UNC SCHOOL OF LAW

NORTH CAROLINA LAW REVIEW

Volume 94 | Number 1 Article 4

12-1-2015

Private Data, Public Safety: A Bounded Access Model of Disclosure

Mary D. Fan

PRIVATE DATA, PUBLIC SAFETY: A BOUNDED ACCESS MODEL OF DISCLOSURE*

MARY D. FAN**

A growing volume of crucial information for protecting public health and safety is controlled by private-sector entities. The data are private in two senses—both proprietary and secluded from scrutiny. Controversies over corporate secrecy, such as sealed settlements that hide deaths due to product defects or nondisclosure of potentially hazardous substances, illustrate how corporate privacy and public safety can conflict. Courts are conflicted about when to defer to companies' claims of the right to keep information private when important public interests are implicated by the data that companies refuse to disclose. This Article proposes allowing what it terms "bounded access" to share private data important to public health and safety with safeguards for the private interests at stake.

In contrast to mandated public-disclosure regimes, bounded access would provide information access to trained professionals capable of effectively using data to detect health and safety harms while honoring data protections. The paradigmatic audience for bounded access disclosures is researchers overseen by institutional review boards and trained in how to minimize damage to data owners. Information aggregation and de-identification can help protect the anonymity of the private entities and their product lines, thereby ameliorating the concerns of private entities regarding prematurely rousing consumer panic, injuring brand reputation, or destroying trade secrets.

Such bounded access would address the limitations of general public disclosure, such as conflict with the Fifth Amendment

** Henry M. Jackson Professor, University of Washington School of Law. Core Faculty Member, Harborview Medical Center, Injury Prevention & Research Center. This Article benefitted greatly from the insights of participants at a presentation of the paper at a conference convened by NYU School of Law and the United Nations University and at the 2015 Privacy Law Scholars Conference hosted by the UC Berkeley Center for Law & Technology. Many thanks also to Ryan Calo, Kevin Davis, Joshua A.T. Fairfield, Benedict Kingsbury, Jeremy McCabe, and Elizabeth Porter for great insights and suggestions and to B.J. Patrick Cross, Sam Fuller, and Travis Hinman for excellent editing.

takings clause or piling more disclosure on the information-overloaded consumer. Information would be rich in technical details to facilitate effective expert analyses rather than pared down for general public consumption. The proposed approach thus balances private-sector interests with the public interest in protecting population health and safety.

INTRODUCTION

Information is power to govern, protect, and defend.[1] To facilitate democratic decision making and to act as a check on power, the public can obtain information held by the government under state and federal sunshine laws.[2] Increasingly, however, a treasure trove of

1. *Cf., e.g.*, SUSAN STRANGE, THE RETREAT OF THE STATE: THE DIFFUSION OF POWER IN THE WORLD ECONOMY, at ix, 53, 100–09 (1996) (describing the relationship between information and power and how changes in methods of communication diffuse power).

2. As Justice Louis Brandeis famously wrote: "Sunlight is said to be the best of disinfectants; electric light the most efficient policeman." LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 92 (1914); *see also, e.g.*, Adriana S.

information on matters affecting public safety and security are controlled by private-sector entities rather than the government.[3] Private-sector companies are generally not subject to sunshine laws that apply to government actors.[4] Even the health and safety information that companies must report to governmental agencies can be shielded from disclosure based on claims of trade secrets, confidentiality, or proprietary information.[5] Such data are private in two senses—both proprietary and secluded from scrutiny.[6]

Corporations do not have a right to privacy, according to a longstanding rule.[7] The literature on corporate privacy is generally

Cordis & Patrick L. Warren, *Sunshine As Disinfectant: The Effect of State Freedom of Information Laws on Public Corruption*, 115 J. PUB. ECON. 18, 23–24 (2014) (discussing the impact of state sunshine laws on preventing public corruption).

3. For a discussion and numerous examples, see *infra* Section I.B.

4. *See, e.g.*, Freedom of Information Act of 1966, Pub. L. No. 89-487, 80 Stat. 250 [hereinafter FOIA] (codified as amended at 5 U.S.C. § 522 (2012)) (requiring federal agencies to maintain and disclose their records, subject to specific exemptions).

5. *See, e.g.*, 5 U.S.C. § 552(b) (2012) (providing an exemption under FOIA for "trade secrets and commercial or financial information obtained from a person and privileged or confidential"); 100 Reporters L.L.C. v. U.S. Dep't of Justice, 307 F.R.D. 269, 277 (D.D.C. 2014) ("[T]his court routinely has recognized that the submitter of documents to a government agency has a cognizable interest in maintaining the confidentiality of those documents . . . . "); Pub. Citizen v. U.S. Dep't of Health & Human Servs., 975 F. Supp. 2d 81, 91–93 (D.D.C. 2013) (allowing Pfizer to intervene to challenge disclosure of reports that the pharmaceutical company was required to submit to the Department of Health and Human Services under settlement agreements of litigation over promoting off-label uses of drugs).

6. *See, e.g.*, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1804–05 (2002) (providing three relevant definitions of "private": [1a] "intended for or restricted to the use of a particular person, group, or class <a *private* park>"; [1b] "belonging to or concerning an individual person, company, or interest <a *private* house>"; [3b] "not known or intended to be known publicly: secret").

7. Browning-Ferris Indus. of Vt., Inc. v. Kelco Disposal, Inc., 492 U.S. 257, 284 (1989) (O'Connor, J., concurring in part, dissenting in part) ("[A] corporation is 'an artificial being, invisible, intangible, and existing only in contemplation of law.' As such, it is not entitled to ' "purely personal" guarantees' whose ' "historic function" has been limited to the protection of individuals.' Thus, a corporation has no . . . right to privacy." (internal ellipses and citations omitted)); United States v. Morton Salt Co., 338 U.S. 632, 652 (1950) ("[C]orporations can claim no equality with individuals in the enjoyment of a right to privacy."); Arnold v. Pa. Dep't of Transp., 477 F.3d 105, 111 (3d Cir. 2007) ("The District Court correctly found that, as an entity, Baker 'clearly had no privacy interest' . . . ." (internal brackets omitted)); Crum & Crum Enters., Inc. v. NDC of Cal., L.P., Civ. No. 09-145 (RBK), 2011 WL 886356, at *3 (D. Del. Mar. 10, 2011) ("[B]usiness entities do not have a right to privacy."); Warner-Lambert Co. v. Execuquest Corp., 691 N.E.2d 545, 548 (Mass. 1998) ("Cases from other jurisdictions unanimously deny a right of privacy to corporations."); RESTATEMENT (SECOND) OF TORTS § 652I cmt. c (AM. LAW INST. 1977) ("A corporation as such has no right to privacy."); *cf.* RESTATEMENT OF DATA PRIVACY PRINCIPLES § 2(1)–(2) (AM. LAW INST., Preliminary Draft No. 2, Oct. 24, 2014) (focusing on privacy protections for personal information, defined as "any data that refers to an identified person" and "singl[es] out . . . a specific individual from others").

focused on the issue of whether corporations should have the right to common law or constitutional privacy.[8] In contrast, this Article illuminates how corporations enjoy plenty of privacy by other means and addresses the question of how the secrecy that shields them should be curtailed to protect the public.

Who needs the right to privacy enjoyed by ordinary natural persons, when corporations can lock up information via property, contract, and trade secret law?[9] The challenge that courts, agencies, legislatures, and citizens face is strong protection for private data that sometimes keeps secret information that is important for protecting the public.[10] Examples of ongoing controversies include claiming

8. *See, e.g.*, Anita L. Allen, *Rethinking the Rule Against Corporate Privacy Rights: Some Conceptual Quandaries for the Common Law*, 20 J. MARSHALL L. REV. 607, 626–38 (1987) (analyzing whether corporations should enjoy the protections of common law privacy torts); Elizabeth Pollman, *A Corporate Right to Privacy*, 99 MINN. L. REV. 27, 84–88 (2014) (discussing whether corporations should have a constitutional right to information privacy); Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 815–17 (2005) (discussing the nonextension of Fifth Amendment protections to businesses that receive subpoenas). By corporate privacy, this Article means protections for corporations that affirmatively shield business information from disclosure. This is different than privacy protections for consumer information that corporations must honor, or material nonpublic information that securities laws require to be disclosed. *See, e.g.*, Julie Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1929 (2013) (using the term corporate "privacy practices" to refer to how businesses use the consumer data they amass); Kenneth E. Scott, *Insider Trading: Rule 10b-5, Disclosure and Corporate Privacy*, 9 J. LEGAL STUD. 801, 817 (1980) (discussing required disclosures of material nonpublic information under the Securities and Exchange Commission's Rule 10b-5).

9. *See infra* notes 10–11 for examples and *infra* Part I for a discussion and more examples; *see also, e.g.*, KIM LANE SCHEPPELE, LEGAL SECRETS: EQUALITY AND EFFICIENCY IN THE COMMON LAW 231 (1988) ("Although corporations have been held to have no right of privacy, corporate actions in trade secrecy look very much like personal actions in privacy for public disclosure of private facts.").

10. *See, e.g.*, FED. R. CIV. P. 26(c)(1)(G) (authorizing courts to prohibit discovery of "a trade secret or other confidential research, development, or commercial information"); Tavoulareas v. Wash. Post Co., 724 F.2d 1010, 1017–23 (D.C. Cir.), *vacated on other grounds*, 737 F.2d 1170 (D.C. Cir. 1984) (en banc) (per curiam) (holding that the confidentiality of sensitive commercial information overcame the presumption of openness in discovery); Masonite Corp. v. Cty. of Mendocino Air Quality Mgmt. Dist., 49 Cal. Rptr. 2d 639, 648 (Cal. Ct. App. 1996) (holding that emissions information designated as both "emission factors" and trade secrets by manufacturing company are not subject to public release); State *ex rel.* Lucas Cty. Bd. of Comm'rs v. Ohio Envtl. Prot. Agency, 724 N.E.2d 411, 417–20 (Ohio 2000) (refusing to order disclosure by hazardous-waste landfill operator of tracking information regarding processing and emissions of potentially hazardous materials); 160 CONG. REC. S2912 (daily ed. May 12, 2014) (statement of Sen. Sheldon Whitehouse) ("While confidentiality agreements can be useful tools to protect sensitive information and trade secrets, too often they are used to hide important safety concerns from regulators, policymakers, the news media, public health experts, and the general public. Over the past 20 years, we have learned of numerous cases where court-approved secrecy has shielded serious public health and safety dangers from the public—putting hundreds, if not thousands of lives at risk. These cases have involved hydraulic

trade secret protection against disclosing potentially hazardous ingredients or emissions; creating secret settlements that hide deaths linked to auto defects; or locking up drug counterfeiting information as "proprietary data."[11]

This Article discusses when and how the robust de facto privacy that corporations enjoy should yield for public health or safety reasons. The issue is of great legal import because litigants, concerned citizens, and regulatory agencies often seek data and face a lack of information access.[12] Courts are divided over when to defer to companies' claims of the right to keep information private—even when important public interests are implicated by the data that companies refuse to disclose.[13] The question is a very timely and live

fracturing, or 'fracking,' asbestos, defective auto components, and 'adverse incidents' from drugs."); *see also infra* Part I for a discussion and more examples, including pending legislation.

11. *See, e.g.*, *State* ex rel. *Lucas Cty. Bd. of Comm'rs*, 724 N.E.2d at 417–20 (nondisclosure of emissions information); 160 CONG. REC. S2912–13 (daily ed. May 12, 2014) (statement of Sen. Sheldon Whitehouse) (discussing how secret settlements have put lives at risk); Robert Cockburn et al., *The Global Threat of Counterfeit Drugs: Why Industry and Governments Must Communicate the Dangers*, 2 PLOS MED. 0302, 0303–05 (2005) (discussing concerns over the refusal of pharmaceutical companies to release drug counterfeiting investigation information under a claim that the data is proprietary); *see also infra* Section I.B for more examples and discussion.

12. *See, e.g.*, Conn. Indem. Co. v. Superior Court, 3 P.3d 868, 874 (Cal. 2000) (discussing a claim by corporate entities that subpoenas issued by city officials investigating groundwater contamination with carcinogenic substances conflicted with their privacy interests); Cmtys. for a Better Env't v. City of Richmond, 108 Cal. Rptr. 3d 478, 490–91 (Cal. Ct. App. 2003) (discussing refusal of Chevron to show the public or decision makers proprietary data relied upon by its expert in evaluating refinery project impact); Bridgestone/Firestone, Inc. v. Superior Court, 9 Cal. Rptr. 2d 709, 715 (Cal. Ct. App. 1992) (holding that information about allegedly defective product was "potentially necessary" to plaintiffs alleging deaths due to defect but refusing to order disclosure due to claim of trade secrets); Powder River Basin Res. Council v. Wyo. Oil & Gas Conservation Comm'n, 320 P.3d 222, 234–35 (Wyo. 2014) (remanding for consideration of whether information regarding the identity of chemicals used in fracking is a trade secret not subject to disclosure); Opening Brief for Appellant General Motors Corp. at *15–16, *21, Phillips v. Gen. Motors Corp., 289 F.3d 1117 (9th Cir. 2001) (No. 01-35126), 2001 WL 34095231 (arguing that General Motors settlement information is protected by the confidentiality terms of the agreements); *cf.* Takeda Pharm., USA v. Burwell, Nos. 14-cv-1668 (KBJ), 14-cv-1850 (KBJ), 2015 WL 252806, at *18 (D.C. Cir. Jan. 13, 2015) (arguing against consideration of third-party proprietary data by the Food and Drug Administration in fulfilling its duty to review the safety and effectiveness of marketed drug products).

13. *Compare, e.g.*, *Tavoulareas*, 724 F.2d at 1017–25 (reversing the district court's decision to grant the *Washington Post*'s discovery requests to Mobil Oil Corp. on grounds that the presumption of openness of discovery materials was overcome by Mobil Oil Corp.'s privacy interests grounded in its interest in sensitive commercial information), *and Bridgestone/Firestone, Inc.*, 9 Cal. Rptr. 2d at 715 (holding that information on potentially defective tires was not subject to disclosure even though "potentially necessary" to the case of injured plaintiffs because of trade secret protections), *and State* ex rel. *Lucas Cty.*

issue for Congress as well as the courts, with legislators introducing various bills in recent years to cut back some forms of corporate secrecy that conflict with public health and safety.[14]

While there are extensive financial disclosure laws for publicly traded companies to ensure the financial wellbeing of the marketplace and protect investors,[15] there is no general law of information access to facilitate the protection of public health and safety. Because of the lack of information access, concerned citizens and watchdog groups may have to sue to attempt to access information through discovery.[16] The Supreme Court's decisions in *Ashcroft v. Iqbal*[17] and *Bell Atlantic Corp. v. Twombly*[18] have heightened civil complaint pleading standards. This barrier-raising makes it easier to dismiss cases even before discovery, thereby

Bd. of Comm'rs, 724 N.E.2d at 417–20 (holding landfill operator's data on waste generators, relative amounts of waste generated, whether certain generators' wastes failed tests more often and whether a waste generator's chemicals had to be mixed longer to be properly treated for disposal were trade secrets that may not be disclosed), *with Conn. Indem. Co.*, 3 P.3d at 874 (declining to decide whether corporations have a privacy right against disclosure of information to city officials investigating potential groundwater contamination), *and Powder River Basin Res. Council*, 320 P.3d at 235 (declining to decide whether chemical ingredients used in fracking are trade secrets not subject to disclosure).

