2010

New Governance, Preemptive Self-Regulation, and the Blurring of Boundaries in Regulatory Theory and Practice

Jason M. Solomon

Repository Citation
https://scholarship.law.wm.edu/facpubs/680

Copyright c 2010 by the authors. This article is brought to you by the William & Mary Law School Scholarship Repository.
https://scholarship.law.wm.edu/facpubs
NEW GOVERNANCE, PREEMPTIVE SELF-REGULATION,
AND THE BLURRING OF BOUNDARIES IN REGULATORY
THEORY AND PRACTICE

JASON M. SOLOMON*

In the literature on “new governance” forms of regulation, the blurring of traditional boundaries is a pervasive but largely implicit theme. This Article makes this theme explicit, and argues that the capacity to blur boundaries is one of new governance’s signature strengths. New governance regulation frequently blurs the roles of regulatory actors, the stages of regulation, the modes of regulation, the functions of a regulatory regime; and the structure of the regulatory regime. The Article applies this lens to a series of case studies, and demonstrates how industry attempts at preemptive self-regulation have created opportunities where new governance forms of regulation could have emerged. Turning prescriptive, this Article calls attention to the political and strategic dynamics around attempts to regulate new domains, and calls on policymakers and scholars to embrace the blurred boundaries of new governance approaches as a possible approach that combines the best of state-centered and self-regulatory forms of governance.

Introduction ................................................................. 591
I. Blurring Boundaries as Descriptive Regulatory Theory .... 594
II. Case Studies: Missed Opportunities for New Governance .... 597
   A. Data Security ..................................................... 599
   B. Childhood Obesity and Sugar-Sweetened Beverages ....... 606
   C. Censorship, the Internet, and China ......................... 611
III. Blurring Boundaries with New Governance: Prescriptions
     for Policy-Makers—Preemptive Self-Regulation’s
     Opportunity for New Governance ............................. 622
Concluding Thoughts .................................................... 624

INTRODUCTION

In the literature on regulatory theory, visual metaphors abound. And John Braithwaite, an Australian and one of the leading regulatory scholars in the world, appears to be responsible for many of them.

In the entry on “Regulation” for the Oxford Handbook of Legal Studies, co-authored with Christine Parker, Braithwaite and Parker

* Assistant Professor, University of Georgia School of Law. Thanks to all the participants at the Transatlantic Conference on New Governance and the Transformation of Law, and particularly David and Louise Trubek for organizing and hosting the Symposium at the University of Wisconsin.
invoke a series of Russian dolls, one inside the other, to convey the different layers of "governance studies" or regulatory theory.¹ In his classic work with Ian Ayres, Responsive Regulation, Braithwaite uses a pyramid to invoke the continuum from the state-centered, command regulation at the tip to self-regulation or none at all at the base, with many models in between.² In a piece on criminology, Braithwaite portrays the night watchman state, sitting alone in a boat, at times steering, at times rowing—at times perhaps fed up with being caught in the middle of this swirling sea of regulatory categories, and so tossing the oars aside and going for a swim.³

"New governance," meanwhile, enters the world of regulatory theory, uplifted by the rhetoric of newness,⁴ and bathed in light. Entering the tired debate between regulation and deregulation, new governance presents a light at the end of the tunnel, a third way. For the regulatory state, new governance represents a "bright future." And a recent collection of works on new governance, authored by many at this conference, was described by one scholar as a "mosaic that is largely . . . bright."⁵

In this Article, I aim to shed some light on the use of "new governance" in regulatory theory and practice by developing a theme which may appear rather dull. The theme plays on a visual metaphor as well, that of blurring boundaries.

Here I use the term "new governance" differently than the way it is used in much of the literature, which uses the term "new governance" to refer to a specific kind of regulatory approach, generally one with particular attributes such as benchmarking, transparency and democratic participation. The Open Method of

---

¹ John Braithwaite & Christine Parker, Regulation, in THE OXFORD HANDBOOK OF LEGAL STUDIES 119, 119-20 (Peter Cane & Mark Tushnet eds., 2003).
Coordination (OMC) in the EU is a prime example. For the purposes of this Article, I use “new governance” more as a term to describe a regulatory strategy or tool—or, as Ayres and Braithwaite use the term “responsive regulation” in their book as an “attitude.”

Call it a regulatory state of mind.

The central argument of the Article is that one of new governance's signature strengths is its capacity for blurring boundaries in theory and practice. In Part I, I describe how blurring boundaries is a theme that pervades the academic literature on new governance, and other related third-way forms of regulation. Though the idea of blurring boundaries is implicit and mentioned in passing in several works, this Article makes the idea explicit and central to discussions of new governance.

With the help of this conceptual frame for thinking about new governance, Part II turns to a series of case studies. The case studies differ from existing new governance accounts in that they are all “pre-regulation”—that is, the case studies are of issues that were not subject to regulation, and describe how the issues got onto the public agenda, and the various pushing and pulling that ensued over how best to regulate that particular domain. The purpose of these case studies is to demonstrate the opportunities for overlapping regulatory frameworks or blurred boundaries on the modes of regulation. Importantly, these case studies are ones where new governance did not emerge. I draw out lessons from the case studies, and explain what a new governance approach in these domains might have looked like.

In Part III, I sketch the way the political and strategic dynamics around the possibility of regulation in these areas can be harnessed to blur the boundaries between the roles and functions of public and private-sector actors and enable a new governance approach to emerge. In understanding how new governance approaches can emerge in the context of past episodes, policy-makers can be ready to use such approaches on future issues. Doing so can chart a regulatory path that blurs the boundary between state-centered and self-regulatory, public and private, and might even lead to better policy outcomes going forward.

---

6. See, e.g., Lobel, supra note 4, at 442 (“[T]he obsessive maintenance of traditional boundaries—including those of public and private, profit and nonprofit, formal and informal, theory and practice, secular and religious, left and right—is no longer a major concern with the shift to the Renew Deal paradigm.”).
I. BLURRING BOUNDARIES AS DESCRIPTIVE REGULATORY THEORY

In seeking to define "new governance," scholars have taken a number of different approaches. The most common approach is to define it as a "type" or "mode" of regulation and then list a set of attributes which make something "new governance" regulation. In this Section, I seek to add to typologies like these by positing that "blurring boundaries" is an attribute of new governance regulation as well. Below I explain how the idea of blurring boundaries pervades new governance regulation and thought, before applying the idea to case studies in Parts II and III.

The idea of blurred boundaries is operative in new governance theory in several ways, which I describe below. They are: (1) blurring the roles of regulatory actors; (2) blurring the stages of regulation; (3) blurring the modes of regulation; (4) blurring the functions of a regulatory regime; and (5) blurring the structure of the regulatory regime. Each of these blurred boundaries has been pointed out by other scholars. My modest contribution in this Part is to bring them together in a unified theme to use as a conceptual frame for the case studies and prescriptive advice for policy-makers below.

Roles. In any regulatory domain, there are generally state actors who are doing the regulating, private-sector actors who are being regulated, and third-parties who may provide input into how the area ought be regulated either because it affects them or their business

---

personally or because they are a nongovernmental organization working in the area, or for other reasons. New governance blurs these roles in several ways. Regulated entities are involved themselves in setting the standards, \(^8\) third parties may be involved in monitoring and enforcement, and state actors may serve as facilitators who oversee mechanisms for information pooling, \(^9\) rather than the experts in administrative agencies envisioned when the administrative state began (at least in the U.S.). \(^10\) The "private role in public governance" \(^11\) may go as far as second-order agreements to implement the regulatory standard that in turn operate to change the content of the standard down the road. \(^12\)

**Stages.** The conventional story on regulation involves either the formulation of something called "law," which is more or less fixed, and can then be "enforced" by state actors trying to maximize compliance. Regulated entities either comply or they do not. If they do not, they are punished. Or else regulation involves the formulation of something called "policy," which involves the balancing of the number of factors to inform the way the state approaches a particular issue. Once the policy is formulated, the next stage is "implementation." So one might, for example, have the United States Congress decide that national policy will be that all able-bodied adults must work and will be cut off from public assistance after a certain period of time even if they cannot find work. Then the relevant federal agency will work to execute or implement that policy through the states.

