivatives without the full knowledge of other market participants. If these institutions were to default, their counterparties would also incur significant losses, creating a systemic risk.").

68. Wallace C. Turberville, *Derivatives Clearing: At the End of the Beginning*, NEW DEAL 2.0 (Aug. 23, 2010, 10:57 AM), <http://www.newdeal20.org/2010/08/23/derivatives-clearing-at-the-end-of-the-beginning-18210>.

69. Real Time Public Reporting of Swap Transaction and Pricing Data, 75 Fed Reg. 76,140, 76,930 (proposed Dec. 7, 2010) (to be codified at 17 C.F.R. pt. 43) ("The Commodity Futures Trading Commission ('Commission') is proposing rules to require public reporting of certain swap transaction pricing and volume data and to establish a procedure for determining appropriate minimum sizes for block trades and large notional swap transactions.").

70. The new Office of Financial Research should promote these goals. For background on the office, see JENNIFER S. TAUB, GREAT EXPECTATIONS FOR THE OFFICE OF FINANCIAL RESEARCH 1 ("The Office of Financial Research ("OFR") is a rarely-discussed but potentially powerful agency established by the Wall Street Reform and Consumer Protection Act of 2010 ("Dodd-Frank"). Often compared to a storm-warning system, the OFR, through its two units, a Data Center and a Research and Analysis Center, can continually gather up and analyze detailed financial information collected from a variety of banks and other financial firms.").

some limited group of federal officials may well be required.⁷¹ A systemic risk regulator needs a complete and current picture of the overall level of debt, wealth, and risk in an economy.⁷²

Though the rise of the “shadow banking system” and “dark pools” may make its spread inevitable, trade secrecy appears inappropriate when a Gordian knot of gambles can put the entire global financial system at risk. As Stephen Mihm has noted, “a web of extraordinarily complex securities and wagers that has made the world’s financial system so opaque and entangled that even many experts confess that they no longer understand how it works.”⁷³ Some systemic risk regulator should be given critical information in real time.⁷⁴ Transparency would also help global regulators clamp down on the trillion dollars of funds lost each year to tax authorities in the developing world due to illicit financial flows.⁷⁵

CONCLUSION

Many current public policy battles concern the balance between

71. For a fuller exploration of “qualified transparency” in another regulatory context, see *Beyond Innovation and Competition*, *supra* note 13. The Securities and Exchange Commission has begun a program of intensified market surveillance. Press Release, Sec. and Exch. Comm’n, SEC Proposes Consolidated Audit Trail System to Better Track Market Trades (May 26, 2010) available at <http://www.sec.gov/news/press/2010/2010-86.htm> (Proposing a rule to “establish a consolidated audit trail system that would enable regulators to track information related to trading orders received and executed across the securities markets.”).

72. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, §§ 111-123, (2010) (establishing a Financial Stability Oversight Council (“FSOC”), a ten member board chaired by the Secretary of the Treasury and composed mainly of the heads of federal economic agencies). The FSOC’s purpose is “to identify risks to the financial stability of the United States that could arise from the material financial distress or failure” or large bank and non-bank financial companies. *Id.* § 112(a)(1)(A); see also SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP & AFFILIATES, *THE DODD-FRANK ACT: COMMENTARY AND INSIGHTS* 21 (2010).

73. Stephen Mihm, *The Black Box Economy*, BOSTON GLOBE, Jan. 27, 2008, at E1 (describing an “immense shadow economy of novel and poorly understood financial instruments created by hedge funds and investment banks over the past decade” as “a deep[] change in the financial system that may leave regulators, and even Congress, powerless when they try to wield their usual tools” to address economic crisis.).

74. Mike Masnick, *Garbage In ... Radical Transparency Out?*, TECHDIRT (Feb. 24, 2009, 02:34 PM), <http://www.techdirt.com/articles/20090224/0023453876.shtml> (asking “how the various quants on Wall Street got so suckered into believing their risk models that didn’t take into account the idea that mortgage defaults weren’t necessarily independent events,” and concluding that “[e]ven if people know that a computer model is ‘just a model,’ it leads to situations where they just rely on the computer because the computer said so – not taking into account its obvious faults”).

75. RAYMOND BAKER, *CAPITALISM’S ACHILLES HEEL: DIRTY MONEY AND HOW TO RENEW THE FREE MARKET SYSTEM* 23-24 (2005); see also Hilaire Avril, *Political Elites Ensure Continuing Flight of Dirty Money*, IPS (Sept. 16, 2009), <http://www.ipsnews.net/africa/nota.asp?idnews=48460> (describing a definitive study of “illicit financial flows from developing countries [estimated at] a trillion dollars a year”).

secrecy and disclosure at large corporations. The financial crisis has turned public attention to the undisclosed risks on the balance books of the largest banks and the confidential Federal Reserve interventions that kept the banking system afloat during the crisis of 2008. Secret and unfair pricing practices by hospitals and insurers pose a major challenge for the implementation of health care reform. Key intermediaries in the financial, health, and information sectors play a role in today's economy akin to that of the great trusts which originally inspired the Sherman and Clayton Acts, making or breaking the economic fates of many individuals. As novelist Adam Haslett put it, they are the "master[s] of conditions others merely suffer[]."76