14. *E.g.*, Sunshine in Litigation Act of 2014, S. 2364, 113th Cong. (introduced May 20, 2014) (endeavoring to prohibit courts from restricting access to information "relevant to the protection of public health or safety" by sealing such information in court records, ordering nondisclosure of such information obtained in discovery, or approving such restrictions in settlement agreements); Safety Over Secrecy Act of 2014, S. 2317, 113th Cong. (introduced May 12, 2014) (endeavoring to prohibit courts from approving confidential settlements that seal information relating to "protecting the public from a hazard to public safety or health"); Sunshine in Litigation Act of 2014, H.R. 4361, 113th Cong. (introduced Apr. 1, 2014) (prescribing protections similar to S. 2364); Sunshine in Litigation Act of 2011, H.R. 592, 112th Cong. (introduced Feb. 9, 2011) (prescribing protections similar to S. 2364); Sunshine in Litigation Act of 2010, H.R. 5419, 111th Cong. (introduced May 26, 2010) (similar); Sunshine in Litigation Act of 2009, H.R. 1508, 111th Cong. (introduced Mar. 12, 2009) (similar); Sunshine in Litigation Act of 2008, H.R. 5884, 110th Cong. (2008) (introduced Apr. 23, 2008) (similar).

15. *E.g.*, Investment Company Act of 1940, ch. 686, 54 Stat. 789 (codified as amended at 15 U.S.C. §§ 77aaa–77bbbb (2012)) (prescribing disclosure requirements for companies engaged primarily in investing and trading in securities and whose own securities are publicly offered); Securities Act of 1933, ch. 38, § 10, 48 Stat. 74, 81 (codified at 15 U.S.C. §§ 77a, 77j (2012)) (prescribing required disclosures in prospectuses to investors); Disclosure Required by Sections 406 and 407 of the Sarbanes-Oxley Act of 2002, 68 Fed. Reg. 5110 (Jan. 31, 2003) (codified as amended at 17 C.F.R. pts. 228–229, 249 (2014)) (discussing updates to financial disclosure requirements).

16. *See, e.g.*, Lonny Sheinkopf Hoffman, *Access to Information, Access to Justice: The Role of Presuit Investigatory Discovery*, 40 U. MICH. J.L. REFORM 217, 270, 278–79 (2007) (discussing the use of pretrial discovery as a way for plaintiffs to investigate and get information they need but otherwise cannot get presuit).

17. 556 U.S. 662 (2009).

18. 550 U.S. 544 (2007).

reducing the ability of even the extreme approach of lawsuits to reach corporate information.[19]

This Article proposes bounded access to address the challenge of unlocking legally shielded corporate data that directly impacts public health, safety, and security.[20] Bounded access gives professionals—who are obligated by professional ethics to honor data use and protection safeguards—the ability to view data that would otherwise be locked away.[21] The paradigmatic examples of such professionals include attorneys, who are ethically bound to comply with court orders, and researchers, who are ethically bound to comply with data protections—and are even required to have Institutional Review Board ("IRB") approval before acquiring and using sensitive data.[22] Such professionals can contribute expertise in detecting and evaluating threats to public safety, thereby serving as a check to ensure that dangers do not slip by government agencies, as well as addressing public safety issues that fall outside the domain of any regulatory agency at all.[23]

Bounded access remedies the limitations of the dominant paradigm of disclosure to an information-pummeled consumer.[24] The general concern of mandated disclosure regimes is to correct the imbalance in sophistication and information between the consumer

19. *See, e.g.*, Arthur R. Miller, *From* Conley *to* Twombly *to* Iqbal*: A Double Play on the Federal Rules of Civil Procedure*, 60 DUKE L.J. 1, 10, 17–18, 50–52 (2010) (discussing the major impact of *Iqbal* and *Twombly* in shifting the "center of gravity of federal litigation . . . forward in time[,]"making the motion to dismiss of "potentially life-or-death significance[,]" thus constituting "a continued retreat from the principles of citizen access, private enforcement of public policies, and equality of litigant treatment in favor of corporate interests and concentrated wealth"); Jonah B. Gelbach, Note, *Locking the Doors to Discovery? Assessing the Effects of* Twombly *and* Iqbal *on Access to Discovery*, 121 YALE L.J. 2270, 2325–32, 2338 (2012) (finding that *Twombly* and *Iqbal* have prevented plaintiffs in at least 21.5% of cases facing a motion to dismiss from even reaching discovery).

20. *See infra* Part III.

21. *See infra* Section III.A.

22. *See, e.g.*, Maness v. Meyers, 419 U.S. 449, 458 (1975) ("We begin with the basic proposition that all orders and judgments of courts must be complied with promptly."); Comm. on Prof'l Ethics & Conduct of the Iowa State Bar Ass'n v. McCullough, 465 N.W.2d 878, 885 (Iowa 1991) ("[A] lawyer has a duty to obey a court order and a duty not to advise a client to ignore it . . . . These principles are so obvious and basic that we should not have to remind the bar of them."); John A. Robertson, *The Law of Institutional Review Boards*, 26 UCLA L. REV. 484, 485–94 (1978) (discussing the rise of IRB requirements for researchers and their institutions).

23. *See infra* Section III.A.

24. *See, e.g.*, Richard Craswell, *Static Versus Dynamic Disclosures, and How Not To Judge Their Success or Failure*, 88 WASH. L. REV. 333, 335–39 (2013) (discussing disclosure regimes aimed at improving consumer decisions).

and the company.[25] Companies are required to inform consumers of information relevant to smart decision-making—for example, that cigarettes kill, that one has the right to inspect a house for lead-based products before buying it, or that the effective mortgage rate is actually higher than the advertised rate.[26] The information is often no secret; it is just not readily known to the humble, expertise-limited consumer.[27] And even if the information is well known to all, society may want the facts to be conspicuous to the consumer at the point of purchase.[28]

The challenge to access arises when information is made secret by contract, trade secret, or property. Courts, regulatory agencies, and disclosure laws tend to tiptoe around such claims of corporate

25. Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 705–09 (2011) (discussing the aim of correcting the information imbalance between a company and the hypothetical "Chris Consumer").

26. *See, e.g.*, ARCHON FUNG, MARY GRAHAM & DAVID WEIL, FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 183–215 (2007) (analyzing examples of eighteen disclosure regimes); Ben-Shahar & Schneider, *supra* note 25, at 653–71 (presenting numerous examples of disclosures, such as credit terms, contract boilerplate, and health, insurance, financial, and other consumer disclosures).

27. Illinois, for example, requires lenders to provide the following notice before making a high-risk home loan:

> YOU SHOULD BE AWARE THAT YOU MIGHT BE ABLE TO OBTAIN A LOAN AT A LOWER COST. YOU SHOULD SHOP AROUND AND COMPARE LOAN RATES AND FEES. LOAN RATES AND CLOSING COSTS AND FEES VARY BASED ON MANY FACTORS, INCLUDING YOUR PARTICULAR CREDIT AND FINANCIAL CIRCUMSTANCES, YOUR EMPLOYMENT HISTORY, THE LOAN-TO-VALUE REQUESTED, AND THE TYPE OF PROPERTY THAT WILL SECURE YOUR LOAN. THE LOAN RATE AND FEES COULD ALSO VARY BASED ON WHICH LENDER OR BROKER YOU SELECT. IF YOU ACCEPT THE TERMS OF THIS LOAN, THE LENDER WILL HAVE A MORTGAGE LIEN ON YOUR HOME . . . . YOU ARE NOT REQUIRED TO COMPLETE THIS LOAN AGREEMENT MERELY BECAUSE YOU HAVE RECEIVED THIS DISCLOSURE OR HAVE SIGNED A LOAN APPLICATION.

815 ILL. COMP. STAT. ANN. 137/95 (West, Westlaw through 2014 Public Act 98-1174).

28. *E.g.*, 15 U.S.C. § 1333 (2012) (requiring all cigarettes to bear one of the following disclosures: "WARNING: Cigarettes are addictive. WARNING: Tobacco smoke can harm your children. WARNING: Cigarettes cause fatal lung disease. WARNING: Cigarettes cause cancer. WARNING: Cigarettes cause strokes and heart disease. WARNING: Smoking during pregnancy can harm your baby. WARNING: Smoking can kill you. WARNING: Tobacco smoke causes fatal lung disease in nonsmokers. WARNING: Quitting smoking now greatly reduces serious risks to your health"); 15 U.S.C. §§ 1601–1667 (2012) (requiring disclosure of interest rates and fees, including the annual percentage rate, a standardized measure of the cost of obtaining credit).

information secrecy rights, carving out exemptions from disclosure requirements.[29] Moreover, in some cases, courts have found general public disclosure of health and safety information designated as trade secrets to be a taking of property without just compensation in violation of the Fifth Amendment.[30]

Instead of general disclosures to information-overloaded consumers, bounded disclosure's audience is expert professionals obligated by the ethical rules of their field to comply with protections for sensitive information.[31] Bounded access would be permitted based on a showing of both a need to detect or prevent public health, safety, or security threats and a data-use plan with safeguards for sensitive information.[32] Such protected access addresses Fifth Amendment takings claims.[33] Bounded access also reduces the risk of prohibitive resistance by companies concerned about revealing sensitive proprietary data and suffering reputational damage from premature consumer alarm.[34] Bounded disclosure thus optimizes the utility of disclosure so that the benefits are enhanced while the costs are reduced.

This Article proceeds in three parts. Part I discusses de facto corporate privacy secured through contract, property, and trade secret law, and how these protections can conflict with the need for data to address public health and safety challenges. Three contemporary controversies illustrate how the interests in private data and public safety can conflict. The first example involves claiming trade secret protection to avoid disclosure of potentially hazardous ingredients or emissions.[35] The second example is the recurring controversy over secret settlements of suits involving defects resulting in injuries or deaths.[36] The third example involves

29. *See* examples cited *supra* notes 5, 10, and *infra* Section I.B.1.

30. *E.g.*, Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1008–14 (2014); Philip Morris, Inc. v. Reilly, 312 F.3d 24, 35–47 (1st Cir. 2002) (en banc). For a discussion, see *infra* Section I.B.1.

31. *See infra* Section III.A.

32. *See infra* Part III.

33. For a discussion, see *infra* Section III.A.

34. *See, e.g.*, Kathryn M. Braeman, *Overview of FOIA Administration in Government*, 34 ADMIN. L. REV. 111, 113 (1982) (discussing the complexities of handling FOIA requests for business records submitted to agencies because the companies submitting the information "want[] the information protected at all costs" while the information-seeker "wants the information released at all costs").

35. *See infra* Section I.B.1.

36. *See infra* Section I.B.2.

the refusal of pharmaceutical companies to disclose proprietary data regarding the counterfeiting of their drugs.[37]

Part II discusses how the prevailing approach of mandated general disclosure to consumers is insufficient to address the private-data, public-safety conflict. In some cases, legislatures may face a formidable Fifth Amendment takings clause issue in mandating disclosure.[38] Additionally, companies argue that general disclosures risk prematurely alarming consumers and damaging brand reputation.[39] From the consumer's perspective, such disclosures merely pummel people already suffering from information overload with another disclosure dump.[40] Moreover, the typical general consumer is not an expert at digesting data to detect risks and formulate preventative measures, rendering disclosure an often fruitless mandate.[41]

Part III proposes the bounded model of information access to balance the public interest in access with safeguards for sensitive, protected information. Such a model allows data access by experts and motivated groups that can demonstrate good cause to pierce corporate privacy to address important public health or safety issues.[42] Rather than piling more disclosures on the bewildered, information-overloaded general consumer, bounded access is meant for specialists such as researchers or lawyers who are ethically obligated to comply with data use and protection safeguards and who are better situated to use their expertise to detect potential threats to public safety.[43] Instead of what the Article terms "thin" information, which is distilled down and rendered catchy to communicate effectively to the individual consumer, bounded access uncovers "thick information," including technical detail necessary to permit effective expert analysis.[44] Bounded access also overcomes Fifth Amendment takings claims that have bedeviled attempts to mandate public disclosure of public health, safety, and environmental information implicating trade secrets. Bounded access can thus accommodate corporate privacy without allowing it to obscure or trump the public interest in protecting population health, safety, and security.

37. *See infra* Section I.B.3.
38. *See* discussion *infra* Section I.B.1.
39. *See infra* Section II.A.
40. *See infra* Section II.B.
41. *See infra* Section II.B.
42. *See infra* Part III.
43. *See infra* Section III.A.
44. *See infra* Section III.C.

I. CORPORATE PRIVACY BY CONTRACT, PROPERTY, AND TRADE SECRET LAW

Warren and Brandeis's iconic article that launched the right to privacy discussed how contract and property law stretched and evolved to protect privacy before the formal designation of a right to privacy.[45] "Although the courts have asserted that they rested their decisions on the narrow grounds of protection to property, there are recognitions of a more liberal doctrine," wrote Justices Brandeis and Warren.[46] In groping for protections, contract law also offered an avenue: "[T]he courts, in searching for some principle upon which the publication of private letters could be enjoined, naturally came upon the ideas of a breach of confidence," stretching the principles of traditional contract law.[47]

Today, it is well settled that natural persons enjoy the right to privacy as such, without need to stretch contract and property concepts to protect private information.[48] It is often said that, in contrast to natural persons, companies do not have a right to privacy.[49] As the foundational article on the right to privacy

45. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 204–12 (1890); *see also*, Melvin B. Nimmer, *The Right of Publicity*, 19 L. & CONTEMP. PROBS. 203, 203 (1954) (discussing the influence of *The Right to Privacy* and calling the article "perhaps the most famous and certainly the most influential law review article ever written").

46. Warren & Brandeis, *supra* note 45, at 204.

47. *Id.* at 211.

48. *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 652A & cmts. a–d (AM. LAW. INST. 1977) (recognizing the right to privacy); William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 384–89 (1960) (collecting the large corpus of cases since the Warren and Brandeis privacy article that cemented the formal right to privacy as such); Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1891–95, 1903–07 (2010) (tracing the development and crystallization of privacy law).

49. *E.g.*, Browning-Ferris Indus. of Vt., Inc. v. Kelco Disposal, Inc., 492 U.S. 257, 284 (1989) (O'Connor, J., concurring in part, dissenting in part) ("[A] corporation is 'an artificial being, invisible, intangible, and existing only in contemplation of law.' As such, it is not entitled to ' "purely personal" guarantees' whose ' "historic function" . . . has been limited to the protection of individuals.' Thus, a corporation has no . . . right to privacy.") (quoting Trs. of Dartmouth Coll. v. Woodward, 17 U.S. (4 Wheat.) 518, 536 (1819) and First Nat'l Bank of Boston v. Bellotti, 435 U.S. 765, 779 n.14 (1978)); United States v. Morton Salt Co., 338 U.S. 632, 652 (1950) ("[C]orporations can claim no equality with individuals in the enjoyment of a right to privacy."); Arnold v. Pa. Dep't of Transp., 477 F.3d 105, 111 (3d Cir. 2007) ("The District Court correctly found that, as an entity, 'Baker clearly had no privacy interest.' " (internal brackets omitted)); Crum & Crum Enters. v. NDC of Cal., L.P., Civ. No. 09-145 (RBK), 2011 WL 886356, at *3 (D. Del. Mar. 10, 2011) ("[B]usiness entities do not have a right to privacy."); Warner-Lambert Co. v. Execuquest Corp., 691 N.E.2d 545, 548 (Mass. 1998) ("Cases from other jurisdictions unanimously deny a right of privacy to corporations."); RESTATEMENT (SECOND) OF

illuminated, however, we must look beyond formal designations to see how the law protects the right against disclosure of information.

In reality, companies enjoy vigorous protections against disclosure of embarrassing information. This Part begins by discussing the main legal sources of such privacy by means other than constitutional protection. The Part then illustrates the discussion with examples of contemporary clashes between this forceful de facto corporate privacy and the public interest in detecting and preventing harm.