New governance blurs the boundaries between law and enforcement, and policy and implementation. \(^13\) To use the example

---


10. Another major blurring of roles, of course, has been the performance of traditionally governmental services by private entities. For an overview of such developments, see *GOVERNMENT BY CONTRACT: OUTSOURCING AND AMERICAN DEMOCRACY* (Jody Freeman & Martha Minow eds., 2009). For a look at how the financial crisis led to a new model of privatizing government functions altogether, see Stephen M. Davidoff & David Zaring, *Regulation by Deal: The Government's Response to the Financial Crisis*, 61 ADMIN. L. REV. 464, 535-36 (2009).


13. It may also blur the boundary between law and policy, but that boundary may never have been so clear.
above, under a new governance approach, it might be that Congress sets a goal that all states will maximize the number of able-bodied adults who are employed, and it might make available a certain amount of money to incentivize states to work towards this goal. Then, the states would formulate plans to best achieve this goal, and start to follow those plans. After a few years, those plans would be revisited in light of experience and learning from benchmarking against peers. Under such an approach, it is difficult to tell where policy ends and implementation begins.

Modes. New governance approaches also blur the boundaries between modes of regulation. One can think about this by returning to Ayres and Braithwaite’s regulatory pyramid, which includes intermediate approaches such as enforced self-regulation and co-regulation. Though much of the literature treats new governance as a particular mode of regulation that could simply be included as another line on the pyramid, new governance might also be a strategy or tool to blur boundaries between modes of regulation. One can think about this as either using multiple approaches at once, or making it possible to move relatively easily from mode to mode as circumstances change. This latter point, of course, is the provisional or flexible attribute that many new governance theorists emphasize.

Functions. The basic functions of a regulatory regime are commonly described as setting standards, monitoring compliance, and enforcing noncompliance. To a certain extent, this relates to the “stages” of regulation I describe above, but is functional rather than temporal. New governance blurs these functions: if the goal is continuous improvement in achieving regulatory goals, as laid out particularly by Dorf and Sabel by analogy to the private sector, then the relevant actors are always working together to better achieve the goal. Monitoring and enforcement really become one, and the standards are

14. See Ayres & Braithwaite, supra note 2, at 39.
15. See Kenneth Armstrong & Claire Kilpatrick, Law, Governance, or New Governance? The Changing Open Method of Coordination, 13 Colum. J. Eur. L. 649, 652-53 (explaining that new governance can be seen as a regulatory “tool” or “instrument”).
16. See Dorf & Sabel, supra note 7, at 322-23. This is more of a temporal limitation than a blurred boundary. The idea is that both the means and the ends of regulation ought be treated as provisional in light of inevitable uncertainty and limited knowledge. For discussion in the context of Gunther Teubner’s “reflexive law,” see Eric W. Orts, Reflexive Environmental Law, 89 Nw. U. L. Rev. 1227, 1265 (1994) (“[R]eflexive law recognizes the cognitive and normative limitations of a legal system operating in a complex modern society.”).
17. See Dorf & Sabel, supra note 7, at 292-314 (explaining how innovation in the private sector has increased the problem-solving abilities of firms).
frequently revisited during the monitoring process. Again, the full-employment example is useful here.

**Structure.** Regulatory approaches are commonly characterized as either centralized or decentralized, or alternatively, oriented horizontally or vertically. New governance blurs what are commonly seen as binary choices. In the choice between centralized and decentralized, new governance is commonly characterized as decentralized, but the center plays an important role as well in pooling information and perhaps retaining some kind of backstop enforcement mechanism. Meanwhile, in federal systems like the U.S. and EU, new governance approaches can work both vertically—with the U.S. Congress or federal administrative agency, or the EU Commission at the top—and horizontally, with states or other subunits learning from one another through benchmarking.

I have explained in this Part how blurring boundaries is a critical idea in new governance theory. Though I offer this idea as a modest contribution to descriptive regulatory theory, my prediction is that blurred boundaries of this kind—whether under the guise of “new governance” regulation or not—will be a hallmark of the twenty-first-century regulatory state.

I next turn in Part II to a series of case studies to help illuminate the possible opportunities for new governance to “scale up,” in part through a conscious strategy by policy-makers to blur boundaries—a strategy I discuss and recommend in Part III.

**II. Case Studies: Missed Opportunities for New Governance**

Having introduced the conceptual frame of blurring boundaries as a way of thinking about new governance regulation, this Section turns to a series of regulatory case studies that I then analyze in Part III as missed opportunities for new governance.

One question that has arisen in these early stages of the new governance literature is what kinds of regulatory domains and what kinds of issues, are most likely to lend themselves to new governance approaches. Environmental regulation, for example, seems to be the locus of many new governance approaches, both in the U.S. and EU.¹⁸ Dorf and Sabel look at controversies in three broad categories:

---

"conflicts of economic interest, the provision of public services, and disputes over rights arising from moral differences." I have previously referred to attempts to address "intractable social problems" such as public education or drug treatment in the U.S. as a common site for new governance approaches.

Here, I look to a category that may hold particular promise: new areas of regulation, that is, issues or industries that have not previously been subject to regulation, perhaps because they did not exist. I explain more in Part III why this is an area of particular promise, but to preview, the pushing and pulling involved in debates about regulating new issues may lend itself to blurring boundaries as a means of short-term political compromise, but with long-term benefits for regulatory design.

As Ed Rubin puts it in his article, "[I]n the United States, regulation is typically established in response to a particular economic or social problem, the 'problem' being, of course, a socially constructed perception." When the problem emerges on the public agenda, the potential target of regulation has key strategic choices to make in the face of litigation and "legislative threats." The regulatory debate frequently takes place in the same regulation-versus-deregulation framework that occupies the theoretical literature, and third-way options are not always apparent.

As the case studies below are focused on the regulation of particular industries, it should be no surprise that we see the industries each used some form of "preemptive self-regulation" to react to concern from the public and policy-makers—expressed either through potential lawsuits or the threat of increased regulation—by announcing that they will do the job of regulation themselves. The aim is to take the wind out of the sails of the regulators, and the thrust of much recent regulatory scholarship is that this kind of increased reliance on the private sector might well be a good thing.

In that context, I consider three recent case studies in the U.S. of new issues that have risen to the public agenda. The case studies deal with (1) data privacy and security; (2) the sales and marketing of soda to children; and (3) the regulation of speech abroad by Internet service providers. In considering these case studies, this Article explores the form of self-regulation undertaken by the relevant industries, the

19. Dorf & Sabel, supra note 7, at 284.
20. See Solomon, supra note 5, at 835.
regulation that occurred at the state level, and the alternatives that had been put forth by policy-makers at the federal level.

My methodology here is intended as an addition to the existing new governance literature. Rather than look at case studies where new governance has succeeded or failed, I look at where new governance did not arise, but could have.\textsuperscript{23} The idea is that these kinds of case studies are important in answering the critical questions in the next phase of new governance theory about what the circumstances are where new governance is most likely to emerge and succeed, and also how new governance can scale up more generally.

\textit{A. Data Security}\textsuperscript{24}

In the last decade, the public has become increasingly aware of data-security breaches, and the resulting identity theft.\textsuperscript{25} Misplaced hardware such as backup tapes and hacking attempts and theft by employees can all result in the loss of confidential personal information.\textsuperscript{26} In addition to the loss or theft of physical objects containing data, many data breaches occur virtually, through hacking or other types of fraud. The organizations that experience these losses include state and federal government agencies, retail corporations, financial institutions, and data brokers.\textsuperscript{27}

One high-profile example of a data-security breach stemming from fraud involved ChoicePoint, a company based in Alpharetta, Georgia.\textsuperscript{28} Founded in 1997 as a spin-off from the credit reporting agency

\textsuperscript{23} There is an unexplored assumption here that a policy-maker or "policy entrepreneur" could have successfully pushed a new governance approach if motivated to do so, but did not; certainly this assumption is worth greater exploration. I make no attempt to explain why such an approach did not emerge in these cases.

\textsuperscript{24} Thanks to Alison Lerner, University of Georgia School of Law, class of 2010, for drafting the case study that served as the basis for this Section, and Matt Weiss, University of Georgia School of Law, class of 2008, for doing much of the initial research.


\textsuperscript{26} See generally Paul N. Otto et al., The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information, IEEE SECURITY & PRIVACY, Sept.–Oct. 2007, at 15 (giving general background information on data breaches).