Consultants frequently tell academics that they are obliged to become more "corporate" in outlook—to pay more attention to the bottom line and to develop more proprietary products and services.⁷⁷ These pressures are particularly intense in fields with immediate commercial relevance. However, certain principles of openness derived from traditional science and academic life might end up serving the long-term economic interests of American industries.⁷⁸ While the university can learn from the for-profit corporation, governments regulating intermediaries should also learn from the openness principles of universities. For example, Victoria Stodden has argued that, in the case of computational scientific research, "results should be independently replicable," otherwise, science cannot progress.⁷⁹ Similarly, sequential innovation in the private sector relies on later "improvers" being able to stand on the shoulders of earlier innovators.⁸⁰ Trade secrecy threatens to

76. ADAM HASLETT, *UNION ATLANTIC* 162 (2010).

77. JAMES C. GARLAND, *SAVING ALMA MATER: A RESCUE PLAN FOR AMERICA'S PUBLIC UNIVERSITIES* 199–200 (2009) (claiming that universities need to become more efficient and should be "deregulated," with revenues tied to "performance"); GAYE TUCHMAN, *WANNABE U: INSIDE THE CORPORATE UNIVERSITY* (2009) (observing and critiquing trends toward academic corporatization).

78. See, e.g., Victoria Stodden, *Enabling Reproducible Research: Licensing for Scientific Innovation*, INT'L J. COMM. L. & POL'Y 2, 2 (2009) ("[P]revailing scientific norms . . . provide both that results be replicated before accepted as knowledge, and that scientific understanding be built upon previous discoveries for which authorship recognition is given."). Patent law's disclosure requirement reflects such scientific standards; trade secrecy dispenses with them. See also Victoria Stodden et al., *Reproducible Research*, 12 COMPUTING SCI. & ENGINEERING 8, 8 (2010) (I was a contributing author for this proposal).

79. Stodden, *supra* note 78, at 8. As she notes in the article, the OECD's Istanbul Declaration "call[ed] for governments to make their data freely available online as a 'public good.'" *Id.* Given extensive government support for the finance and health care industries, it is appropriate for public authorities to impose openness requirements on firms in many situations as a condition for future support.

80. SCOTCHMER, *supra* note 33, at 156 ("When innovation is cumulative, an important incentive problem is to ensure that each innovator is rewarded enough to take account of the benefits conferred on future innovators. The future innovators may, in fact, be the original

nip that process in the bud, siloing innovation in search, health care, and finance into the firms best able to create authoritative data stores. There is no necessary relationship between being the best data-gatherer and finding the best interpretations and applications of that data.

Globalization accelerates competition and stratification within and among economies. A power law distribution of cultural, political, and economic inequality can only be legitimated by democracy, markets, or some combination of the two.⁸¹ Such forms of spontaneous coordination are perceived as fair because they are governed by knowable rules: a majority or plurality of votes wins, as does the highest bidder. Yet our markets, research, and life online are increasingly mediated by institutions that suffer serious transparency deficits. When a private entity grows important enough, it should be subject to transparency requirements that reflect its centrality.⁸² The increasing intertwining of governmental, business, and academic entities should provide some leverage for public-spirited appropriators and policymakers to insist on more general openness.⁸³

Laws promoting transparency have shed some light on troubling practices. However, new automated authorities are often so complex that merely revealing them will not solve the problems discussed above. Transparency should be a first step toward an *intelligible* society, where leading firms' critical decisions can be understood not merely by their own engineers and mathematicians, but also by risk managers and regulators. However well an "invisible hand" coordinates economic activity generally, markets depend on reliable information about the practices of core firms that finance, rank, and rate entities in the rest of the economy. Brandishing quasi-governmental authority to determine which enterprises are funded and found, they need to be held to a higher standard than the average firm.

innovator's rivals.").

81. For a leading attempt to provide such a justification, see YOCHAI BENKLER, *THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM* (2006). For a critique of Benkler's optimism here, see Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149 (2008).

82. The Freedom of Information Act only applies to the government, but given private companies' increasingly governmental role in today's society, it is time to consider applying some of its strictures to key private sector entities. See, e.g., Levine, *supra* note 9; ALASDAIR ROBERTS, *BLACKED OUT: GOVERNMENT SECRECY IN THE INFORMATION AGE* 158 (2006) (discussing interaction of privatization and FOIA); Craig D. Feiser, *Privatization and the Freedom of Information Act: An Analysis of Public Access to Private Entities Under Federal Law*, 52 FED. COMM. L.J. 21 (1999).

83. See, e.g., Samuel E. Trosow, *Copyright Protection for Federally Funded Research: Necessary Incentive or Double Subsidy?*, 22 CARDOZO ARTS & ENT. L.J. 613 (2004) (discussing the importance of leveraging federal subsidies to encourage openness).