A. Who Needs the Common Person's Privacy? Secrecy by Other Means

Notwithstanding the formal absence of a corporate right to privacy, companies seeking to keep data from being disclosed can invoke claims grounded in property and contract, including trade secret claims.[50] These protections are so strong that even the rules governing disclosure under sunshine laws or discovery in civil litigation yield to them.[51] For example, the Federal Freedom of Information Act ("FOIA") exempts from disclosure "trade secrets and commercial or financial information obtained from a person and privileged or confidential."[52] In civil litigation, Federal Rule of Civil Procedure 26(c)(1)(G) allows parties facing discovery requests to move for a protective order "to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense,

TORTS § 652I cmt. c (AM. LAW. INST. 1977) ("A corporation . . . has no personal right of privacy.").

50. *See, e.g.*, Tavoulareas v. Wash. Post Co., 724 F.2d 1010, 1029 (D.C. Cir.) (holding that Mobil Oil Corp's privacy interests in sensitive commercial information overcame the presumption of openness in discovery and defeated the *Washington Post*'s discovery requests in litigation), *vacated on other grounds*, 737 F.2d 1170, 1017–25 (D.C. Cir. 1984) (en banc) (per curiam); Bridgestone/Firestone, Inc. v. Superior Court, 9 Cal. Rptr. 2d 709, 715 (Cal. Ct. App. 1992) (holding that information on potentially defective tires was not subject to disclosure even though potentially necessary to the case of injured plaintiffs because of trade secret protections); State *ex rel.* Lucas Cty. Bd. of Comm'rs v. Ohio Envtl. Prot. Agency, 724 N.E.2d 411, 417–20 (Ohio 2000) (holding that trade secret protection precluded disclosure of city landfill operator's data on waste generators, relative amounts of waste generated, whether certain generators' wastes failed tests more often, and whether a waste generator's chemicals had to be mixed longer to be properly treated for disposal).

51. *See, e.g.*, 5 U.S.C. § 552(b) (2012) (exempting from FOIA requirements, "trade secrets and commercial or financial information obtained from a person and privileged or confidential"); FED. R. CIV. P. 26(c)(1)(G) (authorizing courts to prohibit discovery of "a trade secret or other confidential research, development, or commercial information"); MASS. R. CIV. P. 26(c) (similar); MICH. CT. R. 2.302(c)(8) (similar); PA. R. CIV. P. 4012(a)(9) (similar).

52. 5 U.S.C. § 552(b).

including . . . requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way."[53] Numerous states have identical or nearly identical provisions in their rules governing civil discovery.[54]

A trade secret is nonpublic information that is the subject of reasonable efforts to maintain its secrecy and that confers a business advantage over competitors who lack that information.[55] Such information can include formulas, processes, technical know-how, compilations of vital business information, and similar kinds of secret knowledge.[56] The aims of trade secret protection are to foster healthy competition, reduce the need for companies to pursue extensive self-help security precautions, and encourage innovation.[57]

To be a trade secret, the information need not be novel or original as with a patent or copyright, but it must be both kept secret and valuable because it is secret.[58] In contrast, the inventor of a patentable material must disclose the art—the novel idea—to gain protection because "the ultimate goal of the patent system is to bring new designs and technologies into the public domain through disclosure."[59] Unlike patents, which are time limited, trade secrets may indefinitely deprive the public of information.[60]

There is a vigorous debate over whether a trade secret is a form of property.[61] Traditionally, the central concern of trade secret protection is the breach of a confidence by revelation of a secret.[62] As

53. FED. R. CIV. P. 26(c)(1)(G).

54. *E.g.*, FLA. R. CIV. P. 1.280(c)(7); IOWA CT. R. 1.504(7); MASS R. CIV. P. 26(c); MICH. CT. R. 2.302(c)(8); MINN. R. CIV. P. 26.03(g); MISS. R. CIV. P. 26(d)(7); OHIO R. CIV. P. 26(C); OR. R. CIV. P. 36(C)(7); PA. R. CIV. P. 4012(a)(9); WASH. CT. R. 26(c)(7).

55. UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM'N 1985).

56. *Id.*; *see also, e.g.*, John C. Stedman, *Trade Secrets*, 23 OHIO ST. L.J. 4, 5–6 (1962) (listing and discussing examples and the broad swath of information that might constitute trade secrets).

57. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 485 (1974).

58. UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM'N 1985); SCHEPPELE, *supra* note 9, at 232–40.

59. Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 151–52 (1989).

60. *See, e.g.*, Andrew A. Schwartz, *The Corporate Preference for a Trade Secret*, 74 OHIO ST. L.J. 623, 648–50 (2013) (discussing how the perpetual nature of trade secrets and the lack of requirement to disclose should lead companies to prefer trade secret over patent protection).

61. *See, e.g.*, SCHEPPELE, *supra* note 9, at 240 ("A number of cases have indicated that it is breach of confidence, rather than any property theory, that underlies the decisions in these cases."); Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1, 16 (2007) ("[T]he question of whether or not trade secrets are property has raged on for many years.").

62. *See, e.g.*, DuPont de Nemours Powder Co. v. Masland, 244 U.S. 100, 102 (1917) (Holmes, J.) ("Whether the plaintiffs have any valuable secret or not the defendant knows

Justice Holmes wrote for the Supreme Court: "the starting point . . . is not property or due process of law, but that the defendant stood in confidential relations with the plaintiffs" and "fraudulently abuse[d] the trust" by disclosure of a secret.[63] Breach of confidence is a concept that draws on principles of contract, tort, and privacy rather than property.[64] Nevertheless, the Supreme Court has held that trade secrets are a form of intangible property.[65] Most states also accord trade secrets property protection.[66]

The debate over the legal heritage of trade secrets is not just academic. The issue has a practical impact in litigation. For example, Monsanto Company argued all the way to the Supreme Court that health and safety disclosures required under the Federal Insecticide, Fungicide, and Rodenticide Act[67] ("FIFRA") would reveal trade secrets and thereby constitute an unconstitutional governmental taking of property.[68] The Supreme Court agreed, ruling that the data the Environmental Protection Agency ("EPA") sought were trade secrets and a form of intangible property implicating the Fifth Amendment's protections against takings without just compensation.[69]

Regardless of whether information meets the requirements for trade secrets, companies can also create and protect confidential information by contract.[70] Two main ways to create secrecy by

the facts, whatever they are, through a special confidence that he accepted. The property may be denied but the confidence cannot be."); SCHEPPELE, *supra* note 9, at 240 ("[T]he presence of a confidential relationship can be said to be at the heart of the protection of trade secrets.").

63. *Masland*, 244 U.S. at 102.

64. *See, e.g.*, Entm't Research Grp., Inc. v. Genesis Creative Grp., Inc., 122 F.3d 1211, 1226–27 (9th Cir. 1997) (discussing the tort of breach of confidence "based upon the concept of an implied obligation or contract between the parties that confidential information will not be disclosed"); Young v. U.S. Dep't of Justice, 882 F.2d 633, 641 (2d Cir. 1989) ("[W]hile contract theories may have contributed to the development of the breach-of-confidence cause of action, it owes its existence to several doctrines, including the right to privacy.").

65. *See, e.g.*, Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1003–04 (1984) (holding that health and safety data are implicated by trade secret protections and that trade secrets are a form of intangible property).

66. *See* Philip Morris, Inc. v. Reilly, 312 F.3d 24, 31 (1st Cir. 2002) (en banc) ("In most states, trade secrets are property protected by the Takings Clause.").

67. Pub. L. No. 98-201, 97 Stat. 1379 (codified as amended at 7 U.S.C. § 136 (2012)).

68. *Ruckelshaus*, 467 U.S. at 992–93, 998–99, 1003–04.

69. *Id.* at 1004. Section I.B.1 will further delve into the complexities of *Ruckelshaus* and the Fifth Amendment implications of trade secret disclosure provisions.

70. *See, e.g.*, Peter C. Quittmeyer, *Trade Secrets and Confidential Information Under Georgia Law*, 19 GA. L. REV. 623, 624 (1985) ("Complementing trade secrets, 'confidential information' in Georgia may include almost any other business information

contract include nondisclosure agreements and settlement agreements with nondisclosure provisions.[71] The legal protection of corporate information comes through enforcement of the contract.[72] Nondisclosure contracts are often used with employees, licensees, prospective purchasers, and other companies.[73] Such agreements are more likely to be time limited because of prohibitions against unreasonable restraints of trade and employment that consider how long people are prohibited from using their know-how.[74]

In contrast, nondisclosure provisions in secret settlements with injured plaintiffs may lack any time limit.[75] One example of a confidentiality clause provides that the parties:

> [E]xpressly understand and agree that this Agreement and its contents (including, but not limited to, the fact of payment and the amounts to be paid hereunder) shall remain CONFIDENTIAL and shall not be disclosed to any third party whatsoever, except the Parties' counsel, accountants, financial advisors, tax professionals retained by them, any federal, state, or local governmental taxing or regulatory authority, and the Parties' management, officers and Board of Directors, and except as required by law or order of court. Any person identified in the preceding sentence to whom information concerning this Agreement is disclosed is bound by this

of importance, but legal protection of confidential information occurs only through enforcement of the express terms of a contractual relationship or, less frequently, the implied terms of a confidential relationship."); Linda K. Stevens, *When Should a Confidentiality Agreement Contain a Time Limit?*, 19 FRANCHISE L.J. 3, 4 (1999) (discussing how confidentiality agreements can protect information otherwise not entitled to trade secret protection).

71. Terry Morehead Dworkin & Elletta Sangrey Callahan, *Buying Silence*, 36 AM. BUS. L.J. 151, 152–53 (1998); Quittmeyer, *supra* note 70, at 665; Stevens, *supra* note 70, at 3–4.

72. Quittmeyer, *supra* note 70, at 665–66.

73. Alan E. Garfield, *Promises of Silence: Contract Law and Freedom of Speech*, 83 CORNELL L. REV. 261, 301 (1998).

74. *See, e.g.*, Thomas v. Best Mfg. Corp., 218 S.E.2d 68, 70 (Ga. 1975) (holding that a perpetual nondisclosure agreement is so broad as to be unreasonable); Gary Van Zeeland Talent, Inc. v. Sandas, 267 N.W.2d 242, 248–50 (Wis. 1978) (similar); Stevens, *supra* note 70, at 4 (advising lawyers to include a time limit in their nondisclosure agreements to avoid problems).

75. Examples of actual secret settlement confidentiality provisions are, for obvious reasons, not publicly available. However, model clauses are instructive. *See, e.g.*, LITIG. SOLS. LAW GRP., A SAMPLER OF CONFIDENTIALITY CLAUSES FOR INCLUSION IN SETTLEMENT AGREEMENTS, http://lslg.com/pdfs/A%20Sampler%20of%20Confidentiality%20Clauses_020510.pdf (last modified Feb. 2, 2010) [http://perma.cc/Q8DJ-4J9X].

> confidentiality provision and the disclosing party shall be liable for any breaches of confidentiality . . . . [76]

In securing settlements, plaintiffs face powerful pressure to accede to blanket secrecy provisions that require silence not only about the settlement terms but also the facts of the case.[77]

The current rules of discovery in litigation and by the public through sunshine laws accommodate this manufactured de facto corporate privacy.[78] Federal FOIA and most similar state sunshine laws flatly exempt "trade secrets and commercial or financial information obtained from a person and privileged or confidential[.]"[79] Notwithstanding the reference to a "person" in the provision, the exemption covers information submitted by a wide range of entities, including companies.[80] By executive order, businesses that submit information to federal agencies may claim exemption from disclosure by designating such information "confidential commercial information" and stating that "disclosure could reasonably be expected to cause substantial competitive harm."[81] When someone submits a request for such information to the government, the owner of the information is entitled to notice to defend against release.[82]

Federal Rule of Civil Procedure 26(c)(1)(G) and similar state rules are permissive in the sense that they give courts discretion to

76. JEREMY A. MERCER & EVAN A. BLOCH, SETTLEMENT AGREEMENT AND RELEASE: A U.S. EXAMPLE 4 (2012), http://www.pepperlaw.com/uploads/files/bloche_settlementagreementandrelease_ausexample_2_503_1929.pdf [http://perma.cc/R4LN-6QMU].

77. *See id.*

78. *See* discussion *supra* notes 50–54.

79. 5 U.S.C. § 552(b) (2012); *see also* DEL. CODE ANN. tit. 29, § 10002 (LEXIS through 80 Del. Laws, Ch. 193) (stating that "[t]rade secrets and commercial or financial information obtained from a person which is of a privileged or confidential nature" is not a public record subject to disclosure); OHIO ADMIN. CODE 6121-1-18(C)(4) (West, Westlaw through Sept. 30, 2015) (noting that "confidential trade secrets or other confidential material . . . are . . . not subject to disclosure to the public"); Theresa M. Costonis, Annotation, *What Constitutes Commercial or Financial Information, Exclusive of Trade Secrets, Exempt from Disclosure Under State Freedom of Information Acts—General Rules of Construction*, 5 A.L.R. 6th 327 (2005) ("Virtually all states have an information act and most have an exemption thereto applicable to commercial or financial information.").

80. *See, e.g.*, 5 U.S.C. § 551(2) (" '[P]erson' includes an individual, partnership, corporation, association, or public or private organization other than an agency."); FCC v. AT&T, 131 S. Ct. 1177, 1185 (2011) (noting that the provision "clearly applies to corporations").

81. Exec. Order No. 12,600, 3 C.F.R. 235, 236 (1987–1988).

82. *Id*. at 237–38.

issue a protective order rather than command that such orders issue.[83] The discovery rules are tilted toward preventing embarrassment by disclosure, however, by specifying that preventing "embarrassment" is a basis to grant a protective order—and *not* specifying that the need to detect and prevent threats to public health or safety is a countervailing reason *not* to grant requests.[84] As discussed in the next section, companies have successfully claimed these accommodations for corporate privacy, locking up information relevant for detecting and addressing public health and safety concerns.

B. Three Contemporary Controversies over Corporate Secrecy and Public Health and Safety

A major aim of protections against disclosure of corporate trade secrets or confidential information is to reduce the risk of "annoyance, embarrassment, oppression, or *undue* burden or expense."[85] Implicit in these goals is the reduction of unwarranted embarrassment and other costs—though not all embarrassment or other costs—that are inherent in the discovery process.[86] The challenge is determining how and where to strike the balance when the public benefit outweighs the costs and imposition upon private interests. As discussed below, controversies have flared when companies wield robust protections for corporate privacy to ward off attempts to investigate potential public health and safety concerns.

Sometimes the disclosure battle is over whether nongovernmental actors may have access to information required by law to be reported to governmental agencies.[87] Sometimes the battle

83. FED. R. CIV. P. 26(c)(1)(G) (stating courts "may, for good cause," issue such an order).

84. *Id*. (stating courts may "issue an order to protect a party or person from . . . embarrassment"). This omission contrasts with more progressive state provisions such as California Evidence Code section 1060, which provides that "the owner of a trade secret has a privilege to refuse to disclose the secret, and to prevent another from disclosing it, if the allowance of the privilege will not tend to conceal fraud or otherwise work injustice." CAL. EVID. CODE § 1060 (West, Westlaw through ch. 807 of 2015 Reg. Sess. & Ch. 1 of 2015–2016 2d Ex. Sess.).

85. FED. R. CIV. P. 26(c)(1) (emphasis added).

86. *See, e.g.*, Knoettgen v. Superior Court, 273 Cal. Rptr. 636, 638 (Cal. Ct. App. 1990) ("In all forms of discovery . . . witnesses are afforded statutory protection from *unwarranted* intrusiveness, annoyance, embarrassment, and oppression." (emphasis added)).