\textsuperscript{28} Evan Perez, Identity Theft Puts Pressure on Data Sellers, WALL ST. J., Feb. 18, 2005, at B1.
Equifax, ChoicePoint is a data broker, serving clients by compiling and maintaining billions of profiles on individuals and businesses in the United States.

Like other data brokers at the time, ChoicePoint existed in an industry largely unregulated, operating outside the boundaries of the main federal laws governing data security and privacy, the federal Fair Credit Reporting Act and the Privacy Act. Though Congress had passed a law in 1999 subjecting financial institutions to some degree of scrutiny on protecting personal information, data brokers like ChoicePoint were not covered by this law either.

The data broker industry had been self-regulating through its trade group, the Individual Reference Services Group (IRSG). The IRSG had propagated a series of data-security guidelines and general

29. Id.
31. The federal government, through the Federal Trade Commission (FTC), can charge "consumer reporting agencies" with violations of the Fair Credit Reporting Act (FCRA) for data breaches. See Daniel J. Solove & Chris Jay Hoofnagle, A Model Regime of Privacy Protection, 2006 U. ILL. L. REV. 357, 359-60 (2006) (describing the weakness inherent in using the FCRA to handle data-security breach cases). The FCRA requires that consumer-reporting agencies institute procedures to ensure accuracy, and allows for procedures which have now become familiar, such as the ability to access one's credit report and correct mistakes on it. Id. at 360. Additionally, government agencies are subject to the Privacy Act of 1974, which regulates public sector use of confidential information and is modeled after the FCRA. Privacy Act of 1974, 5 U.S.C. § 552a (2006). Finally, companies under the purview of the SEC may face violations of the Exchange Act for data security-breach incidents. See Otto et al., supra note 26, at 17-18. However, data brokers like ChoicePoint are not covered under any of these statutes. See id. at 15.
32. See Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (2006). Under the 1999 Gramm-Leach-Bliley Act (GLBA), the financial services industry was subject to regulations "to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." Id. § 6801(b)(3) (emphasis added). The relevant agencies released a set of Guidelines that required financial institutions to develop and implement a set of procedures to protect against the release of confidential personal information. See, e.g., Gideon Emcee Christian, A New Approach to Data Security Breaches, 7 CANADIAN J.L. & TECH. 149, 155-56 (2009) (describing the GLBA and subsequent agency action); see also Ritu Singh, Two-Factor Authentication: A Solution to Times Past or Present? The Debate Surrounding the Gramm-Leach-Bliley Security Safeguards Rule and the Methods of Risk Assessment and Compliance, 2 I/S: J.L. & POL'Y FOR INFO. SOC'Y 761, 763-65 (2006) (discussing the implementation of the Guidelines and the lax enforcement and compliance with GLBA).
principles. 34 But the self-regulatory attempts of the industry were weak, and not effective in controlling access to confidential information.

On February 14, 2005, MSNBC.com broke the story that individuals had posed as ChoicePoint clients to gain access to ChoicePoint’s databases. 35 The article also revealed that fifty fake companies had been established to acquire consumer data from ChoicePoint and that the breach had likely affected 35,000 consumers in California. 36 A few days later, ChoicePoint publicly acknowledged for the first time that this breach had occurred several months prior. 37 On February 16, the Atlanta Journal-Constitution reported that law enforcement agents had predicted that the problem extended beyond California and likely placed hundreds of thousands of non-Californians at risk. 38 On that same day, ChoicePoint acknowledged that it would send out 35,000 statements to consumers outside of California notifying them of the potential for identity theft due to the 2004 security breach. 39

The incident spurred a flurry of litigation and legislative action all over the country. Several complaints were filed against ChoicePoint asserting several types of claims. It faced a class action lawsuit brought by shareholders, 40 and several individual lawsuits. 41 Scrutiny of ChoicePoint hit its apex as the company filed a Form 8-K with the Securities and Exchange Commission (SEC) acknowledging ongoing government investigations by the SEC and the Federal Trade Commission (FTC). 42 Thirty-eight state attorneys general publicly submitted a joint letter to ChoicePoint demanding that it notify residents within their state regarding any of their personal information that may have been disseminated during the company’s security breach. 43 ChoicePoint eventually reached a settlement with the FTC, in which it agreed to pay a $10 million civil penalty, create a $5 million fund to

36. Id.
38. Id.
39. Id.
41. Otto et al., supra note 26, at 18.
43. 38 AGs Send Open Letter to ChoicePoint, ASSOC. PRESS FIN. WIRE, Feb. 19, 2005.
compensate the victims of identity theft, and supply detailed information to the FTC every two months for two years on its compliance with data-security measures.

In addition to action against ChoicePoint specifically, the media attention to the issue spurred state governments and the federal government into taking action on the issue. Some states had passed data breach notification laws before the ChoicePoint incident. In 2002, a security breach had compromised the social security numbers of all California state employees. The employees were not informed of the problem for several months, and the way the breach was handled led to the enactment of the first data-security breach notification law, S.B. 1386. This was the first time that state or federal law required notification to the person whose data was compromised. Other states, in the wake of increased public awareness on the issue, also enacted data breach notification laws. As of 2009, forty-one states and the District of Columbia have data breach notification laws.


45. FTC Consent Order, supra note 44.


47. Id. California Security Breach Notification Act, CAL. CIV. CODE § 1798.82 (West 2009).

48. See ALASKA STAT. § 45.48.010 (2009); ARIZ. REV. STAT. ANN. § 44-7501(L)(4) (2009); ARK. CODE ANN. § 4-110-105(a)(1) (2009); COLD. REV. STAT. § 6-1-716 (d)(1) (2009); CONN. GEN. STAT. § 36a-701b(b) (2009); DEL. CODE ANN. tit. 6, § 12B-102(a) (2009); D.C. CODE § 28-3852(a) (2009); FLA. STAT. § 817.5681(1)(a) (2006); GA. CODE. ANN. § 10-1-912 (2009); HAW. REV. STAT. § 487N-2(a) (2009); IDAHO CODE ANN. § 28-51-104(5), 28-51-105 (2009); 815 ILL. COMP. STAT. § 530/10 (2008); IND. CODE § 24-4.9-3-1 (LexisNexis Supp. 2009); IOWA CODE ANN. § 715C.1-2 (West Supp. 2009); KAN. STAT. ANN. § 50-7a02(a) (2008); LA. REV. STAT. ANN. § 51:3074(a) (West Supp. 2010); MD. CODE ANN. § 14-3502(A) (LexisNexis 2009); MASS. GEN. LAWS ch. 93H, § 3 (LexisNexis Supp. 2009); MINN. COMP. LAWS ANN. § 445.72 (West 2009); MONT. CODE ANN. § 325E.61, Subdiv. 1, (West 2010); MO. ANN. STAT. § 407.1500.2 (West 2010); MONT. CODE ANN. § 30-14-1704(1) (2009); NEB. REV. STAT. ANN. § 87-803 (LexisNexis 2009); NEV. REV. STAT. ANN. § 603A.220 (LexisNexis 2007); N.H. REV. STAT. ANN. § 359-C:19(V) (YEAR); N.J. STAT. ANN. 56:8-163(12)(a) (West YEAR); N.Y. GEN. BUS. LAW § 899-aa.2 (Publisher YEAR); N.C. GEN. STAT. § 75-65 (YEAR); N.D. CENT. CODE § 51-30-02 (YEAR); OHIO REV. CODE ANN. § 1349.19(A)(1)(a) (Publisher YEAR), 2008 H.B. 2245(a) (YEAR) (Okla.); OR. REV. STAT. § 646A.604 (2009); 73 PA. CONS. STAT. § 2303 (2008); R.I. GEN. LAWS § 11-49.2-3 (Supp. 2008); S.C. CODE ANN. § 39-1-90 (Supp. 2009); TENN.
The majority of those state laws are primarily modeled after California’s groundbreaking notification law. That law required any company that stored consumer data electronically to notify any California resident impacted by a security breach to the company’s databases if the company had reason to believe that any unencrypted information about the consumer had been accessed by an unauthorized individual or entity. That statute required notification “in the most expedient time possible and without unreasonable delay . . . .” Failure to provide notice in the event of a breach would result in civil liability, including class action lawsuits. The California law provided limited exceptions to this requirement. A company could provide substitute notice through e-mail, a posting on its Web site, or through major statewide media if the cost of providing notice exceeded $250,000, the number of consumers impacted exceeded 500,000, or the company did not have sufficient contact information to reach the impacted consumers individually.