87. *See, e.g.*, Masonite Corp. v. Cty. of Mendocino Air Quality Mgmt. Dist., 49 Cal. Rptr. 2d 639, 648 (Cal. Ct. App. 1996) (upholding a company's objection to public disclosure of information regarding air emissions "factors" required to be reported to county air management regulators); State *ex rel.* Lucas Cty. Bd. of Comm'rs v. Ohio Envtl. Prot. Agency, 724 N.E.2d 411, 417–20 (Ohio 2000) (refusing to order public disclosure of

is over whether a corporation has to disclose such information to government regulators.[88] And sometimes the battle is over mandated disclosure directly to consumers.[89] Three contemporary controversies illustrate this clash: nondisclosure of potentially hazardous or toxic product components, secret settlements, and nondisclosure of drug counterfeiting information.

1. Privacy by Trade Secret: Hiding Potential Hazards

Companies fighting against having to disclose information about potentially hazardous ingredients, product defects, toxic emissions, and other potential public harms frequently claim that the information sought is a trade secret.[90] For example, when Bridgestone/Firestone Tire Company faced lawsuits across the country for deaths due to separating tires leading to car crashes, the company successfully used claims of trade secret to ward off attempts to obtain discovery of the rubber formula used in the tires.[91] Though the formula was relevant to the case brought by bereaved relatives and crash survivors, courts refused to allow its discovery, holding that,

data submitted by hazardous-waste landfill operator to state environmental protection agency).

88. *See, e.g.*, Ruckelshaus v. Monsanto Co., 467 U.S. 986, 998–99, 1003–04 (1984) (considering claim that disclosures required under federal law to the EPA would reveal trade secrets and violate the takings clause); Philip Morris, Inc. v. Reilly, 312 F.3d 24, 26, 28–31 (1st Cir. 2002) (en banc) (invalidating a Massachusetts law requiring disclosure of ingredient lists for all cigarette, snuff, and chewing tobacco products sold in the state and allowing for disclosure of such information whenever disclosure "could reduce risks to public health"); Jaymar-Ruby, Inc. v. FTC, 496 F. Supp. 838, 845 (N.D. Ind. 1980) (considering claim by corporation that disclosure to state law enforcement agency would constitute a Fifth Amendment taking of a trade secret).

89. *See, e.g.*, Me. Educ. Ass'n Benefits Tr. v. Cioppa, 695 F.3d 145, 149–50 (1st Cir. 2012) (considering claim by trust that a state law requiring health insurers to disclose aggregate loss information would reveal a trade secret and be an uncompensated taking in violation of the Fifth Amendment); Pharm. Care Mgmt. Ass'n v. Rowe, 429 F.3d 294, 305–06 (1st Cir. 2005) (arguing that statute mandating that pharmaceutical companies disclose to customers information regarding discounts and other contract terms requires disclosures of trade secrets and constitutes a regulatory taking without just compensation).

90. *E.g.*, *Ruckelshaus*, 467 U.S. at 1003–06; *Cioppa*, 695 F.3d at 149; *Pharm. Care Mgmt. Ass'n*, 429 F.3d at 305–06; *Philip Morris, Inc.*, 312 F.3d at 28–31; *Masonite Corp.*, 49 Cal. Rptr. 2d at 648; Bridgestone Ams. Holding, Inc. v. Mayberry, 878 N.E.2d 189, 193 (Ind. 2007); Am. Tobacco Co. v. Evans, 508 So.2d 1057, 1061 (Miss. 1987); *State* ex rel. *Lucas Cty. Bd. of Comm'rs*, 724 N.E.2d at 417–20; Crum v. Bridgestone/Firestone N. Am. Tire, LLC, 907 A.2d 578, 584 (Pa. Super. Ct. 2006); *In re* Cont'l Gen. Tire, Inc., 979 S.W.2d 609, 612 (Tex. 1998).

91. Bridgestone/Firestone, Inc. v. Superior Court, 9 Cal. Rptr. 2d 709, 715 (Cal. Ct. App. 1992); *Mayberry*, 878 N.E.2d at 196–97; *Crum*, 907 A.2d at 588. For a history of the Bridgestone Tire controversy and the pattern of deaths hidden for years while deaths continued to accumulate, see Keith Bradsher, *S.U.V. Tire Defects Were Known in '96 but Not Reported*, N.Y. TIMES, June 24, 2001, at A1.

to access the information, the plaintiffs had to meet the high burden of showing that it was necessary to prove their case.[92]

The solicitude for trade secrets was so strong that it even trumped the interest of crash survivors in the more progressive jurisdiction of California.[93] California law limits protection of trade secrets in discovery only where it "will not tend to . . . work injustice."[94] The California Court of Appeals ruled that preventing discovery of a trade secret "may not be deemed to 'work injustice' . . . simply because it would protect information generally relevant to the subject matter of an action or helpful to preparation of a case."[95] Rather, like courts in other jurisdictions, the California court required the person seeking the evidence to make a prima facie case that "the information sought is essential to a fair resolution of the lawsuit" and "necessary to the proof of, or defense against, a material element" of the cause of action.[96] Even though the accident survivors in the case submitted an expert declaration that the chemical recipe for the tire would help them determine why the tire failed, the court found this need insufficient to meet the high bar.[97] The court reasoned that the expert did not specify how the formulas were necessary for him to reach conclusions and noted that, in another case, he drew conclusions without access to formula information.[98]

Even where the law requires disclosure, companies have raised Fifth Amendment takings clause challenges against it.[99] The landmark case in this area is the Supreme Court's decision in *Ruckelshaus v. Monsanto Co.*[100] *Ruckelshaus* concerned the constitutionality of disclosures of health, safety, and environmental data submitted to the EPA by companies seeking to register pesticide products for sale.[101]

92. *Bridgestone/Firestone, Inc.*, 9 Cal. Rptr. 2d at 716; *Mayberry*, 878 N.E.2d at 196–97; *Crum*, 907 A.2d at 588.

93. *Bridgestone/Firestone, Inc.*, 9 Cal. Rptr. 2d at 715.

94. CAL. EVID. CODE § 1060 (West, Westlaw through Ch. 807 of 2015 Reg. Sess. & Ch. 1 of 2d Ex. Sess.).

95. *Bridgestone/Firestone, Inc.*, 9 Cal. Rptr. 2d at 712.

96. *Id.* at 713.

97. *Id.* at 716.

98. *Id.*

99. *E.g.*, Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1003–06 (1984); Me. Educ. Ass'n Benefits Tr. v. Cioppa, 695 F.3d 145, 148 (1st. Cir 2012); Pharm. Care Mgmt. Ass'n v. Rowe, 429 F.3d 294, 305–06 (1st Cir. 2005); Philip Morris, Inc. v. Reilly, 312 F.3d 24, 28–31 (1st Cir. 2002); *id*. at 48, 51 (Selya, J., concurring).

100. 467 U.S. 986 (1984).

101. *Ruckelshaus*, 467 U.S. at 1000–01.

To understand the complex holding of the case, it is important to understand its statutory context. The statutory regime at issue was FIFRA.[102] Before amendments in 1972, FIFRA did not have provisions regarding the authorized use and disclosure of data submitted by pesticide companies in connection with their product registrations.[103] In 1972, however, Congress amended FIFRA.[104] The 1972 amendments added a new provision governing public disclosure of data, including a provision that prohibited the EPA from publicly disclosing data that related to "trade secrets or commercial or financial information[.]"[105] Heavy litigation followed over several provisions left unclear after the 1972 amendments.[106] In 1978, Congress enacted new legislation, again amending FIFRA, including revisions to the data disclosure provisions.[107] The 1978 amendment added a new provision requiring disclosure of all health, safety, and environmental data even if the company claimed the information was a trade secret.[108]

Chemical and agricultural products company Monsanto sued, challenging the provision requiring disclosure of health, safety, and environmental data.[109] The Supreme Court ruled that a trade secret is a form of intangible property protected by the takings clause of the Fifth Amendment.[110] The more complex question was whether disclosure of the data constituted a taking.[111]

Generally, analysis of whether a taking has occurred is fact dependent and ad hoc.[112] A court examines the question of whether regulation has gone too far and become a taking in light of several factors, including "the character of the governmental action, its economic impact, and its interference with reasonable investment-

102. *Id.* at 990 (construing Pub. L. No. 98-201, 97 Stat. 1379 (codified as amended at 7 U.S.C. § 136 (2012)).

103. *Ruckelshaus*, 467 U.S. at 1008.

104. Federal Environmental Pesticide Control Act of 1972, Pub. L. No. 92-516, 86 Stat. 973 (1972).

105. *Id.* § 10(b), 86 Stat. at 989.

106. *Ruckelshaus*, 467 U.S. at 993–95.

107. Federal Pesticide Act of 1978, Pub. L. No. 95-396, 92 Stat. 819 (codified at 7 U.S.C. § 136(h)(d) (2012)).

108. *Id.* § 15(2)(d)(1) (codified at 7 U.S.C. § 136h(d) (1982)). The provision has been amended yet again and no longer allows for disclosure of health, safety, and environmental data to qualified requesters notwithstanding claims of trade secrets as it did under the 1978 amendment. *See* Federal Pesticide Act of 1978, Pub. L. No. 95-396, 92 Stat. 819 (codified at 7 U.S.C. § 136h(d) (2012)).

109. *Ruckelshaus*, 467 U.S. at 998.

110. *Id.* at 1003–04.

111. *Id.* at 1004.

112. Kaiser Aetna v. United States, 444 U.S. 164, 175 (1979).

backed expectations."[113] Thus, interference with investment-backed expectations—beyond mere impingement on a "unilateral expectation or an abstract need"—is one of several factors weighing in favor of finding a taking.[114]

Rather than examining all the factors, however, the *Ruckelshaus* Court found that just one factor—reasonable investment-backed expectations—was "so overwhelming" that it was dispositive.[115] The Court held that between 1972 and 1978, when FIFRA expressly forbade disclosure of trade secrets, Monsanto had a reasonable investment-backed expectation of nondisclosure predicated on that explicit statutory assurance.[116] Monsanto could therefore claim a taking if the EPA then publicly disclosed the information, upsetting Monsanto's expectations of continuing control and power to exclude others from knowledge of the data.[117]

In contrast, the Court ruled that after 1978, when FIFRA was amended to announce that health, safety, and environmental information was subject to public disclosure, Monsanto could have no reasonable investment-backed expectation of confidentiality.[118] While it is true that disclosure was the price of registration of a pesticide, "such restrictions are the burdens we all must bear in exchange for 'the advantage of living and doing business in a civilized community.' "[119] Even before 1972, when FIFRA was simply silent about disclosure, Monsanto had no reasonable expectation of confidentiality.[120] As a company in an industry that "long has been the focus of great public concern and significant government regulation," it was likely that the government would find disclosure to be in the public interest.[121]

While *Ruckelshaus* seemed to have struck a balance, allowing public disclosure where a regulatory law gives notice and dispels investment-backed expectations of confidentiality, the lower courts continue to wrestle with takings clause challenges to disclosure laws.[122] The First Circuit's en banc decision in *Philip Morris, Inc. v.*

113. PruneYard Shopping Ctr. v. Robins, 447 U.S. 74, 83 (1980).
114. *Ruckelshaus*, 467 U.S. at 1005–06.
115. *Id.* at 1005.
116. *Id.* at 1011.
117. *Id.*
118. *Id.* at 1006.
119. *Id.* at 1007 (quoting Andrus v. Allard, 444 U.S. 51, 67 (1979)).
120. *Id.* at 1008.
121. *Id.* at 1009.
122. *See, e.g.*, Me. Educ. Ass'n Benefits Tr. v. Cioppa, 695 F.3d 145, 148 (1st Cir. 2012); Pharm. Care Mgmt. Ass'n v. Rowe, 429 F.3d 294, 305–06 (1st Cir. 2005); Philip Morris,

Reilly[123] illustrates how strong protections for trade secrets still remain notwithstanding *Ruckelshaus*.[124] At issue in *Philip Morris* was the 1996 Massachusetts Disclosure Act, which was enacted out of concern that some tobacco product additives worsened health consequences and potentially increased nicotine delivery in cigarettes marketed as low nicotine.[125] Without knowing the identity of tobacco product additives, it was hard to investigate the adverse health consequences of product interactions or study the impact of additives popular in products marketed to younger consumers.[126] The law also aimed to publicize the ingredient lists of various brands to raise public awareness about additives and inform consumer choice.[127]

Philip Morris sued, alleging that the ingredients in tobacco products are trade secrets and that public disclosure constituted a taking without just compensation.[128] Writing for the en banc court, Judge Torruella proceeded to painstakingly analyze each of the myriad factors governing when a regulation becomes a taking rather than viewing the investment-backed expectation factor as dispositive, as the Supreme Court did in *Ruckelshaus*.[129] The decision drew on the Supreme Court's multi-factor test in *Penn Central Transportation Co. v. New York City*,[130] weighing (1) the economic impact of the regulation, (2) the interference with reasonable investment-backed expectations, and (3) the character of the governmental action.[131]

Even though there was no express promise of confidentiality in the law, and tobacco is a heavily regulated product, the *Philip Morris* court nonetheless found that the Massachusetts public health law interfered with reasonable investment-backed expectations and constituted an impermissible taking.[132] The court narrowly distinguished *Ruckelshaus*, explaining that it dealt with property interests in data already submitted to the EPA whereas Philip Morris was refusing to submit data altogether.[133] The effect of *Philip Morris* is that once a company complies with a data submission requirement

Inc. v. Reilly, 312 F.3d 24, 26, 28–31 (1st Cir. 2002) (en banc); Bridgestone Ams. Holding, Inc. v. Mayberry, 878 N.E.2d 189, 193 (Ind. 2007).

123. 312 F.3d 24 (1st Cir. 2002).
124. *Philip Morris*, 312 F.3d at 28–31, 47.
125. MASS. GEN. LAWS ch. 94, § 307B (1996); *Philip Morris*, 312 F.3d at 28.
126. *Philip Morris*, 312 F.3d at 28.
127. *Id.*
128. *Id.* at 30.
129. *Id.* at 35–47; *see* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1005 (1984).
130. 438 U.S. 104 (1978).
131. Penn Cent. Transp. Co. v. City of New York, 438 U.S. 104, 123–24 (1978).
132. *Philip Morris*, 312 F.3d at 45–46.
133. *Id.* at 38.

and gives information to the government it has less ability to challenge public disclosure, whereas a company that challenges a law at the outset and refuses to disclose data to the government has a much greater chance of prevailing.[134]

The *Philip Morris* decision swept even more broadly than just cabining *Ruckelshaus*'s reasoning regarding investment-backed expectations. In addition, the *Philip Morris* court ruled that the Disclosure Act "essentially destroys the tobacco companies' trade secrets" and rendered the economic impact of the regulation potentially dispositive.[135] Even more sweepingly, the decision indicated that legislatures seeking to protect public health through disclosure regulations must "show more than a *possible* beneficial effect."[136] The *Philip Morris* court cited less intrusive regulatory regimes and concluded that legislatures must demonstrate that proposed public health disclosure regimes "further the stated goal of promoting public health in such a way as to counterbalance the tremendous private loss involved."[137] *Philip Morris* thus illustrates that corporate privacy through trade secret protection remains vigorously alive and well in the lower courts after *Ruckelshaus*, posing a roadblock to general public disclosure statutes meant to protect health and safety.

2. Privacy by Contract: Secret Settlements

Another powerful way to hide embarrassing information of public import is through secret settlements—a recurring controversy that tends to erupt into public view belatedly, following rising victim counts.[138] A settlement is essentially a private contract with provisions enforced by courts.[139] Settlement of lawsuits for injuries due to product defects, toxic emissions, or other public health and safety issues using agreements with nondisclosure provisions essentially

134. *See id.* at 50 (Selya, J., concurring) ("After all a secret remains a secret when not divulged.").

135. *Id.* at 42 (majority opinion).

136. *Id.* at 44.

137. *Id.* at 45.

138. *See, e.g.*, Alison Lothes, Comment, *Quality, Not Quantity: An Analysis of Confidential Settlements and Litigants' Economic Incentives*, 154 U. PA. L. REV. 433, 433–35 (2005) (citing numerous examples such as the Catholic Church's sex-abuse scandal, litigation over the Ford Pinto, infertility, deaths due to use of the Dalkon Shield (an intrauterine device, or IUD) and more).

139. *See, e.g.*, Kokkonen v. Guardian Life Ins. Co. of Am., 511 U.S. 375, 381 (1994) (discussing methods to enforce contractual terms in settlement agreements).

creates corporate privacy by contract.[140] Because casualties are concealed by settlement contracts, death and injury counts may rise unchecked until the problem becomes too big to hide, erupting into national attention. A recent example is the scandal over the use of secret settlements by General Motors to conceal from the public deaths due to ignition switch defects in several models of its cars.[141]

To put the General Motors scandal into its legal and historical context, it is helpful to have a brief history of the Transportation Recall Enhancement, Accountability, and Documentation Act ("TREAD Act").[142] The TREAD Act was birthed in tragedy: the deaths of 271 people and injuries of more than 700 others in accidents involving Ford Explorer SUVs with defective Bridgestone/Firestone tires that suffered tread separation, causing the SUVs to roll over.[143] Congress acted in response to public outrage over Ford Motor Company and Bridgestone/Firestone's failure to report to the National Highway Transportation Safety Administration ("NHTSA") numerous lawsuits involving deaths or serious injuries due to

140. *Cf.* Richard A. Epstein, *The Disclosure Dilemma: Why a Ban on Secret Settlements Does More Harm than Good*, BOS. GLOBE, Nov. 3, 2002, at D4 ("Secret settlements allow both parties to get on with their lives by preserving privacy interests.").

141. Paul M. Barrett, *The GM Fiasco and Overuse of Secret Settlements: Four Blunt Points*, BLOOMBERG BUSINESSWEEK (June 25, 2014), http://www.businessweek.com/articles/2014-06-25/the-gm-fiasco-and-the-overuse-of-secret-settlements-four-blunt-points [http://perma.cc/5GQ9-9GM5] (discussing the controversy over General Motors' alleged "past policy of secretly settling lawsuits that could have brought defects to public attention years before the massive recalls of recent months"); Editorial, *Sealed Settlements Could Kill: Our View*, USA TODAY (Mar. 10, 2014, 7:56 PM), http://www.usatoday.com/story/opinion/2014/03/10/sealed-settlements-general-motors-priests-bridgestone-firestone-editorials-debates/6270853/ [http://perma.cc/WXM6-UJWP] (detailing controversy over the sealed settlement of a case alleging death due to a General Motors ignition-switch defect—nine years before the company finally issued a recall after thirteen deaths allegedly due to the defective ignition switches in Chevrolet Cobalt cars); *Rep. Nadler Introduces Bill To Stop Companies, Like GM, from Hiding Safety Flaws*, CONGRESSMAN JERROLD NADLER (Apr. 1, 2014), http://nadler.house.gov/press-release/rep-nadler-introduces-bill-stop-companies-gm-hiding-safety-flaws [hereinafter *Nadler Press Release*] [http://perma.cc/TJX8-QJ35] (discussing proposed legislation, termed the Sunshine in Litigation Act, to "prevent companies . . . from concealing evidence of wrongdoing that puts our public health and safety at risk" by using confidential settlements "to keep lifesaving information from the public").

142. *See* H.R. REP. NO. 106-954, at 6–7 (2000) (discussing background and need for legislation).

143. *See id.*; Kevin M. McDonald, *Don't TREAD on Me: Faster than a Tire Blowout, Congress Passes Wide-Sweeping Legislation that Treads on the Thirty-Five Year Old Motor Vehicle Safety Act*, 49 BUFF. L. REV. 1163, 1163, 1171–79 (2001) (detailing the controversy leading to the legislation).

defective tires and that the company had recalled its products overseas due to crash findings.[144]

Moreover, for four years, companies and plaintiffs' attorneys negotiating settlements had kept secret information about a pattern of tire failures and consumer deaths and injuries in order to negotiate a settlement.[145] It took a Houston television station's report on the deaths and serious injuries to alert the public.[146] Congressional hearings brought even more information to light, including that—contrary to the public's assumption that SUVs were safer—SUVs were actually more likely to roll over, with some models at particularly high risk.[147] Like the information about the tire-defect-related crashes, the information about which SUV models were particularly dangerous was locked away in confidential company files.[148]

The TREAD Act included detailed disclosure requirements to NHTSA in hopes of unlocking files containing important public health and safety information.[149] Vehicle manufacturers must report to the government all motor vehicle defects and all incidents of serious or fatal crashes linked to a vehicle defect for which the manufacturer has received notice.[150] The reporting requirements are intended to enable more effective government safety surveillance and timely recalls.[151] The reporting requirements are also backed by civil penalties for failure to report and criminal liability for intentional misreporting.[152]

The luster of the TREAD Act's surveillance system was damaged after revelations of NHTSA inaction despite reports of a potential ignition switch defect in Chevrolet Cobalts and Saturn Ions manufactured by General Motors.[153] The defect, which caused an engine and electrical system shut-off and disabled vehicle air bags,

144. McDonald, *supra* note 143, at 1163, 1171–79.
145. Bradsher, *supra* note 91, at A1.
146. FUNG ET AL., *supra* note 26, at 1–2.
147. *Id.* at 2.
148. *Id.*
149. *See* 49 U.S.C. § 30166(e)–(m) (2012).
150. *Id.* § 30166(m).
151. *See* McDonald, *supra* note 143, at 1185–86.
152. *See* 49 U.S.C. §§ 30165(a), 30170(a)(1) (2012).
153. MAJORITY STAFF OF H. COMM. ON ENERGY & COMMERCE, STAFF REPORT ON THE GM IGNITION SWITCH RECALL: REVIEW OF NHTSA, at 1–2 (2014), http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/OI/20140915GMFootnotes/NHTSAreportfinal.pdf [http://perma.cc/BZ2E-P3Q2] [hereinafter REVIEW OF NHTSA]; Christopher Jensen, *In G.M. Recalls, Inaction and Trail of Fatal Crashes*, N.Y. TIMES, Mar. 3, 2014, at B1.

was linked to at least 35 and allegedly as many as 153 deaths.[154] It was not until 2014 that General Motors issued a recall amid controversy over why the company and NHTSA had not acted sooner.[155]

The controversy and delay in the public being alerted also has re-ignited concern over "secret settlements" in which claimants alleging injury or death due to defects are paid in settlements placed under protective order to prevent disclosure.[156] The public outcry has prompted the reintroduction of legislation to curb settlement secrecy in cases involving issues of public health or safety.[157] The proposed legislation would forbid courts from entering protective orders or approving settlement agreements that would restrict disclosure of information "relevant to the protection of public health or safety."[158] The most recently introduced version of the bill contains an exception where "the public interest in the disclosure of past, present, or potential health or safety hazards is outweighed by a specific and substantial interest in maintaining the confidentiality of the information or records in question" and the protection "is no broader than necessary to protect the confidentiality interest asserted."[159] As Rep. Jerrold Nadler, the sponsor of one of the bills, explained, the legislation is aimed at "prevent[ing] companies . . . from concealing evidence of wrongdoing that puts our public health and safety at risk"

154. Tribune Staff, *Death Toll Rises to 35 in Faulty GM Ignition Switch Claims*, CHI. TRIB. (Nov. 24, 2014, 2:14 PM), http://www.chicagotribune.com/classified/automotive/chi-gm-ignition-switch-deaths-20141124-story.html [http://perma.cc/8FNG-AMWN]; Jensen, *supra* note 153, at B1; Ben Klayman, *Deaths Linked to GM Ignition-Switch Defect Rise to 23*, REUTERS (Sept. 29, 2014, 10:13 AM), http://www.reuters.com/article/2014/09/29/us-gm-recall-compensation-idUSKCN0HO1F220140929 [http://perma.cc/752G-4QUQ] (stating that 153 death claims had been reported).

155. REVIEW OF NHTSA, *supra* note 153, at 1–2; Jensen, *supra* note 153, at B1.

156. *See, e.g.*, Barrett, *supra* note 141 (discussing General Motors controversy); Editorial, *Secrecy that Kills*, N.Y. TIMES, June 1, 2014, at SR10 (detailing congressional investigation into the General Motors scandal).

157. Sunshine in Litigation Act of 2014, S. 2364, 113th Cong. (introduced May 20, 2014) (endeavoring to prohibit courts from restricting access to information "relevant to the protection of public health or safety" by sealing such information in court records, ordering nondisclosure of such information obtained in discovery, or approving such restrictions in settlement agreements); Safety Over Secrecy Act of 2014, S. 2317, 113th Cong. (introduced May 12, 2014) (endeavoring to prohibit courts from approving confidential settlements that seal information relating to "protecting the public from a hazard to public safety or health"); Sunshine in Litigation Act of 2014, H.R. 4361, 113th Cong. (introduced Apr. 1, 2014) (prescribing protections similar to Senate Bill 2364).

158. S. 2364 sec. 2, § 1660(a)(1); H.R. 4361 sec. 2, § 1660(a)(1); *see also* S. 2317 sec. 2, § 1660(b)(1)(A) (slightly different language).

159. S. 2364 sec. 2, § 1660(a)(1)(B).

by using confidential settlements "to keep lifesaving information from the public."[160]

While the General Motors scandal has given the settlement sunshine legislation new momentum, the legislation is likely to face the same powerful opposition that killed prior such legislation in 2008,[161] 2009,[162] 2010,[163] and 2011.[164] In 2011, similar legislation emerged from the Senate Judiciary Committee with bipartisan support—only to die under intense fire from the business community concerned about the consequences of public disclosure of such settlements.[165] Absent such legislative intervention, the creation of secrecy by contract remains unchecked.

3. Privacy by "Proprietary Data": Counterfeit Drugs

Claiming that data are "proprietary" is a third way to create corporate privacy. As a case study of this approach, consider the case of counterfeit drugs. Dubbed "medicrime" for short,[166] the social costs of counterfeiting drugs or creating poor-quality substitutes go beyond intellectual property offenses. People have died after ingesting contaminated counterfeit medicines or from taking what they thought were prophylactic or treatment drugs that were actually fakes, leaving them unprotected or untreated.[167] Hospitalization and deaths have

160. *Nadler Press Release*, *supra* note 141.

161. Sunshine in Litigation Act of 2008, H.R. 5884, 110th Cong. (introduced Apr. 23, 2008).

162. Sunshine in Litigation Act of 2009, H.R. 1508, 111th Cong. (introduced Mar. 12, 2009).

163. Sunshine in Litigation Act of 2010, H.R. 5419, 111th Cong. (introduced May 26, 2010).

164. Sunshine in Litigation Act of 2011, H.R. 592, 112th Cong. (introduced Feb. 9, 2011).

165. *See* Barrett, *supra* note 141.

166. *See* Council of Europe, Convention on the Counterfeiting of Medical Products and Similar Crimes Involving Threats to Public Health, *opened for signature* Oct. 28, 2011, C.E.T.S. No. 211 [hereinafter MEDICRIME Convention] (calling for signatories to criminalize drug counterfeiting and related public health crimes).

167. *See, e.g.*, Kristina M. Lybecker, *Rx Roulette: Combatting Counterfeit Pharmaceuticals in Developing Nations*, 28 MANAGERIAL & DECISION ECON. 509, 510 (2007) (summarizing infamous cases, such as the deaths of more than 2,500 people vaccinated with counterfeit anti-meningitis drugs during a meningitis outbreak); Paul N. Newton et al., *Manslaughter by Fake Artesunate in Asia—Will Africa Be Next?*, 3 PLOS MED. e197, 0752–55 (2006) (discussing problems with counterfeit anti-malarial drugs plaguing Asia and a case of a death due to treatment with counterfeit drugs); Rachel Ehrenberg, *Counterfeit Crackdown: New Scientific Tools Help Tell Fake Meds from the Real Thing*, SCI. NEWS, June 18, 2011, at 22–24 (discussing how more than fifty Nigerian children died after taking contaminated counterfeit teething medicine and the death of a twenty-two-year-old Argentinian woman after receiving an injection of counterfeit iron); Lindsay Kines, *Counterfeit Pills Kill B.C. Woman; Internet Site Linked to Death: Coroner*,

even ensued from seemingly less serious counterfeiting of pleasure-enhancing drugs taken for erectile dysfunction, such as Cialis.[168]

Because law enforcement resources to combat the spread of counterfeit medicines are stretched thin or missing in the areas of greatest risk, private actors, particularly major drug companies, play critical investigative and enforcement roles.[169] Pharmaceutical companies use private investigators to detect and try to shut down counterfeiting enterprises.[170] Recognizing the need to have the expertise of major drug companies in investigating and securing prosecution of counterfeiters, the World Health Organization ("WHO") even gave large pharmaceutical companies seats on its International Medical Products Anti-Counterfeiting Task Force, the largest anti-counterfeiting working group, despite outcry from smaller generic manufacturers.[171] In addition, the security departments of twenty-five major pharmaceutical companies run the nonprofit Pharmaceutical Security Institute and its private, secure database containing member reports of fake drugs and packaging.[172]

The pharmaceutical companies view the database as proprietary and confidential and do not release the information to researchers—and perhaps not even to the WHO or other intergovernmental or governmental organizations.[173] Without access to the databases, researchers are unable to identify and study drugs vulnerable to counterfeiting. While private companies certainly have an interest in shutting down entities they view as counterfeiters, this is counterbalanced against their interest in keeping matters quiet so that the public is not alerted and does not lose trust in the brand.[174] The

EDMONTON J., July 6, 2007, at A5 (reporting on the death of a fifty-eight-year-old woman who died from a toxic overload of metals after ingesting counterfeit pills she bought online).

168. Neil Campbell et al., *Internet-Ordered Viagra (Sildenal Citrate) Is Rarely Genuine*, 9 J. SEXUAL MED. 2943, 2947 (2012) (discussing findings regarding counterfeit Viagra); Shih Ling Kao et al., Letter to the Editor, *An Unusual Outbreak of Hypoglycemia*, 360 NEW ENG. J. MED. 734, 734–35 (2009).

169. INST. OF MED., COUNTERING THE PROBLEM OF FALSIFIED AND SUBSTANDARD DRUGS 16 (Gilliam J. Buckley & Lawrence O. Gostin eds., 2013); Cockburn et al., *supra* note 11, at 0303.

170. Cockburn et al., *supra* note 11, at 0303.

171. *See* INST. OF MED., *supra* note 169, at 16.

172. *Id.* at 86–87.

173. Cockburn et al., *supra* note 11, at 0303–05. Cockburn et al. questioned the database keepers about release of information to the WHO and governmental authorities but did not receive a direct answer beyond a reiteration that the information is proprietary and confidential. *Id*.

174. *Id.* at 0303.

secrecy impedes the ability to conduct independent checks and scrutiny.

Concern over the adulteration of medicines has existed as long as medicinal use.[175] Harmful medicines exist because of a range of misconduct, from passing off a drug as made by another manufacturer, to adulterating medicines, to a combination of these misbehaviors or otherwise producing substandard drugs.[176] One common distinction in usage today is between counterfeit drugs—referring to drugs falsified as to source, identity, or both—and substandard drugs that fail to meet specifications, for example, by having the wrong concentration of active ingredients.[177] The problem is intensifying in modern times, however, because of the ease of mass manufacturing knock-offs, globalization of supply chains, and the rise of Internet pharmacies.[178]

While the regions hardest hit by the use problems also tend to be in developing parts of the world, the problem is not just a poor-country or developing-world issue.[179] With the rise of global trade, Internet pharmacies, and the lucrative nature of producing fake or substandard drugs for sale, officials in countries like the United States, Canada, Britain, and other European Union nations are expressing concern.[180] Counterfeit Viagra, Ritalin, antibiotics, and other drugs have been in circulation in the United States.[181]

175. WORLD HEALTH ORG., COUNTERFEIT DRUGS: GUIDELINES FOR THE DEVELOPMENT OF MEASURES TO COMBAT COUNTERFEIT DRUGS 11 (1999).