After the ChoicePoint incident, members of Congress introduced a wave of data breach notification bills. One bill, introduced by California Senator Dianne Feinstein, sought to create a strong uniform

49. Compare California Security Breach Notification Act, CAL. Civ. CODE § 1798.82, with sources cited supra note 48. Other states adopted similar statutes using California’s legislation as a template but varied based on their definitions of “personal information,” their notification requirements related to encrypted information, conditions necessary to trigger notification requirements, the procedures necessary to satisfy actual notice, the situations in which substitute notice was permissible, and the timetable for notification, which ranged from a set time period (i.e., forty-five days in Florida) to more vague requirements (such as California’s requirement to notify consumers in the “most expedient time possible and without unreasonable delay”). Id.

50. See GINA MARIE STEVENS ET AL., CONG. RESEARCH SERV., CRS REPORT FOR CONGRESS, DATA SECURITY: FEDERAL AND STATE LAWS (2006), available at http://assets.opencrs.com/rpts/RS22374_20060203.pdf. While most states are like California in that they require notification when there has been any “unauthorized access” of personal information, several states have a higher threshold for when notification is triggered: instead of simply unauthorized access, these states require some determination of “likelihood of misuse.” Schwartz & Janger, supra note 27, at 932–34. For example, Florida’s data-breach law requires disclosure when unauthorized access “materially compromises the security, confidentiality, or integrity of personal information . . . .” FLA. STAT. ANN. § 817.5681(4) (West 2006).

51. CAL. Civ. CODE § 1798.82; CONG. RESEARCH SERV., supra note 50.
52. CAL. Civ. CODE § 1798.82; CONG. RESEARCH SERV., supra note 50.
53. CAL. Civ. CODE § 1798.82(g)(2)–(3); CONG. RESEARCH SERV., supra note 50.
notification requirement, while another bill limited notification to cases where there was a "significant risk of identity theft." Other bills focused on what Cary Coglianese and David Lazer have called "management-based regulation." Rather than focusing on a notification requirement, these proposals added a requirement that companies implement a program to protect data, while leaving the specifics to individual companies. A bipartisan bill in the House said specifically that the consumer reporter companies to be regulated had to utilize "the current state of the art in administrative, technical, and physical safeguards for protecting" the personal data. None of these bills ever became law, and data brokers remain largely unregulated.

54. See Notification of Risk to Personal Data Act, S. 115, 109th Cong. (2005). The bill also broadened the scope of required disclosures, eliminated any safe harbor for disclosed encrypted information, and created additional federal agencies to combat identity theft and to oversee statutory compliance. Id. Enforcement authority was provided to the state attorneys general, who could sue the companies responsible for data breaches for civil remedies. Id.


57. See, e.g., Identity Theft Protection Act, S. 1408, 109th Cong. § 2(b)(1) (2005) (introduced by Sen. Gordon Smith (R-Or.)). As with Senator Sessions’s legislation, this bill required the implementation of a program to secure personal consumer information through "administrative, technical, and physical safeguards . . ." Id. The most robust such bill was introduced by, among others, Senators Arlen Specter (R-Pa.), and Patrick Leahy (D-Vt.), the Chairman and Ranking Democratic Member of the Senate Judiciary Committee. Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong. (2005). The bill mandated that companies create a personal data privacy and security program, id. § 2, based in part on the Interagency Guidelines for financial institutions, and also set third-party contractors hired to process data, id. § 502.

58. Data Accountability and Trust Act, H.R. 4127, 109th Cong. § 2(a)(1)(B) (2005) (DATA) (introduced by Rep. Cliff Stearns (R-Fla.). DATA required establishing a policy for information collection, appointing a data-security officer within the organization, taking preventative and corrective action, and creating a process for the disposal of obsolete data. Id. § 2(a)(2). In the case of a breach, the FTC would then be authorized to require the data broker to submit its information protection policy to an FTC audit. Id. § 2(b).

The state notification laws—now the primary means of regulation—have their critics. The strict-liability nature of some of the state notification laws has come under criticism for requiring notification even when a breach may pose no actual threat to the consumer. Overly ambitious notification laws, which require notification for almost any type of breach, may lead to "envelope triviality," a term which describes the phenomenon in which consumers begin to disregard data breach notices as just another piece of junk mail because so many of them arrive in the mail.

In the case of data security, when the legislative smoke cleared after the ChoicePoint and other incidents, the data-broker industry was left largely unregulated. Though subject to varying notification laws in different states ex post, there was no governmental push to improve security and minimize the risk of breach ex ante. Perhaps, though, the notification laws are all that is needed. It may be that the reputational sanction of having to notify thousands of individuals of any breach provides the necessary incentive for firms to invest in security programs that will minimize the chances of such breach from recurring.

One key lesson of experimentalism (let alone the recent financial crisis), of course, is that we just do not know. We do not know how technology and other changes in the data-broker industry are going to affect the likelihood of breach. We do not know whether and in what circumstances a combination of market incentives and self-regulation are going to be sufficient. And we do not know when another high-profile incident will galvanize public attention sufficiently to make any kind of regulation even possible.

This is where the ability to blur boundaries among modes of regulation, at the time when the issue is of high public salience, can be quite useful.

Consider how a new governance approach might have worked in the case of ChoicePoint and its aftermath. Congress could have passed a law directing the FTC to work with industry and consumer groups to establish preliminary standards for companies' data-security programs, based perhaps on the existing interagency guidelines for financial institutions. Then the law could have enlisted the existing industry self-


61. Schwartz & Janger, supra note 27, at 952. Another critique of the current crop of state and federal data notification laws is that it is impossible for businesses to comply with a patchwork of state law plus federal regulation. Even without the federal legislation on the table, businesses today must be aware of forty-two subtly different notification laws, plus any applicable federal regulations under the FTC, SEC, and HIPAA.
regulation mechanism, the IRSG, for benchmarking going forward, while giving consumer groups a formal seat at the table in making sure that companies were continuing to work towards achieving the standards. The FTC might issue periodic reports on companies' progress as an additional spur for improvement.62

By building in a mechanism for periodically revisiting the standards, and giving the FTC authority to take punitive action against companies that are fallen seriously short, Congress could build in blurred boundaries such that the regulatory regime could move to a more "top-down" approach if needed, and without the need for more regulatory authority.

B. Childhood Obesity and Sugar-Sweetened Beverages63

In 2001, the Surgeon General issued a "call to action" on the problem of obesity.64 Though he defined the problem as severe among people of all ages, there was a particular focus on the rapid rise in obese children and what could be done about it.65 The Surgeon General's recommendations, as well as the rest of the Bush administration's reaction in the months to follow, focused in part on encouraging exercise in schools and healthier eating.66 The response of the Congressional majority followed similar lines, with legislation to fund exercise programs, obesity-related research, and educational programs to encourage good nutrition.67

This case study focuses on the issue of sugar-sweetened beverages (SSBs), including sodas, fruit juices, and sports drinks, contributing to childhood obesity in the United States.

At the time of the Surgeon General's call to action, existing federal regulation of the sale of SSBs in schools was, and is, slight, falling

---

62. Another model can be found in Schwartz and Janger's article. Id. at 960-70 (proposing a coordinated response agent (CRA) that will be more comprehensive than simple notification laws).

63. Thanks to Rachel Goodrich, University of Georgia School of Law, class of 2010, for drafting the case study on which this Section is based.


65. See id. at 19–21.

66. See id. at 33–35.

67. See also Child Nutrition and WIC Reauthorization Act of 2004, Pub. L. No. 108-265, 118 Stat. 729. The Act requires local educational institutions using the National School Lunch Program to establish local wellness policies setting forth "nutrition guidelines . . . for all foods available on each school campus under the local educational agency during the school day with the objectives of promoting student health and reducing childhood obesity . . . ." Id. § 204(a)(2).
under the Child Nutrition Act, which authorizes the Secretary of
Agriculture to regulate “competitive foods”—foods and beverages sold
in competition with the National School Lunch Program and the
National School Breakfast Program. Such foods are only permitted if
state and local governments ban the sale of “foods of minimal
nutritional value” in the lunchroom while meals are served. Federal
regulations identify soda as a food of minimal nutritious value.