176. INST. OF MED., *supra* note 169, at 1–2 (noting the problem is "vastly aggravated by modern manufacturing and trade" and international supply chains). WORLD HEALTH ORG., *supra* note 175, at 11.

177. *See, e.g.*, J.-M. Caudron et al., *Substandard Medicines in Resource-Poor Settings: A Problem that Can No Longer Be Ignored*, 13 TROPICAL MED. & INT'L HEALTH 1062, 1063 (2008) (using the distinction).

178. *See, e.g.*, INST. OF MED., *supra* note 169, at 1–2 (noting the problem is "vastly aggravated by modern manufacturing and trade" and international supply chains); WORLD HEALTH ORG., *supra* note 175, at 11 (discussing the fertile environment for counterfeiting due to "[n]ew global trade arrangements, free trade agreements and deregulation" as well as "inequitable income and wealth distribution, and variable social and economic development"); Marilynn Larkin, *Combating Counterfeit Drugs Online*, 6 LANCET INFECTIOUS DISEASE 552, 552 (2006) (responding to concerns that the "Internet has become 'the primary tool for criminal organizations to advertise, communicate and conduct sales of counterfeit pharmaceuticals' " with a compendium of anti-counterfeiting online resources).

179. G. Jackson, S. Patel & S. Khan, *Assessing the Problem of Counterfeit Medications in the United Kingdom*, 66 INT'L J. CLINICAL PRAC. 241, 242–43 (2011).

180. *See, e.g.*, *id.* (reporting on concerns in the United Kingdom, European Union, and United States); Mark Townsend, *Health Fears Grow as Fake Drugs Flood Britain*, GUARDIAN: OBSERVER (U.K.) (Jan. 3, 2009), http://www.theguardian.com/business/2009/jan/04/fake-pharmaceuticals-drugs-china-nhs [http://perma.cc/8QLB-5ZJ6] (reporting on

Alarmed that criminal enterprises are sending bad medicines across borders into Europe, the Council of Europe drafted the first international treaty on counterfeit medicines and related crimes—dubbed the "MEDICRIME Convention"—which opened for signature in October 2011.[182] The Convention requires signatories to criminalize manufacturing, supplying, or trafficking in counterfeit medicines and to share data for law enforcement purposes.[183] There are forty-seven European nations represented by the Council of Europe.[184] In addition, in 2010, the Ministers of the Council of Europe asked that the Convention be circulated widely with an invitation to nonmember states to join.[185] To date, however, only nineteen nations have signed the Convention.[186]

While prominent stories about and seizures of counterfeit drugs may rouse periodic attention, sustained attention and research is difficult because of the scarcity of data on the issue.[187] Data on the scope of the problem are difficult to obtain because of the covert nature of the illicit industry and severe underreporting, particularly in the hardest-hit regions of the world.[188] Making matters worse, medicines are taken by the ill, elderly, and infirm.[189] Even when people sicken or die because of taking counterfeit or substandard drugs, they may not realize it is because of the drug rather than the illness.[190] As Valerio Reggi, coordinator of the WHO anti-

counterfeit pills "made in China, labelled in French, and then shipped to Singapore" where they "ended up in Liverpool and from there were sold straight into the heart of the National Health System, Britain's healthcare provider system").

181. *See, e.g.*, *Buyer Beware: The Danger of Purchasing Pharmaceuticals Over the Internet: Hearing Before the Permanent Subcomm. on Investigations*, 108th Cong. 2–3 (2004) (discussing dangers of drugs illegally sold by online pharmacies and deaths due to such drugs); Campbell et al., *supra* note 168, at 2943–49 (discussing findings regarding counterfeit Viagra); Gardiner Harris, *Medicines Made in India Set Off Safety Worries*, N.Y. TIMES, Feb. 15, 2014, at A1 (discussing concerns over entry of counterfeit drugs into U.S. supply chain); *FDA Warns Bogus Pills Contain Viagra, Cialis Drugs*, FOXNEWS.COM (May 13, 2011), http://www.foxnews.com/us/2011/05/13/fda-warns-bogus-pills-contain-viagra-cialis-drugs [http://perma.cc/3EZR-PXKB].

182. MEDICRIME Convention, *supra* note 166.

183. *Id.* at arts. 5–6, 11–12, 16–17.

184. *The Medicrime Convention*, COUNCIL EUR., https://www.edqm.eu/en/the-medicrime-convention-1470.html [http://perma.cc/BXT7-GG23].

185. *Id.*

186. *Id.*

187. *See, e.g.,* Paul N. Newton et al., *Counterfeit Anti-Infective Drugs*, 6 LANCET INFECTIOUS DISEASE 602, 602, 610 (2006) (noting the problem is "under-recognised[,]" research in the area is limited, and there are data availability challenges).

188. *See* INST. OF MED., *supra* note 169, at 85–128 (describing the data available about medicine quality and the limitations of that data); Cockburn et al., *supra* note 11, at 0303.

189. INST. OF MED., *supra* note 169, at 15.

190. *Id.*

counterfeiting taskforce explained, "It's difficult to link a dead body to a counterfeit drug bought at a street market."[191] Because of the difficulty in measuring the trade in false pharmaceuticals and linking deaths and illnesses to fake drugs, the Institute of Medicine recently concluded: "Deaths from fake drugs go largely uncounted, to say nothing of the excess morbidity and the time and money wasted by using them."[192]

Despite the difficulty in obtaining data, there have been attempts to estimate the prevalence of counterfeit medicine; unsurprisingly, these numbers vary widely because of the data deficit. Estimates indicate that from 10% to over 50% of medicines in some parts of the developing world are counterfeit.[193] Though the WHO estimated in 2006 that the prevalence in upper-income countries like the United States, Canada, and members of the European Union is less than 1% of the drug supply,[194] there are indications that sales of counterfeit medicines may be growing because of the rise of Internet pharmacies and other gray and black markets.[195] Because of the scarcity of studies on prevalence, many of the estimates of the magnitude of the problem have relied on "gray literature" such as media reports of cases that have surfaced or litigation documents.[196]

Field surveys that systematically and randomly sample and test medicines from a representative cross section of a region's or a country's markets offer the best estimates of the scope of the drug-supply problem.[197] Such field surveys are difficult and potentially prohibitively expensive to undertake, however, particularly in the hardest-hit low- and middle-income nations with a large, heterogeneous pool of gray markets.[198] Only recently have attempts

191. Makiko Kitamura, *West African Leaders Not Doing Enough To Stop Fake Drugs: WHO*, AGENCE FRANCE PRESSE, Oct. 13, 2006, Westlaw (no unique identifier).

192. INST. OF MED., *supra* note 169, at 16.

193. JULIAN MORRIS & PHILLIP STEVENS, COUNTERFEIT MEDICINES IN LESS-DEVELOPED COUNTRIES: PROBLEMS AND SOLUTIONS 3–4 (2006); Cockburn et al., *supra* note 11, at 0303; Paul N. Newton, Michael D. Green & Facundo N. Fernández, *Impact of Poor-Quality Medicines in the 'Developing' World*, 31 TRENDS PHARMACOLOGICAL SCIS. 99, 99–100 (2010).

194. WORLD HEALTH ORG., COUNTERFEIT MEDICINES: AN UPDATE ON ESTIMATES (Nov. 15, 2006), http://www.who.int/medicines/services/counterfeit/impact/TheNewEstimatesCounterfeit.pdf [http://perma.cc/SN2W-EAPC].

195. Facundo M. Fernández, Michael D. Green & Paul N. Newton, *Prevalence and Detection of Counterfeit Pharmaceuticals: A Mini Review*, 47 INDUS. & ENGINEERING CHEMICAL RES. 585, 585 (2008); Jackson et al., *supra* note 179, at 242–43; WORLD HEALTH ORG., *supra* note 194.

196. INST. OF MED., *supra* note 169, at 85, 94.

197. *Id.* at 102–03.

198. *See id.* at 103.

been made to systematically quantify the prevalence of counterfeit drugs. In 2011, the Promoting the Quality of Medicines program, funded by the U.S. Agency for International Development launched its Medicines Quality Database ("MQDB").[199] Overseen by the U.S. Pharmacopeial Convention, the database is a valuable development because it allows access to data from participating countries on samples of medicines tested pursuant to standardized guidelines to enhance quality, validity, reliability, and comparability of the data obtained.[200] There are currently twelve participating countries, contributing more than 12,500 records of drug tests in total.[201] The four longest-participating countries are Cambodia,[202] Laos,[203] Vietnam,[204] and Thailand.[205] While a promising start, the coverage remains limited. Private partners are important in expanding the web of surveillance—but effective surveillance is stymied by the veil of secrecy surrounding counterfeiting information uncovered by companies with the resources and expertise to investigate.[206]

II. WHY A CONSUMER-ORIENTED GENERAL DISCLOSURE MODEL IS NOT ENOUGH

While corporate secrecy that stifles public protection is a problem, general public disclosure is not a feasible cure in the sensitive contexts where companies claim rights to corporate privacy secured by trade secret, contract, or property law.[207] As discussed in Part I, some courts have held that general disclosure of protected

199. *Medicines Quality Database (MQDB)*, U.S. PHARMACOPEIAL CONVENTION, http://www.usp.org/global-health-impact-programs/promoting-quality-medicines-pqmusaid/medicines-quality-database-mqdb [http://perma.cc/WS5A-AWZ5].

200. Laura A. Krech et al., *The Medicines Quality Database: A Free Public Resource*, 92 BULL. WORLD HEALTH ORG. 2 (2014), http://www.scielosp.org/pdf/bwho/v92n1/0042-9686-bwho-92-01-02.pdf [http://perma.cc/B522-AP3C].

201. Cambodia, Colombia, Ecuador, Ghana, Guyana, Kenya, the Lao People's Democratic Republic, Mozambique, Peru, the Philippines, Thailand, and Vietnam all participate in the MQDB. The MQDB's annual Quick Reports include data for each of these listed countries. *See Medicines Quality Database (MQDB)*, U.S. PHARMACOPEIAL CONVENTION, http://www.usp.org/global-health-programs/promoting-quality-medicines-pqmusaid/medicines-quality-database-mqdb (click "Access the MQDB"; agree to the terms of use; select "Quick Report," select a country from the list; click "next"; select a year; click "next" to view results).

202. Data available for nine years, for 2003 and from 2005–2012. *See id.*

203. Data available for eight years, from 2003–2011. *See id.*

204. Data available for nine years, from 2003–2011. *See id.*

205. Data available for four years, from 2004–2005 and 2008–2009. *See id.* Guyana also contributed four years, but the span was narrower, ranging from 2008 to 2011. *See id.*

206. Cockburn et al., *supra* note 11, at 0303.

207. *See* discussion and examples *supra* Part I.

trade secrets—even to protect public health and safety—is an unconstitutional taking of property without compensation in violation of the Fifth Amendment.[208] Secret settlement agreements have been routinely sanctioned by courts despite recurring controversy and repeated congressional efforts to prohibit judicial sanction of contracts preventing disclosure of information important to public health and safety.[209]

Moreover, even where general disclosure might be an option, it may not be the most effective way when balancing the costs of disclosure with the benefits. This Part begins by discussing the ascendant consumer-oriented approach to disclosure. The Part then turns to why piling more disclosures on information-overloaded, nonexpert consumers is not the most effective solution for the private-data, public-safety conflict.

A. Consumer, Protect Thyself

In numerous contexts, from wastewater contamination to financial disclosure laws, legislatures have enacted targeted transparency regimes with disclosure as a centerpiece of efforts to enable better protection.[210] Two major aims of disclosure as a tool to protect public health and safety include enabling informed consumer choice and allowing consumers to self-protect to prevent harm.[211] A major assumption and goal of mandatory disclosure is a better-informed individual decision maker, who Omri Ben-Shahar and Carl E. Schneider dub "Chris Consumer."[212]

Mandated disclosure works well for Chris Consumer when information is stripped down and rendered into an accessible

208. *See* discussion *supra* Section I.B.1.

209. *See* discussion *supra* Section I.B.2.

210. *See, e.g.*, Safe Drinking Water Act Amendments of 1996, Pub. L. No. 104-182, 110 Stat. 1613 (codified as amended in scattered sections of the U.S. Code); INT'L FED'N OF ACCOUNTANTS (IFAC), INTERNATIONAL FINANCIAL REPORTING STANDARDS (IFRS): AN AICPA BACKGROUNDER 2–3, 5–8 (2011), http://www.ifrs.com/pdf/ifrsupdate_v8.pdf [http://perma.cc/Q74D-GXTC] (providing an accessible overview of International Financial Reporting Standards and their convergence and adoption history); FUNG ET AL., *supra* note 26, at 7–9, 12–13, 21–23, 92–105, 133–40 (offering numerous examples of mandated disclosure including a discussion of water contamination disclosures as an example of the pitfalls of complex disclosures to consumers and international corporate financial reporting disclosure requirements as an example of a successful regime); Cass R. Sunstein, *Information Regulation and Informational Standing:* Akins *and Beyond*, 147 U. PA. L. REV. 613, 613–14, 618–25 (1999) (discussing the rise of information dissemination requirements as a regulatory tool and offering numerous examples).

211. *See* discussion and examples *infra* notes 214–22.

212. Ben-Shahar & Schneider, *supra* note 25, at 705–10.

decisional heuristic.[213] An excellent example is the TREAD Act's savvy strategy of giving consumers digestible vehicle roll-over safety information through a five-star rating system based on government crash tests.[214] The five-star crash rating system enables consumers to exercise better-informed choice, rendering complex government crash-test results an accessible decisional heuristic.[215] Such disclosure effectively enables informed consumption in light of known public health and safety information with technical details removed.

Mandated disclosure is also used to facilitate consumer self-protection. Data breach notification laws are an example. The laws generally require businesses and governmental entities holding personally identifiable information, such as account or credit card numbers, to notify individuals when there is a breach involving unauthorized access to such information.[216] The aim of data breach disclosure laws is to alert individuals so they can self-protect and minimize damage from crimes such as identity theft.[217]

A thicket of data breach notification laws has rapidly grown and spread since California enacted the nation's first data breach disclosure law in 2002.[218] Today, forty-seven states, the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands all have

213. M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1030–47 (2012).

214. *See, e.g.*, FUNG ET AL., *supra* note 26, at 2 (counting the TREAD Act as a success giving "[i]nformation . . . new power because policymakers did not stop at simply placing facts about risks in the public domain—where they could be easily lost in the cacophony of new-car hype" but instead "required that information be presented in a format that was designed to be user-centered" through a "simple five-star ratings [system] based on government tests of each new model").

215. NHTSA Final Policy Statement on Consumer Information; New Car Assessment Program; Rollover Resistance, 68 Fed. Reg. 59,250, 59,250 (Oct. 14, 2003) (to be codified at 49 C.F.R. pt. 575).

216. For a list of legislation, see *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Oct. 22, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [http://perma.cc/4687-SZL2] (listing state data breach notification laws).

217. *See, e.g.*, Cal. S.B. No. 1386, § 1 (2002) (enacted) (explaining the law's aim to ensure timely notification to potential victims of identity theft so that individuals can "act quickly to minimize the damage"); Council Directive 2009/136, art. 59, 2009 O.J. (L 337) 11, 19 (EC) ("[T]he notification of security breaches reflects the general interest of citizens in being informed of security failures which could result in their personal data being lost or otherwise compromised, as well as of available or advisable precautions that they could take in order to minimize the possible economic loss or social harm that could result from such failures.").

218. Cal. S.B. No. 1386 (signed by the Governor, Sept. 25, 2002) (codified at CAL. CIV. CODE § 1798.29, .82, .84 (West 2012, Westlaw through Ch. 807 of the 2015 Reg. Sess. & Ch. 1 of 2015–2016 Ex. Sess.)).

data breach notification laws.[219] Congress is also considering numerous proposals for a federal data breach notification law to standardize the obligations that companies face and enable consumers to better self-protect.[220]

Companies operating in the United States currently face a daunting patchwork of data breach notification laws.[221] The laws differ in several ways, including on (1) the definition of the time period in which businesses have to notify consumers of a data breach affecting them; (2) whether failure to notify results in civil or criminal penalties and what those penalties are; (3) whether the people affected have a private right of action; (4) whether access to encrypted data is exempt; and (5) whether immaterial breaches are exempt from disclosure and how to define them. The need to harmonize state laws and recent, high-profile, large data breaches at businesses such as Target, Home Depot, Sony, and JPMorgan have spurred efforts toward a federal data breach law.[222] The content of

219. *See Security Breach Notification Laws*, *supra* note 216 (listing legislation and noting that these laws require companies holding sensitive consumer information to notify consumers in case of a data breach).

220. *E.g.*, Commercial Privacy Bill of Rights Act of 2014, S. 2378, 113th Cong. (introduced May 21, 2014); Data Accountability and Trust Act, H.R. 4400, 113th Cong. (introduced Apr. 4, 2014); Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (introduced Jan. 30, 2014); Data Security and Breach Notification Act of 2013, S. 1193, 113th Cong. (introduced June 20, 2013); SECURE IT, H.R. 1468, 113th Cong. (introduced Apr. 10, 2013).

221. *See, e.g.*, *Protecting Small Businesses Against Emerging and Complex Cyber-Attacks*, 113th Cong., 1st Sess. 14–15 (2013) (statement of Dan Shapero, founder of "ClikCloud," on behalf of CompTIA) ("Who do I notify? Which of those 47 states am I required to disclose to when I have lost data from my consumers?").

222. *See, e.g.*, *Sony and Epsilon: Lessons for Data Security Legislation: Hearing Before the Subcomm. on Commerce, Mfg., and Trade of the Comm. on Energy and Commerce*, 112th Cong. 1–3 (2011) (statement of Rep. Mary Bono Mack, Chairwoman, Subcomm. on Commerce, Mfg., and Trade) (discussing the need for a federal data breach law as illustrated by the "massive data breaches at Sony and Epsilon"); *Protecting Small Businesses Against Emerging and Complex Cyber-Attacks*, *supra* note 221, at 60 (noting recent high-profile breaches); Matthew Goldstein & Nicole Perlroth, *Luck Helped in Discovery of Breach at JPMorgan*, N.Y. TIMES, Nov. 1, 2014, at B1 (detailing discovery of large attack over the summer on JPMorgan affecting the data of 76 million households and seven million small businesses); *Myriad Congressional Initiatives Add Up to Incremental Progress on Cybersecurity*, INSIDE CYBERSECURITY, Jan. 28, 2014, Westlaw, 2014 WLNR 2560669 (reporting on impetus to pass federal data breach legislation after revelation of large data breaches at Target and other retailers). For a beautiful data visualization of major cyberattacks, see *World's Biggest Data Breaches*, INFORMATION IS BEAUTIFUL, http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (last updated Aug. 11, 2015) [http://perma.cc/8K6L-8X9Y].

such a law is hotly contested, however, stalling efforts to enact a federal data breach notification law for nearly a decade.[223]

Companies disagree among themselves about what the content of data breach notification laws should be, depending on the industry sector. For example, the entity representing federal credit unions is advocating mandatory "disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of those that place their personal information at risk."[224] This desire for identification—and the incentives to improve that come from identification—stem from concern that credit unions and other financial institutions bear the brunt of the costs of helping consumers after data breaches of retailers' systems, such as issuing new cards, replacing stolen funds, and dealing with the greater volume of customer service needs.[225] A federal credit union representative expressed concern that, while financial institutions pay the costs, "[t]he negligent entity that caused these expenses by failing to protect consumer data loses nothing, and is often undisclosed to the consumer."[226]

Other industry executives argue that data breaches can be quietly addressed without alarming consumers and drawing negative publicity in cases where data was accessed but not stolen, or stolen but not used.[227] Some business leaders also express concern that revealing a breach alerts other hackers to exploitable weaknesses.[228] A third cluster of arguments centers around cyberattacks by nation-states through their intelligence agents on companies with sensitive

223. *See, e.g.*, Notification of Risk to Personal Data Act, S. 751, 109th Cong. (2005) (not passed); Judy Greenwald, *Pressure Builds for Federal Action on Uniform Approach to Data Laws: Legislative Progress Uncertain in 2012*, BUS. INS., Jan. 2, 2012, at 14–15 (noting history of several data breach bills); Grant Gross, *Year End: Congress Slow on Tech Issues in '07*, INFOWORLD DAILY (Dec. 18, 2007), http://www.infoworld.com/article/2650037/application-development/year-end--congress-slow-on-tech-issues-in--07.html [http://perma.cc/Q78D-6EPS] (discussing legislative defeats); *see also* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 932, 932–65 (2007) (discussing different models of disclosure laws).

224. *Protecting Small Businesses Against Emerging and Complex Cyber-Attacks*, *supra* note 221, at 61 (statement of Brad Thaler, Vice President, Legislative Affairs, Nat'l Ass'n of Fed. Credit Unions) (noting recent high-profile breaches).

225. *Id.* at 59–60.

226. *Id.* at 60.

227. Danny Yadron, *Executives Rethink Merits of Going Public With Data Breaches*, WALL ST. J. (Aug. 4, 2014), http://online.wsj.com/articles/a-contrarian-view-on-data-breaches-1407194237 [http://perma.cc/5E3H-G9GN].

228. *Id.*

national security or intellectual property information.[229] Because such attacks are aimed at obtaining national security- or national competitiveness-related information, the materiality for everyday consumers may be lessened and is counterbalanced by the sensitivity of the information for covert investigation and foreign relations purposes.[230] These arguments highlight a larger concern with mandated disclosure—that information would be better utilized by experts and may even prove counterproductive if generally released.

B. Mandated Disclosure and Its Discontents

While disclosure, also termed targeted transparency, is increasingly ascendant as a regulatory tool, it is also controversial. There is a growing body of literature debating the problems with mandatory disclosure and how to fix them.[231] There is also growing scrutiny of the promulgation of transparency as "a pervasive cliché of modern governance" given "uncritical reverence."[232] The idea behind transparency is making information public to inform and improve individual choices on how to consume, invest, vote, and make other important decisions—and to monitor and improve the behavior of information disclosers who must be attentive to market preferences.[233] The reality may fall short of theory, however.[234]

One of the most powerful and repeated critiques regarding the ineffectiveness of disclosures is that the typical individual is overloaded with information.[235] Information overload can arise from

229. *See, e.g.*, *Cybersecurity Roundtable*, *Sec. and Exch. Comm'n*, at 0020: 13–24 (Mar. 26, 2014) https://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt [http://perma.cc/6U6P-YUZL] (statement of Leslie Thornton, General Counsel of WGL Holdings, Inc.) (discussing "nation-states, spies who seek to steal our national security secrets or our intellectual property" as a "threat vector").

230. *See id*. at 0077–78 ("[T]here's materiality and then there's materiality . . . . [Y]ou wouldn't necessarily disclose a nation-state actor trying to do harm in an industry that's very vulnerable . . . particularly if in that situation you don't have a customer base or an employee base that has been compromised because that's not what they're after[.]").

231. *E.g.*, FUNG ET AL., *supra* note 26, at xii–xiv, 171–82; Ben-Shahar & Schneider, *supra* note 25, at 705–10; Calo, *supra* note 213, at 1030–47; Richard Craswell, *Static Versus Dynamic Disclosures, and How Not To Judge Their Success or Failure*, 88 WASH. L. REV. 333, 369–77 (2013); Aarti Gupta, *Transparency Under Scrutiny: Information Disclosure in Global Environmental Governance*, 8 GLOBAL ENVTL. POL. 1, 1–5 (2008); Clifford Winston, *The Efficacy of Information Policy*, 46 J. ECON. LITERATURE 704, 705–10 (2008).

232. Christopher Hood, *Transparency in Historical Perspective*, *in* TRANSPARENCY: THE KEY TO BETTER GOVERNANCE? 3 (Christopher Hood & David Heald eds., 2006).

233. FUNG ET AL., *supra* note 26, at xi.

234. *Id.*

235. *E.g.*, Ben-Shahar & Schneider, *supra* note 25, at 705–10, 716–20; James Gibson, *Vertical Boilerplate*, 70 WASH. & LEE L. REV. 161, 174–78 (2013) (discussing rising

detailed disclosure requirements and from the accumulation of many disclosures in various domains of an individual's life.[236] Moreover, the typical consumer is likely to have mediocre literacy or numeracy skills and therefore is unable to digest disclosures effectively.[237]

In short, the hope for a better-informed choice is a false one.[238] Yet the fiction is sustained because regulation by disclosures looks attractively cheap—to legislators at least—because there is no need for government expenditures to engage in expensive oversight or to hammer out detailed conduct rules and monitor them.[239]

In addition to the critiques of mandated disclosure in the literature, the private-data, public-safety conflicts discussed thus far illustrate two additional, major limitations of consumer-oriented general disclosure. First, general disclosure is better suited for alerting the public to known dangers rather than detecting and preventing them.[240] Second, general disclosure may not be feasible where information is proprietary, raising Fifth Amendment takings clause concerns when the government requires release of the information to the general public.[241] To address these concerns, the next Part discusses a fresh approach to information access to reduce constitutional concerns and otherwise prohibitive costs to business interests while still allowing sufficient bounded access to detect and prevent threats to public health and safety.

III. EXPERT-ORIENTED BOUNDED ACCESS

Despite all the critiques,[242] general public disclosure is still nice—if you can get it. Too often, however, companies prevail in arguing about the perils of general public disclosure.[243] Rather than allowing data that is important to public health and safety to be locked away altogether, another approach short of consumer-oriented public

information processing costs); *see also, e.g.*, Mark I. Hwang & Jerry W. Lin, *Information Dimension, Information Overload and Decision Quality*, 25 J. INFO. SCI. 213, 213–16 (1999) (summarizing studies on poor decisional quality by individuals facing information overload).

236. Ben-Shahar & Schneider, *supra* note 25, at 686–90; Gibson, *supra* note 235, at 174–78 (discussing rising information processing costs).

237. Ben-Shahar & Schneider, *supra* note 25, at 711–15.

238. *Id.* at 705–29.

239. *Id.* at 682 (noting disclosure looks cheap because it "requires almost no government expenditures, and its costs seem to be imposed the story's villain, the stronger party who withholds information").

240. *See* discussion *supra* Section II.A.

241. *See* discussion *supra* Section I.A.

242. *See* discussion *supra* Section II.B.

243. *See* discussion and examples *supra* notes 50–54, 67–84, 86–98.

disclosure is needed. This Article proposes bounded access as a way to unlock such important protected information for an audience best suited to use it. Such a model would allow access to otherwise protected private data by experts and motivated groups. Only those with the ability to design and adhere to a data protection plan to ensure use is for the purpose of addressing important public health and safety issues would be allowed to access the database.

The bounded access approach can be used in lieu of general public disclosure where public disclosure is otherwise barred by protections for trade secrets, property law, or contractual confidentiality terms.[244] Bounded access is also a way to ameliorate the powerful business objections that general disclosure of sensitive information might otherwise defeat progress.[245] Finally, even where general public disclosure is available, a bounded access regime may give experts more richly detailed information with which to detect and prevent public health and safety harms.

A. Expert Rather than Lay Audience

The bounded access concept proposed here is a model of data disclosure that begins with approval of a data protection protocol and discloses information to persons with the training to analyze the data needed to detect and prevent public health and safety hazards. To gain bounded access, users would need to demonstrate that data access would serve a public or safety purpose and submit a data protection protocol, including demonstrated safeguards. Rather than piling more disclosures on the bewildered, information-overloaded general consumer, bounded access is limited to trained professionals such as researchers who are ethically obligated to comply with data-use and protection safeguards and attorneys who are ethically bound to abide by limitations on disclosure. Such trained and motivated information-seekers are also better suited to maximize the value of disclosure by using their expertise to detect potential threats to public safety.

As a first line of detection and defense, public health researchers are a crucial audience for bounded access. Today, such researchers are bound by a web of laws, regulations, and ethical principles that

244. *See* discussion and examples *supra* Part I.

245. *See, e.g.*, Sunshine in Litigation Act of 2011, H.R. 592, 112th Cong. (introduced Feb. 9, 2011) (died); Sunshine in Litigation Act of 2010, H.R. 5419, 111th Cong. (introduced May 26, 2010) (died); Sunshine in Litigation Act of 2009, H.R. 1508, 111th Cong. (introduced Mar. 12, 2009) (died); Sunshine in Litigation Act of 2008, H.R. 5884, 110th Cong. (introduced Apr. 23, 2008) (died); *see also* discussion *supra* notes 156–65.

safeguard research subjects and protect against nonconsensual disclosures of personally identifiable data.[246] Sanctions for violations of such protections for sensitive data can extend beyond professional penalties to include civil and criminal penalties.[247] Researchers thus have deep expertise in complying with complex limits on the uses of data and revelation of identifiable information that may prove damaging. Researchers also have expertise in conducting analyses with de-identified data to extract important information while limiting any damage to an individual entity.[248]

Disclosure to such trained professionals can contain limitations to mitigate any potential damage to individual private entities, such as prohibiting the release of individually identifiable information while facilitating research. Such protected access overcomes Fifth Amendment takings claims that have bedeviled attempts at mandating public disclosure of public health, safety, and environmental information implicating trade secrets.[249] Courts have held that protective orders limiting access to permitted users and for specified purposes obviate the Fifth Amendment takings issue triggered by compelled disclosure of trade secrets.[250] While bounded access is different than a protective order, which is typically limited to the facts and parties in specific litigation, its user and use restrictions should similarly obviate Fifth Amendment takings concerns.

Limiting the audience renders disclosure nonpublic, averting Fifth Amendment takings concerns.[251] For example, the D.C. Circuit

246. *E.g.*, 45 C.F.R. § 45 (2009) (providing privacy protections for human subjects during government research, including IRB review); 45 C.F.R. §§ 160, 162, 164 (2013) (providing protections for electronic health information); National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, *The Belmont Report*, U.S. DEP'T HEALTH & HUM. SERVS. (Apr. 18, 1979), http://www.hhs.gov/ohrp/policy/belmont.html [http://perma.cc/LD89-95F8] (summarizing basic ethical guidelines by which to protect human subjects in government research).

247. *See, e.g.*, 42 U.S.C. § 1320d-5 (2012).

248. Indeed, de-identifying information for analyses is a vibrant area of scholarly activity. *See, e.g.*, Robert J. Bayardo & Rakesh Agrawal, *Data Privacy Through Optimal K-Anonymization*, 21 PROC. INT'L CONF. ON DATA ENGINEERING 217, 217–18 (2005); James Gardner & Li Xiong, *An Integrated Framework for De-Identifying Unstructured Medical Data*, 68 DATA & KNOWLEDGE ENGINEERING 1441, 1442 (2009); Bradley Malin, Kathleen Benitez & Daniel Masys, *Never Too Old for Anonymity: A Statistical Standard for Demographic Data Sharing via the HIPAA Privacy Rule*, 18 J. AM. MED. INFORMATICS ASS'N 3, 3–5 (2011).

249. *See* discussion and examples *supra* notes 100–37.

250. Griffith v. Goodyear Dunlop Tires N. Am., Ltd., No. 11-CV-7615, 2013 WL 104921, at *2 (W.D.N.Y. Jan. 8, 2013); Republic Servs., Inc. v. Liberty Mut. Ins. Cos., No. Civ. A. 03-494-KSF, 2006 WL 1635655, at *7 (E.D. Ky. June 9, 2006).