The beverage industry has vigorously resisted regulation of SSBs
for years. For example, the National Soft Drink Association (NSDA), a
national trade organization of soft drink manufacturers and sellers,
successfully challenged the sale-of-competitive-foods regulations in
1983 as an unauthorized time-place restriction. Over the next few
decades, though, as state regulation of SSBs increased, the beverage
industry began to change their approach.

In 2002, the NSDA issued press releases arguing for increased
physical activity in schools. These press releases argued that sodas did
not have a role in childhood obesity and championed the “value of
business-school partnerships.” Diverging from the industry’s
approach, Coca-Cola established Model Guidelines for School
Partnerships in 2003, which on the one hand advocated removing soft
drinks from elementary schools, but on the other hand allowed for sales
to older students. Additionally, the guidelines were voluntary both for
schools and suppliers, there was no enforcement of the guidelines, and
there was no way to confirm adherence to the guidelines.

The American Beverage Association, a representative organization
of “beverage producers, distributors, franchise companies and support
industries,” disseminated a vending machine policy for schools in
2005. The policy recommended that (1) only water and 100 percent
juice be provided in elementary schools, (2) non-diet soft drinks and

70. National School Lunch Program, General Purpose and Scope, 7 C.F.R.
71. Nat’l Soft Drink Ass’n, 721 F.2d at 1351.
72. Michelle M. Mello et al., The Interplay of Public Health Law and
    Industry Self-Regulation: The Case of Sugar-Sweetened Beverage Sales in Schools, 98
    statement on efforts to ban or restrict the sale of carbonated soft drinks in schools).
73. Id. (citation omitted).
74. Id.
75. Id.
76. American Beverage Association, About ABA: History,
    http://www.ameribev.org/about-aba/history/ (last visited Feb. 9, 2010).
77. Mello et al., supra note 72, at 600.
juice drinks with less than 5 percent juice be removed from middle schools, (3) and that a maximum of 50 percent soft drinks be available in high school vending machines. Not only was this policy short lived, but it was also non-binding during its tenure. The policy was issued simply as the industry's view of what is appropriate for beverage sales in schools. The policy contained no enforcement mechanism or system to monitor adherence.

In 2004, President Bill Clinton underwent quadruple bypass surgery, which at least one journalist surmised prompted his involvement in the fight on fat. The William J. Clinton Foundation and the American Heart Association formed the Alliance for a Healthier Generation (Alliance) in 2005, "to create a healthier generation by addressing one of the nation's leading public health threats—childhood obesity." In 2006, the Alliance announced an agreement with Cadbury-Schweppes, Coca-Cola, and PepsiCo to minimize the sales of SSBs in schools. The Alliance agreement ordered a phase-out of SSB sales in schools and specified portion sizes. Unlike prior industry self-regulation efforts, the Alliance agreement provided mechanisms for monitoring adherence to the guidelines. The Alliance set a goal for the beverage guidelines to be 100-percent implemented by the 2009-2010 school year.

While the beverage industry made an overture to regulation via the Alliance agreement, the agreement remains less restrictive than some state and local regulation. The only binding provision of the agreement is that the companies support assessing the effect of the new policy. Beverage companies do not pledge to stop working with bottlers who fail to follow the guidelines. The guidelines do not affect

79. Mello et al., supra note 72, at 600.
80. Id.
81. Id.; see Vending Policy, supra note 78.
84. Mello et al., supra note 72, at 600.
85. Id.
86. Id.
87. Id.
88. Id.
89. Id.
90. Id.
existing beverage contracts, only those signed going forward.\textsuperscript{91} Notably, enforcement mechanisms have been non-existent in the industry’s self-regulation efforts.\textsuperscript{92}

The same year as the Alliance agreement with the beverage companies, Senator Tom Harkin (D-Iowa) along with a bipartisan coalition, proposed stronger federal regulation.\textsuperscript{93} Harkin’s proposal included requiring the Secretary of Agriculture to update the thirty-year-old federal nutrition standards for foods of minimal nutritional value.\textsuperscript{94} Additionally, the scope of application would be broadened beyond the cafeteria and into the hallways and school gymnasiums by prohibiting the sale of snack foods anywhere on campus and throughout the entire school day that do not meet the new nutrition standards.\textsuperscript{95} At the same time, Congresswoman Lynn Woolsey (D-Cal.) introduced identical legislation in the House of Representatives.\textsuperscript{96} The American Medical Association and the Parent Teacher Association endorsed the legislation,\textsuperscript{97} but both of the 2006 bills died in committee and met the same fate when reintroduced in the House and the Senate in 2007.\textsuperscript{98}

Meanwhile, activity has continued at the state and local level, as well as with industry self-regulation. State and local governments have taken steps to limit or ban the sale of soda in schools.\textsuperscript{99} California has

\begin{itemize}
\item \textsuperscript{91} Id.
\item \textsuperscript{92} Id.
\item \textsuperscript{94} Id. § 10(b)(1)(A).
\item \textsuperscript{95} Id. § 10(b)(1)(B).
\item \textsuperscript{97} U.S. Senator Tom Harkin, Senator Harkin’s Health and Wellness Update: Harkin Pushes Bipartisan Measure to Improve Kids Health, April 2006 (on file with author).
\end{itemize}
been a leading state in such regulation and since 1979 has required that at least 50 percent of the foods and beverages sold at school during the school day meet nutrition standards. Los Angeles County prohibited sales of sodas in all of its schools in 2004, and the Philadelphia School District has banned beverage sales other than 100 percent juice, water, milk, and “electrolyte replacement” drinks.

The upshot of the attention to childhood obesity in the United States in the early part of the decade, then, has been a scattershot approach. On the one hand, “scattershot” is a pejorative term, but “decentralized” or Hayekian “spontaneous order” are not. Perhaps the efforts of civil society (like Bill Clinton’s foundation), and state and local governments, are making as much progress or more on the issue of childhood obesity than could have been achieved with federal regulation.

It is likely, though, that a national, new governance kind of approach could achieve greater progress. Such an approach could blur the boundary between centralized and decentralized regulation by having the Surgeon General use the bully pulpit, and the U.S. Departments of Health and Human Services and Agriculture be both the sites of information-pooling and the source of funds for states to put into place initiatives to address these issues. It would be decentralized and horizontal, though, by placing the onus on the states to come up with the mechanisms and participate in the benchmarking to address the issue of childhood obesity.

This approach could work much like the Obama Administration’s current “Race to the Top” initiative to spur greater efforts and educational improvement on the states. Under that initiative, the Department of Education has made available millions of dollars to states for educational improvement, but conditioned the funds on the use of data to drive such improvement, including the use of student achievement measures to evaluate teachers.

Similarly, the federal government could make available money for states to promote exercise among kids and put healthy foods in the schools, but condition the money on measures to take sugar-sweetened beverages out of the schools. States could be required to submit plans


101. Mello et al., supra note 72, at 596.
for making progress on childhood obesity—plans to be formulated with the participation of parents and public health agencies—and be required to report regularly on progress. Bill Clinton's Alliance for a Healthier Generation could play a role in monitoring. In this way, continuous improvement towards the goal of decreasing childhood obesity could be built into the regulatory regime so that the momentum from public attention is not lost as other issues move on to the public agenda.

C. Censorship, the Internet, and China

In the 1990s, countries that had speech restrictions on journalists and reporters extended them to cover Internet content. North Korea, Iran, Burma, Turkey, Egypt, Cuba, China, and several other countries aggressively censor the Internet, and many dissidents and bloggers have landed in jail as a result. China has the most sophisticated and extensive methods for controlling its citizens' access to the Internet. The government's controls are so complete that many in the press and in the industry speak of the "Great Firewall of China." Private organizations devoted to free speech in the United States, as well as government-funded organizations like Radio Free Asia and Voice of America, began instituting anti-jamming technology and other methods in an attempt to counteract the efforts of the Chinese government.

Public awareness, including the attention of Congress, began to grow after a few highly publicized incidents in which Chinese dissidents were jailed, as well as because of the increasingly strict regulations implemented by the Chinese government. However, what

102. Thanks to Alison Lerner, University of Georgia School of Law, class of 2010, for her excellent work in drafting the case study that served as the basis for this Section.