251. Exxon Corp. v. FTC, 589 F.2d 582, 589 (D.C. Cir. 1978).

in *Exxon Corp. v. FTC*[252] held that a release of business information, including trade secrets, to Congress is not public divulgement, and thus "does not impair the value of the trade secrets involved . . . [or] involve a deprivation prior to which a hearing is required."[253] Responding to the claim that Congress may publicly disclose the released information, the D.C. Circuit held that "[c]ourts must presume that the committees of Congress will exercise their powers responsibly and with due regard for the rights of affected parties."[254] In other words, we are all professionals here. Courts may presume that professionals will comply with protections accompanying specific-purpose and limited-audience disclosure of information important to public safety.

B. Epidemiological Insights on Privacy and Public Protection

The bounded access proposal draws insights from epidemiology, the science of detecting and preventing threats to public health.[255] Epidemiology investigates the patterns and causes of threats to health and safety in populations of people.[256] An important tool in this endeavor is amassing and using sensitive, highly private data for public health surveillance.[257] The goal of disease surveillance is to systematically gather and pool data to detect the causes, prevalence, incidences, and consequences of injury or disease.[258] Data sharing and pooling for disease surveillance has venerable roots running back to the nineteenth century in U.S. and international practice.[259] For example, public health surveillance led to the discovery that a defective vaccine had caused polio in 40,000 children and left 200 children paralyzed.[260] Such epidemiological surveillance also led to the linkage between high-absorbency tampons and toxic shock

252. 589 F.2d 582 (D.C. Cir. 1978).

253. *Id.* at 589.

254. *Id.*

255. *See* NOEL S. WEISS & THOMAS D. KOEPSELL, EPIDEMIOLOGIC METHODS: STUDYING THE OCCURRENCE OF ILLNESS 10 (2d ed. 2014).

256. *Id.*

257. Scott F. Wetterhall & Eric K. Noji, *Surveillance and Epidemiology*, *in* THE PUBLIC HEALTH CONSEQUENCES OF DISASTERS 37 (Eric K. Noji ed., 1997).

258. Lawrence O. Gostin, Scott Burris & Zita Lazzarini, *The Law and the Public's Health: A Study of Infectious Disease Law in the United States*, 99 COLUM. L. REV. 59, 82 (1999).

259. For histories, see, for example, FUNG ET AL., *supra* note 26, at 142; Denise Koo & Scott F. Wetterhall, *History and Current Status of the National Notifiable Diseases Surveillance System*, 2 J. PUB. HEALTH MGMT. & PRAC. 4, 4–8 (1996).

260. For a history, see Michael Fitzpatrick, *The Cutter Incident: How America's First Polio Vaccine Led to a Growing Vaccine Crisis*, 99 J. ROYAL SOC'Y MED. 156, 156 (2006).

syndrome.[261] Trying to detect threats to population health without such data pooling would be laboring "in the darkness of ignorance," as Assistant Surgeon General J.W. Trask put it in 1915.[262]

Epidemiological surveillance often involves the collection of highly sensitive data such as HIV or other infectious disease status.[263] Such information is publicly reported at the aggregate level with strong protections against damaging disclosure about particular individuals.[264] The discipline of epidemiology thus has important insights about protecting privacy without stifling the generation of knowledge about threats to public health and safety.

While disease surveillance is often conducted by governmental entities,[265] the discipline of epidemiology also shows the import of making data available to nongovernmental researchers for analysis. Many expert eyes are needed to advance protection and prevention (indeed, imagine where biomedical science and technology would be in a world where only the government conducted research). The task of uncovering and combatting threats to public health and safety cannot just be centralized within the government.[266] The recent GM and NHTSA fiasco illustrates the risks of such an approach.[267] While the government has an important role to play in gathering and disseminating information, much of the data gathering and analysis is conducted by nongovernmental researchers with specialized expertise. Nongovernmental, expert eyes, such as researchers or consumer protection attorneys, are like beneficial microbes for the

261. For the epidemiology of the link, see Seth F. Berkley et al., *The Relationship of Tampon Characteristics to Menstrual Toxic Shock Syndrome*, 258 JAMA 917, 917, 920 (1987). *But see* Walter F. Schlech III et al., *Risk Factors for Development of Toxic Shock Syndrome: Association with a Tampon Brand*, 248 JAMA 835, 838–39 (1982).

262. John W. Trask, *Public Health Administration: Its Dependence upon Reports of Sickness*, 28 PUB. HEALTH REP. 1, 2 (1913).

263. *See, e.g.*, AMY L. FAIRCHILD, RONALD BAYER & JAMES COLGROVE, SEARCHING EYES: PRIVACY, THE STATE, AND DISEASE SURVEILLANCE IN AMERICA 66–80 (2007) (discussing the surveillance of conditions such as sexually transmitted diseases).

264. *See, e.g.*, Centers for Disease Control & Prevention, *Guidelines for National Human Immunodeficiency Virus Case Surveillance, Including Monitoring for Human Immunodeficiency Virus Infection and Acquired Immunodeficiency Syndrome*, 48 MORBIDITY & MORTALITY WKLY. REP. RECOMMENDATIONS & REPS., Dec. 10, 1999, at 1, 14–16 (No. RR-13).

265. *See, e.g.*, DAVID P. FIDLER, SARS, GOVERNANCE AND THE GLOBALIZATION OF DISEASE 50–52 (2004) (discussing the state-centrism of international public health regimes).

266. *See, e.g.*, *id.* at 50–57 (discussing the role of nonstate actors in promoting public health).

267. *See* discussion *supra* Section I.B.2; *see also, e.g.*, REVIEW OF NHTSA, *supra* note 153, at 1–2 (investigating why NHTSA missed early warning signs).

surveillance and investigation system, unearthing important factors for threat detection and prevention and airing issues in need of attention.

C. Two Tracks of Disclosure: Thick, Rich Information and Thin, Digestible Information

The data needs for an expert audience are very different from those of "Chris Consumer," who represents the paradigmatic audience for mandated disclosure policies and critiques.[268] For the individual consumer to effectively digest information, the information needs to be made thin and grabby—pared down and rendered catchy through images or sounds that seize rather than dull attention.[269] For population-level surveillance and protection, disclosures should be thick and detail rich—precisely the opposite of effective disclosures for individuals. It is also important to offer technical disclosures detailing sampling techniques as well as the raw data to permit effective systematic study.[270]

This difference in form arises from the difference in uses of data. While consumers and other individuals seek identifying information to make choices among goods or services, data disseminated to experts for population-level protection needs to be detail rich to enable detection of patterns of harm and to enable more effective prevention. While bounded access limits the audience for information, it should allow for more meaningful information for purposes of harm detection and prevention.

Disclosure of such important data exacts costs on the reporting entities. In addition to informing the design of disclosures, an epidemiological perspective also provides insights about how to address concerns about damage resulting from disclosure. At the national level, public health surveillance similarly calls for collection of sensitive data, including disease findings that implicate patient

268. *See* discussion *supra* notes 210–17.

269. *See, e.g.*, Sullivan v. CUNA Mut. Ins. Soc'y, 649 F.3d 553, 558 (7th Cir. 2011) (recommending paring down informational forms to "focus on what matters most" to help employees make "intelligent retirement decisions"); Calo, *supra* note 213, at 1030–47 (detailing how creative forms of "visceral notice" that rouse attention can be more effective than traditional notice).

270. *See, e.g.*, Katharina Pistor, *Reconstruction of Private Indicators for Public Purposes*, *in* GOVERNANCE BY INDICATORS: GLOBAL POWER THROUGH QUANTIFICATION AND RANKINGS 165, 179 (Kevin E. Davis et al. eds., 2012) (arguing that raw data and information about sampling techniques should be accessible so that indicators can more meaningfully be used to improve governance).

privacy.[271] At the international level, disease surveillance also calls for reporting potentially embarrassing data that might have economic repercussions for nations reporting disease outbreaks.[272] Moreover, epidemiological research often operates on sensitive human-subject data, including protected medical records.[273]

The corporate privacy interest secured through trade secret, contract, and propertization is far less compelling than a person's privacy interest in health data. As the Supreme Court has explained, unlike human subjects, corporations "are endowed with public attributes" because "[t]hey have a collective impact upon society, from which they derive the privilege of acting as artificial entities."[274] Moreover, the Health Insurance Portability and Accountability Act ("HIPAA") reflects a democratic judgment about the intensely private nature of health information.[275] Yet even after the enactment of HIPAA, researchers have access to patient health data to enable public health research to detect and prevent harms.[276] *A fortiori*, privacy should not be a bar to access in the less compelling context of corporate privacy.

Moreover, epidemiological research practices such as de-identification can help inform the scope of protection for particularly sensitive business information. Since the passage of HIPAA, researchers have further refined strategies for using de-identified data that is pooled and aggregated to detect public health threats.[277] Where companies have a particularly compelling need for protection and where de-identification does not render investigation infeasible, bounded disclosure could include only data stripped of identifiers linking the information to a particular brand or company.

271. For a discussion, see, for example, FAIRCHILD ET AL., *supra* note 263, at 66–80; Mary D. Fan, *Sex, Privacy, and Public Health in a Casual Encounters Culture*, 45 U.C. DAVIS L. REV. 531, 564–67 (2011); Mary D. Fan, *Decentralizing STD Surveillance: Toward Better Informed Sexual Consent*, 12 YALE J. HEALTH POL'Y L. & ETHICS 1, 7 (2012).

272. For a discussion, see, for example, FIDLER, *supra* note 265, at 34–48; FUNG ET AL., *supra* note 26, at 142.

273. *See, e.g.*, Jacquelyn K. O'Herrin, Norman Fost & Kenneth A. Kudsk, *Health Insurance Portability Act (HIPAA) Regulations: Effect on Medical Record Research*, 239 ANNALS SURGERY 772, 772–76 (2004) (discussing navigating HIPAA requirements in medical records research).

274. United States v. Morton Salt Co., 338 U.S. 632, 652 (1950).

275. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 26 U.S.C., 28 U.S.C., and 42 U.S.C.).

276. Roberta B. Ness, *Influence of the HIPAA Privacy Rule on Health Research*, 298 JAMA 2164, 2164–68 (2007).

277. *Id.*

Because disclosure to the research public is different from disclosure to the consuming, individual public, there should be two tracks of disclosure. The disclosure track at the consumer level should draw on insights about paring down information and making data more digestible.[278] The second track of disclosure to the research public should be detail rich with sufficient technical information to facilitate standardization and adjustment for statistical analyses.[279] Access could be restricted to researchers with the proper credentials and who have IRB clearance, ensuring sufficient controls are in place to protect sensitive data.[280]

In some circumstances, the two-track model may become just a single, higher-track model of disclosure where an industry or company succeeds in convincing legislators that information is particularly sensitive. Even if there is not sufficient consensus for mandating general individual-level disclosure, there should be bounded access to public health, safety, and environmental information. Ultimately, reducing the costs of disclosure is a better way to improve the generation of data from multiple sources. Reducing the costs of cooperation is more desirable than coercing resistant entities because there are innumerable creative ways to resist, thereby undermining mandated general public disclosure.[281]

CONCLUSION

Challenging the conventional view that there is no right to privacy for corporations, this Article has illuminated how companies enjoy plenty of privacy through trade secret, contract, and the propertization of information.[282] These regimes create business privacy by other means and are backed by sanctions.[283] Data

278. *See* discussion *supra* Section II.A.

279. *See* discussion *supra* Section II.B.

280. *Cf.* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 26 U.S.C., 28 U.S.C., and 42 U.S.C.); 45 C.F.R. § 164.501, .508, .512, .514 (2014) (establishing IRB for HIPAA and outlining requirements for approval for use of medical data by covered entities for research purposes).

281. For some colorful illustrations, see, for example, Daniel E. Ho, *Fudging the Nudge: Information Disclosure and Restaurant Grading*, 122 YALE L.J. 574, 582–83, 631 (2012).

282. For expressions of the conventional rule, see, for example, United States v. Morton Salt Co., 338 U.S. 632, 652 (1950) ("[C]orporations can claim no equality with individuals in the enjoyment of a right to privacy."); RESTATEMENT (SECOND) OF TORTS § 652I cmt. c. (AM. LAW. INST. 1977) ("A corporation . . . has no right to privacy.").

283. *See* discussion *supra* Section I.A. For the oft-repeated conventional view, see, for example, Browning-Ferris Indus. of Vt., Inc. v. Kelco Disposal, Inc., 492 U.S. 257, 284

ownership and control has the power to illuminate or obscure dangers to public health and safety. Keeping experts and the public data impoverished can impact what makes it onto the policy and research agenda, what receives sustained attention, and what is under-recognized or hidden until the victim counts rise and become too high to overlook. [284]

For some major public safety and security challenges, such as deaths from auto defects, toxic emissions, hazardous products, and drug counterfeiting, crucial data is controlled by private industry actors. The data is private in two senses—it is both proprietary and secluded from scrutiny. When the interests in private data and public safety conflict, what should the law do?

This Article proposes bounded access as a fresh approach to addressing the legal, theoretical, and practical limitations of consumer-oriented general public disclosure. Where information is propertized, general public access—even to protect public health and safety—may not be feasible because of Fifth Amendment takings concerns.[285] Even if there are not constitutional barriers, there may be formidable political barriers, as illustrated by the repeated demise of the sunshine in litigation acts introduced in Congress over the years.[286] Moreover, even where general disclosure might be an option, information-overloaded consumers may not be best situated to utilize the information effectively to detect and prevent threats to health and safety.[287]

A bounded access model of disclosure addresses these challenges by unlocking otherwise protected private data to grant access to experts capable of effectively using data to detect health and safety

(1989) (O'Connor, J., concurring in part, dissenting in part) ("[A] corporation is 'an artificial being, invisible, intangible, and existing only in contemplation of law.' As such, it is not entitled to ' "purely personal" guarantees' whose ' "historic function" has been limited to the protection of individuals.' Thus, a corporation has no . . . right to privacy." (internal ellipses and citations omitted)); *Morton Salt Co.*, 338 U.S. at 652 ("[C]orporations can claim no equality with individuals in the enjoyment of a right to privacy."); Arnold v. Pa. Dep't of Transp., 477 F.3d 105, 111 (3d Cir. 2007) ("The District Court correctly found that, as an entity, Baker 'clearly had no privacy interest' . . . . " (internal brackets omitted)); Crum & Crum Enters., Inc. v. NDC of Cal., L.P., Civ. No. 09-145 (RBK), 2011 WL 886356, at *3 (D. Del. Mar. 10, 2011) ("[B]usiness entities do not have a right to privacy."); Warner-Lambert Co. v. Execuquest Corp., 691 N.E.2d 545, 548 (Mass. 1998) ("Cases from other jurisdictions unanimously deny a right of privacy to corporations."); RESTATEMENT (SECOND) OF TORTS § 652I cmt. c (AM. LAW. INST. 1977) ("A corporation as such has no right to privacy.").

284. *See* discussion and examples *supra* Section I.B.

285. *See* discussion *supra* Section I.B.1.

286. *See* discussion *supra* notes 157–245.

287. *See* discussion *supra* Section II.B.

harms while honoring data protections. The bounded access model can be used where general public disclosure is barred by constitutional or other protections for propertized information or is otherwise not feasible because of political opposition to general public disclosure. Bounded access may also be valuable in addition to general public disclosure by giving experts richer, more technically detailed information, permitting effective investigation to detect and prevent public health and safety harms. Companies thereby retain a form of privacy. They retain control over their proprietary information for most purposes, with only a limited, safeguarded release for threat detection. The goal of this fresh approach is to maximize risk-detection and harm-prevention capabilities, while reducing the incentives to conceal damaging information for fear of harming a particular brand or product.