104. See id. at 9.


106. In 2002, the Chinese government implemented filtering software based on keywords, which greatly increased its ability to control content. Jill R. Newbold, Aiding the Enemy: Imposing Liability on U.S. Corporations for Selling China Internet Tools to Restrict Human Rights, 2003 U. ILL. J. L. TECH. & POL'Y 503, 511 (2003). In 2003, President Hu Jintao took office, and restrictions on speech tightened further. See RACE TO THE BOTTOM, supra note 103, at 3. In 2004, the government jailed Shi Tao, a prominent anti-government blogger, in a highly publicized incident that created an outcry in the media around the world. Id. at 32; Information Supplied by Yahoo!
became clear in 2005 and 2006 was that U.S.-based Internet Service Providers (ISPs) were actively complying with the Chinese government’s restrictions on speech, essentially counteracting the efforts of the U.S. government and the various non-profit and university-affiliated organizations that were actively engaged in attempts to bring down the firewall.107

Essentially, when the Chinese and other governments asked U.S. companies like Google, Yahoo!, Microsoft, and Cisco for help, the companies listened. Acting under the reasonable assumption that when operating in a foreign country, they were obligated to follow local laws,108 they generally complied with the requests from foreign governments. One of the earliest such examples is the prosecution by the French government of Yahoo! for hosting an online auction of Nazi memorabilia, a practice which is banned in France.109 Though Yahoo! vigorously denied the ability of the French government to control its conduct in this way, since its servers are located in California, it eventually voluntarily changed its policy and blocked the auctions.110


107. Rachel Laing, Hitting Wall in China, SAN DIEGO UNION-TRIB., Feb. 15, 2006; see generally Lloyd, supra note 105.


110. Yahoo! brought the French government’s requests to federal court in the United States to determine if they were enforceable in the U.S., but the court handily ducked the issue by declaring it moot—since Yahoo! had already complied with the order, without further action by the French government, there was no case. See Yahoo! Inc. v. La Ligue Contre Le Racisme et L’Antisemitisme, 433 F.3d 1199 (9th Cir. 2006). Yahoo! also came under fire in the mid-2000s for releasing information that ultimately lead to the arrest and imprisonment of the Chinese dissidents Li Zhi in 2003 and Shi Tao in 2004. See Tom Zeller Jr., Internet Firms Facing Questions About Censoring Online Searches in China, N.Y. TIMES, Feb. 15, 2006, at C3. See also RACE TO THE BOTTOM, supra note 103, at 107–10; Information Supplied by Yahoo! Helped Journalist Shi Tao Get 10 Years in Prison, supra note 106. In addition to the disclosure to Chinese authorities of personal identifying information, Yahoo! also engages in the
Microsoft and Google have also come under fire for their actions. Microsoft admits that it complies with Chinese government speech laws by censoring searches through its MSN portal.\textsuperscript{111} Additionally, in December of 2005, Microsoft shut down the blog of Chinese critic and dissident Zhao Jing in the midst of a scandal in which Chinese authorities were cracking down on the \textit{Beijing News}.\textsuperscript{112} Google’s activities in the Chinese market came into the public eye when it launched Google.cn in January 2006, the Chinese-language version of the widely used search engine.\textsuperscript{113} It explicitly de-lists Web sites that fail to comply with Chinese government law, though its list of blocked terms was developed internally by Google employees, rather than imposed from above by the Chinese government.\textsuperscript{114}

The U.S. government reaction to both the Chinese government and the corporations who have complied with its restrictions has proceeded in fits and starts. During the 1990s, the U.S. government devoted some energy toward breaching the great firewall through Broadcasting Board of Governors, which oversees the International Broadcasting Bureau (IBB), Radio Free Asia, and the Voice of America. These organizations function as reporting agencies and the IBB “works to serve as . . . a free and professional press” to distribute information around the globe.\textsuperscript{115} However, these efforts were not significantly funded, and as the awareness of Chinese censorship grew, Congress began to get interested.

On September 19, 2002, the House Policy Committee released a now oft-cited policy statement entitled, “Tear Down This Firewall.”\textsuperscript{116} It described the various abuses that had been documented by groups such as Reporters Without Borders and Human Rights Watch in repressive regimes, such as denying ISP access, censoring Internet access, and de-listing Web sites in compliance with Chinese government speech laws, which means that certain Web sites are simply unavailable on Yahoo!’s Chinese-language search engine. \textit{See RACE TO THE BOTTOM, supra note 103, at 26.}


\textsuperscript{112} \textit{RACE TO THE BOTTOM, supra note 103, at 43-44.}

\textsuperscript{113} \textit{Id. at 55; Google to Censor Results on New Chinese Search Site, WASH. POST, Jan. 25, 2006, at D10.}

\textsuperscript{114} \textit{RACE TO THE BOTTOM, supra note 103, at 55; Google to Censor Results on New Chinese Search Site, supra note 113.}

\textsuperscript{115} Broadcasting Board of Governors, About the Agency, http://www.bbg.gov/about/index.html (last visited Feb. 12, 2010); Lloyd, \textit{supra note 105.}

content, using cost-prohibitive pricing of e-mail accounts, and banning personal computer ownership. The report listed several countries that are considered the worst offenders, noting that the People's Republic of China "commits the most Internet abuses." It concludes by offering several policies that would form the basis of the legislation introduced on February 14, 2006, the Global Internet Freedom Act (GIFA).

GIFA's stated goal was, among other things, to "develop[] and deploy[] technologies to defeat Internet jamming and censorship." It defines jamming to include not only actual jamming software, but also "censoring, blocking, monitoring, or restricting Internet access and content by using technologies such as firewalls, filters, and 'black boxes.'" Additionally, the bill cites the First Amendment and Article 19 of the United Nations' Universal Declaration of Human Rights as support for its prescriptions.

To counteract jamming, the bill proposed creating an Office of Global Internet Freedom (OGIF) within the International Broadcasting Bureau, which would be charged with developing a "comprehensive global strategy to combat state-sponsored and state-directed Internet jamming . . . ." It also pledged money and support to private anti-jamming efforts, which would presumably go to the four primary companies engaged in those efforts.

GIFA was introduced several times between 2002 and 2006, but never went anywhere. On February 14, 2006, the last time that GIFA was introduced, then-Secretary of State Condoleezza Rice announced the creation of the global Internet Freedom Task Force within the State Department. The task force released its strategy statement in December 2006, which highlighted its three-prong approach: monitoring, responding to threats, and advancing Internet freedom.

117. Id.
118. Id.
119. After the initial introduction of the Global Internet Freedom Act in 2002, it was subsequently introduced twice more but failed to be made into law. See H.R. 4741: Global Internet Freedom Act, GOVTRACK.US http://www.govtrack.us/congress/bill.xpd?bill=h109-4741&tab=related (discussing successive Senate and House bills) (last visited Apr. 9, 2010).
121. Id. § 6.
122. Id. § 2(1).
123. Id. § 4(a); see supra note 115 and accompanying text (discussing the IBB).
124. H.R. 4741 § 3(5); see supra note 105 and accompanying text (discussing of private anti-jamming companies).
126. Smith, supra note 106, at 518.
Though some have praised its approach as "responsible," others have noticed that it got off to a "bumpy start" and has not appeared to accomplish much in its time in existence. The creation of GIF A was no accident. The next day, the Subcommittee on Africa, Global Human Rights, and International Operations, and the Subcommittee on Asia and the Pacific of the House Committee on International Relations held a joint hearing entitled, "The Internet in China: A Tool for Freedom or Suppression?" At this hearing, representatives from Google, Yahoo!, Cisco, and Microsoft submitted to a thorough grilling by congressional representatives. Representative Chris Smith (R-N.J.) said the companies were engaged in a "sickening collaboration, decapitating the voice of the dissidents." He also compared the company's actions to IBM's relationship with the Nazi government, in which IBM provided the Third Reich with punch card technology and organizational systems that helped them automate much of their activities.

The industry defended its actions, claiming that without guidance from Congress, it had no choice but to comply with the local laws of whatever country it was operating in. Some emphasized the need for compromise with foreign governments. Bill Gates spoke publicly the day after the hearing arguing that, "I don't think that a [rule] that said you shouldn't do business in some place whose standards aren't identical to the US would work . . . . Germany bans Nazi hate speech—the US clearly constitutionally protects that. Should I do business in Germany?"

However, though the ISP companies spent most of their time at the hearing defending their actions and calling for guidance, one of the biggest proposals to come out of the hearing was a call for "leadership by the corporations to develop a code of conduct which would spell out how they could operate in China . . . while not harming citizens and

127. Id.
130. Id. at 2 (statement of Rep. Smith).
131. Id.
132. Id. at 65-76 (statement of Elliot Schrage, Vice President for Corporate Communications & Public Affairs, Google, Inc.).
respecting human rights." Additionally, Representative Smith talked about the legislation he was planning to introduce on this issue, the Global Online Freedom Act (GOFA). The day after the joint hearing, February 16, Representative Smith introduced GOFA, which built off GIFA, but was substantially broader in focus. Its mission is "to promote freedom of expression on the Internet, to protect United States businesses from coercion to participate in repression by authoritarian foreign governments, and for other purposes." Once the scope of the problem with corporate interaction abroad became known, GIFA’s tactic of funding anti-jamming efforts suddenly appeared insufficient. Like the earlier GIFA legislation, GOFA would create an Office of Global Internet Freedom (OGIF), but GOFA locates it inside the State Department and gives it some of the same duties as the recently announced GIFA. The shift in location of the OGIF, from the IBB to the State Department, likely represents a growing awareness of the sovereignty issues that are implicated. The OGIF would consult with ISP companies, human rights organizations, and academic organizations to develop the type of "voluntary code of minimum corporate standards related to Internet freedom" that was discussed in the congressional hearing.

GOFA never got out of committee. It was re-introduced by Representative Smith in January of 2007 and reported by the committee in October of 2007, but no action was taken at that time. It was placed on the House calendar in February of 2008, but so far, no action has been taken on it.

After the introduction of GOFA, the ISP companies began working in close collaboration with organizations like the Center for Democracy and Technology (CDT) and the Berkman Center, and with various politicians who had worked on GOFA, to develop the voluntary code of conduct. However, as 2007 passed and no code of conduct was

135. Id.
137. Id.
138. Id. § 104.
139. Id. § 104(b)(6).
released, pressure from the media and from politicians began mounting on companies to take action.\textsuperscript{143}

Finally, on May 20, 2008, the Subcommittee on Human Rights and the Law of the Senate Judiciary Committee held a hearing entitled, “Global Internet Freedom: Corporate Responsibility and the Rule of Law.”\textsuperscript{144} At this hearing, Senator Durbin announced that lawmakers will “no longer . . . tolerate the delay” on the voluntary code of conduct.\textsuperscript{145} Human Rights Watch argued that the primary hold-up on the code has been over who will monitor U.S. ISP company activity abroad.\textsuperscript{146} Organizations like Human Rights Watch (HRW), Reporters Without Borders, and the Berkman Center had advocated for independent monitoring, while the ISP companies insisted that self-monitoring was preferable.\textsuperscript{147} HRW indicated that Google was the most intransigent of the ISP companies, though all were resistant to the idea of outside monitoring.\textsuperscript{148} HRW proposed that the government create a system of compliance rules and penalties that ISP companies should follow in addition to the voluntary code, modeled after the Foreign Corrupt Practices Act (FCPA).\textsuperscript{149} However, not all the human rights and Internet freedom nonprofits were in agreement: the Berkman Center supported the process of a voluntary code of conduct, and did not believe that any legislation would be effective under the current circumstances.\textsuperscript{150}

However, the ISP companies and some others defended their progress, with the CDT announcing that it felt “hopeful that we are close to reaching our goal”\textsuperscript{151} and noted that the talks had already lead to changes in the way the companies operate—for example, Google had begun alerting users in China when results from their searches had been

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{143} Id.
\item \textsuperscript{145} Id. at 3 (statement of Sen. Durbin).
\item \textsuperscript{146} Id. at 10–12 (statement of Arvind Ganesan, Director, Business and Human Rights Program, Human Rights Watch).
\item \textsuperscript{147} Id.
\item \textsuperscript{148} Id. at 12.
\item \textsuperscript{149} Id. Bill Gates himself, actually, suggested modeling legislation on the FCPA. Waters, supra note 133. The FCPA works by requiring that companies put systems in place to prevent abuses, and then holds them accountable when abuses occur. Id.
\item \textsuperscript{150} 2008 Hearing, supra note 144, at 119 (statement of John G. Palfrey, Jr., Clinical Professor of Law and Executive Director, Berkman Center for Internet & Society, Harvard Law School).
\item \textsuperscript{151} Id. at 115 (statement of Leslie Harris, President and CEO, Center for Democracy & Technology).
\end{enumerate}
\end{footnotesize}
censored, and Yahoo! and MSN quickly followed their lead. The meeting ended with Senator Durbin imploring or threatening Google to speed up the progress on the code of conduct.152

Finally, in October of 2008, the ISP companies announced the creation of the Global Network Initiative (GNI), a self-described “multi-stakeholder group of companies, civil society organizations (including human rights and press freedom groups), investors and academics” whose goal is “to protect and advance freedom of expression and privacy in the [information and communications technologies] sector . . . .”153 The primary substance of the GNI’s work as of this writing was the creation of three “core documents” which represent the three “core commitments” of the GNI.154 These three documents are titled Principles, Implementation Guidelines, and the Governance, Accountability & Learning Framework.155

The Principles document reiterates the GNI’s commitment to freedom of expression and privacy, which it defines as basic human rights.156 It also commits itself to “responsible company decision-making,” “multi-stakeholder collaboration,” and “governance, accountability and transparency.”157 It defines freedom of expression “using Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR).”158 In turn, the UDHR defines freedom of expression very broadly, including the “freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”159

The Implementation Guidelines are more detailed, and are designed to provide more concrete guidance for companies on how to conduct their operations.160 However, these guidelines are still extremely general: participant companies “should” use “human rights impact assessments,” which should be adapted over time in response to

155. Id.
157. Id.
158. Id.
159. Id.
changing circumstances, to understand the impact of their actions. \(^{161}\)

The content of a "human rights impact assessment" is left somewhat vague. There are no specific timelines for reporting back to the GNI, and the criteria for what should be reported is fairly open. \(^{162}\) The guidelines do encourage companies to press governments for the legal grounds for their requests. However, the language is still very open: participating companies "will encourage governments to be specific, transparent and consistent in the demands, laws and regulations . . . ." \(^{163}\) Additionally, the Implementation Guidelines ask that "[p]articipants will also encourage government demands that are consistent with international laws and standards on freedom of expression." \(^{164}\)

The third core commitment and accompanying document is to Governance, Accountability, & Learning. \(^{165}\) The most interesting part of this section is the timeline for accountability. From 2009-2010, Phase One: Building Capacity allows companies to continue to self-regulate, making only annual reports to the GNI. \(^{166}\) In 2011, Phase Two will begin which will involve a process of independent assessment to "review and evaluate" the internal systems of each GNI participant to ensure compliance with the Principles. \(^{167}\) By 2012, in Phase Three, the GNI will begin accrediting a pool of independent assessors who "will prepare detailed reports explaining each company's responses to specific government demands" among other things. \(^{168}\) At this point, the

\(^{161}\) Id.

\(^{162}\) Id.

\(^{163}\) Id.

\(^{164}\) Id.


\(^{166}\) Id.

\(^{167}\) Id.

\(^{168}\) Id.
assessors will be reporting back to the Board of the GNI, which will make the final call on whether a given company’s actions are compliant with the principles.169

The response to the creation of the GNI has been tepid.170 The most substantive criticism of the GNI is that after two years of intensive talks, consulting with politicians, the involvement of the most prominent members of both the ISP world and the academic and human rights communities, the best that anyone could come up with was a series of noncommittal, overboard policy goals characterized by an overabundance of unpersuasive clauses like “should” and “are encouraged to.”171 While several of the politicians involved in getting the GNI off the ground released press statements supporting the GNI,172 not everyone was happy with the result.173

The status quo has remained self-regulation.174 Indeed, no independent assessment by the GNI is even scheduled until 2011,

169. Id. These core commitments are carried out by the group’s stakeholders, which include the ISP companies and non-profits discussed earlier. See Global Network Initiative, Participants, http://www.globalnetworkinitiative.org/participants/index.php (last visited Feb. 5, 2010). In addition to the human rights non-profits and academics that were active in the creation of the GNI, the members also include socially responsible investment firms like the Calvert Group and Trillium Asset Management. Id. The only governmental participant is a United Nations Special Representative to the Secretary-General on Business & Human Rights, who has observer status. Id.


though the participants are required to make annual reports to the GNI. 175

The story of the rise and fall of the issue of corporate complicity with foreign censorship, though, could have been a new governance success. The story went like this: corporations collaborated with repressive governments in a way that angered the public and deeply concerned Congress and the State Department. A public outcry ensued, Congressional hearings were held, and the threat of legislation and regulation was dangled over the heads of the offending companies. Desperate to avoid government regulation and not wanting to lose the valuable Chinese market, the companies undertook a series of reforms of behavior in close collaboration with the relevant NGOs. And the resulting governance mechanism—the Global Network Initiative actually looks a lot like a new governance model. 176 Indeed, policymakers could have made the GNI a government-sanctioned entity, as they have done with other self-regulatory organizations. 177

For example, the GNI’s system of accountability arguably resembles the top-down model of new governance seen in the EU, in which guidelines and objectives are set at the EU level, which are built upon and implemented by Member States. 178 In this analogy, the GNI’s Principles are the overarching guidelines and objectives, and each company’s internal policy to comply with and implement the principles are equivalent to the actions by EU Member States. However, this is far from a perfect match—the EU is, of course, a governing political body, rather than a loose coalition of corporate, non-profit, and academic stakeholders. 179

The main problem with the result is the conspicuous absence of any governmental players in the GNI group of stakeholders to allow public values and foreign policy interests to enter into the equation on an ongoing basis. The interactions among Congress, the State Department, private ISP companies, academic research organizations,

175. See Governance, Accountability & Learning Framework, supra note 165.
176. Thanks to Alison Lerner for thoughts on this analogy.
178. Solomon, supra note 5, at 824.
179. Of the twenty-four participants in the GNI as of this writing, fully half of them are high-profile and well-funded non-profit and academic organizations such as Human Rights Watch, the Berkman Center, the Center for Democracy and Technology, and the Electronic Frontier Foundation that were active during the 1990s and 2000s in monitoring and publicizing the activities of the Chinese government. See Global Network Initiative, supra note 169.
and non-profit human rights and Internet freedom groups could easily have resulted in a very collaborative, flexible coalition similar to the GNI, but with the crucial inclusion of a supervising governing body. The OGIF, based in the State Department and as proposed by the GOFA legislation, would have been uniquely suited to that goal. Indeed, a host of commentators and scholars suggested solutions along these lines, though none ever actually used the phrase "new governance." 180

III. BLURRING BOUNDARIES WITH NEW GOVERNANCE: PRESCRIPTIONS FOR POLICY-MAKERS—PREEMPTIVE SELF-REGULATION’S OPPORTUNITY FOR NEW GOVERNANCE

Having provided a sense of the push and pull between self-regulatory and more state-centered approaches in these case studies involving new issues for regulation, I also discussed the case studies as missed opportunities for new governance, and outlined how new governance approaches that embrace the idea of blurred boundaries among the roles and functions of different actors might work in each domain. In doing so, I aimed to offer advice for third-way policy-makers on future issues. Where much of the literature approaches the question as one of optimal institutional design, this Article adopts more of a posture of institutional adaptation, looking at how regulatory dilemmas arise and considering how new governance features can emerge from private ordering.

As someone who believes that this kind of new governance approach is good, my advice to policy-makers is simple. To borrow from and paraphrase the former Republican vice-presidential candidate and Governor of Alaska Sarah Palin, “Blur, baby, blur.” 181 The idea here is that policy-makers could have strengthened desirable features of new governance like transparency, benchmarking and monitoring—thus “capturing” the self-regulation—while still enlisting the industries themselves to do much of the work.


The key to understanding how such an approach might emerge is to see the opportunity created by the preemptive self-regulation by industry on a new issue facing potential regulation. Essentially, the industry creates a new regulatory architecture that can then be captured by regulators for a new governance regulatory regime with blurred boundaries of the kind I have described. So I pause here to flesh out this observation a bit, in part by revisiting the case studies, before concluding.

Each of the three case studies in Part II involved a dynamic more or less like the following: (1) an issue not previously subject to regulation became a matter of public concern; (2) policy-makers became interested in addressing the issue, and proposed various forms of regulation; (3) in an attempt to ward off such government regulation, the industry announces a new regulatory architecture of its own to address the problem. It is this last step that I am calling "preemptive self-regulation."182

The question for policy-makers at this stage, then, is this: is self-regulation enough? It is unlikely that policy-makers address this question directly, though. As a practical matter, the self-regulation frequently acts to deflate the concern, at least among elites, and the industry's political influence—whether it is the data brokers, beverage companies, or ISPs—also serves to stave off more robust government regulation.

In this context, blurring boundaries is political strategy for progressive or third-way policy-makers, designed to achieve "half a loaf" of regulation when the full loaf is politically implausible. But it is also a partial answer to the limits of government agencies—enlisting private-sector entities to do monitoring and enforcement helps address the scarce resource problem. And as new governance theorists have pointed out, it may also be an answer to other regulatory dilemmas such as the inherent uncertainties about how to best solve problems.183

182. Edward Balleisen and Marc Eisner refer to this as a well-established and crucial "tactic in the politics of deflection." See Balleisen & Eisner, supra note 177, at 131 ("Whenever some corner of the business community faces a groundswell of popular support for regulations that will impinge on its commercial practices, the odds are good that its leaders will champion some form of industry-wide regulatory self-governance as a means to forestall more onerous rule making and enforcement by the state.").

183. See Bradley C. Karkkainen, Reply, "New Governance" in Legal Thought and in the World: Some Splitting as Antidote to Overzealous Lumping, 89 MINN. L. REV. 471, 484 (2004) ("Writings of the 'democratic experimentalist' camp, in particular, emphasize the inherent and inescapable epistemic constraints that limit our ability to map and devise comprehensive solutions to complex and dynamic social problems, militating in favor of a regulatory architecture that embraces the provisionality, revisability, and experimental character of all policy determinations.").
The term "agency capture" is commonly used to describe an industry exerting undue influence over the administrative agency that is supposed to be regulating its activity and essentially "capturing" the public agency for its own ends. But we might think of this as an example of "industry capture"—where the government enlists the industry to perform public regulatory functions, capturing private-sector entities like the Individual Reference Services Group for the data-broker industry, a partnership between the Alliance for a Healthier Generation of beverage industry on childhood obesity, and the Global Network Initiative set up to provide guidelines for Internet service providers trying to balance free-speech principles with complying with foreign laws.\(^\text{184}\)

Policy-makers can take advantage of this kind of "industry capture" approach to avoid the result in the three case studies—classic examples of preemptive self-regulation that served to take the issue off the public agenda for the foreseeable future, leaving no public regulatory regime in place. Instead, by blurring the boundaries between the roles and functions of the public and private sectors in regulation, policy-makers can create a new governance regulatory regime with the flexibility to adjust to problems as they arise, and with the necessary "buy-in" from the private sector to encourage cooperation.

CONCLUDING THOUGHTS

After laying out the conceptual frame of "blurring boundaries" in Part I, this Article has tried in Parts II and III to think through the options facing policy-makers in "real time." That is to say, regulatory design rarely takes place on a blank slate, even for issues that have not previously been subject to regulation like the ones I discuss in the case


I invent and use this new term of "industry capture" to refer to the distinct idea that there is this existing private-sector regulatory architecture which the public sector uses for its own ends. Another related idea is that of delegating regulatory authority to firms, explored in Kenneth A. Bamberger, Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State, 56 Duke L.J. 377, 377–78 (2006).
studies. Thinking through how new governance approaches can emerge from the dynamic politics of agenda-setting and the subsequent debate over possible regulatory approaches can help to both identify the circumstances where new governance is likely to succeed, and broaden those circumstances.

A central theme of Ayres and Braithwaite's *Responsive Regulation* is that there is no such thing as an ahistorical optimal regulatory strategy. But in most circumstances, blurring boundaries may well be an optimal regulatory strategy, even though it does not constitute a full regulatory approach.

If new governance scholars have a theory about how to capture self-regulation and other regulatory approaches in order to promote the desiderata of transparency, benchmarking, and deliberation associated with new governance approaches, then policy-makers may be able to scale up "new governance" approaches in the U.S. in a way that has not been possible thus far. This Article has aimed to contribute to that project.

185. *See Ayres & Braithwaite*, supra note 2, at 5 ("[T]he best [regulatory] strategy is shown to depend on context, regulatory culture, and history.").