2009

# Are "Better" Security Breach Notification Laws Possible?

Jane K. Winn
*University of Washington School of Law*

# ARE "BETTER" SECURITY BREACH NOTIFICATION LAWS POSSIBLE?

*By Jane K. Winn*†

I. **INTRODUCTION** ..... 1133

II. **WHAT MAKES "BETTER" REGULATION BETTER?** ..... 1137

III. **CALIFORNIA'S SECURITY BREACH NOTIFICATION LAW** ..... 1142

IV. **CHALLENGES OF REDUCING SECURITY BREACHES** ..... 1151

V. **CAN SBNLS GET "BETTER?"** ..... 1159

VI. **CONCLUSION** ..... 1164

## I. INTRODUCTION

Since California enacted the first security breach notification law (SBNL) in 2002,[1] a tidal wave of security breach notices has been unleashed on American consumers, making the problem of inadequate information security in American businesses visible to the public for the first time. These laws should provide American businesses with incentives to make significant changes in the way they handle and store consumer information in order to reduce the risk that the security of that data will be breached, or at least to reduce the risk that they will be required to notify their customers that a breach has occurred. While SBNLs do appear to be raising public awareness of the problem of computer security, it is unclear what, if any, impact SBNLs are having on the total volume of security breaches, or information security more generally.[2] In the years since the first SBNL was passed, the incessant



† Charles I. Stone Professor and Director, Law, Technology & Arts Group, University of Washington Law School.

1. S.B. 1386, 2001-02 Leg., Reg. Sess. (Cal. 2002), codified at CAL. CIV. CODE §§ 1798.29, 1798.80-.84 (2009).

2. In 2007, the New Zealand Privacy Commissioner was reported as saying that "evidence is emerging that laws to force disclosure of data breaches have a deterrent effect and that it then becomes part of the mindset of businesses to protect themselves against the liabilities that can arise," although no data was cited to support these assertions. Tom Pullar-

drumbeat of public disclosures of security breaches in the mass media suggests that significant improvements in the security of business information systems may be slow in coming.[3]

Part of the problem may be the limited scope of SBNLs themselves, which has created a fragmented, incoherent liability scheme. The nature of any causal connection between security breaches and concrete harms suffered by consumers such as identity theft remains unclear.[4] Because American consumers are not protected by a general right of information privacy, mere notice that a security breach has occurred is not associated with any right to compensation.[5] Attempts to establish a right to damages following receipt of a security breach notice through class action lawsuits have generally only succeeded in clarifying the degree to which no such right exists,[6] al-

---

Strecker, *Data breach law investigated; Statutory code may be alternative to legislation*, THE DOMINION POST, June 11, 2007, at 5. In 2008, researchers at Carnegie Mellon University found that SBNLs were having almost no discernable impact on the volume of identity theft, and noted without reaching any conclusion that they might be changing business behavior. Sasha Romanosky et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, SOCIAL SCIENCE RESEARCH NETWORK, Sept. 16, 2008, at 16, http://ssrn.com/abstract=1268926 (follow "Download" hyperlink). *See also* Marcus Ranum & Bruce Schneier, *Face-Off: State Data Breach Notification Laws-Have they Helped?*, SEARCHSECURITYASIA.COM, Jan. 20, 2009, http://www.searchsecurityasia.com/content/face-state-data-breach-notification-laws-have-they-helped (Ranum argues that SBNLs are "a huge distraction that has more to do with butt-covering and paperwork than improving systems security" while Schneier supports the use of SBNLs to shame companies for bad security and to provide data for research).

3. In 2009, the Ponemon Institute reported that 21 percent of organizations surveyed had encryption strategies, up from 16 percent in 2007. THE PONEMON INSTITUTE, 2008 ANNUAL STUDY: U.S. ENTERPRISE ENCRYPTION TRENDS 2 (2008), http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008_Annual_Study_US_Encryption_Trends_280308.pdf. The study was sponsored by PGP, a major vendor of encryption software, and focused on U.S. information technology companies, a population likely to be more aware of information security issues than companies in other sectors of the economy. *Id.*

4. Romanosky et al., *supra* note 2, at 2-3.

5. *See generally* JANE K. WINN & BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE § 14 (Aspen Law & Business 4th ed. Supp. 2009) (providing an overview of the limitations of information privacy rights under U.S. Law).

6. *See*, *e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007) (holding that increased risk of identity theft is not a cognizable harm); Pinero v. Jackson Hewitt Tax Serv., 594 F. Supp. 2d 710 (E.D. La. 2009); Aliano v. Tex. Roadhouse Holdings, L.L.C., 2008 U.S. Dist. LEXIS 104428 (E.D. Ill. Dec. 23, 2008); Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273 (S.D.N.Y. 2008); Melancon v. La. Office of Student Fin. Assistance, 567 F. Supp. 2d 873 (E.D. La. 2008); Shafran v. Harley-Davidson, 2008 U.S. Dist. LEXIS 22494 (S.D.N.Y. Mar. 24, 2008); Kahle v. Litton Loan Servicing, 486 F. Supp. 2d 705 (S.D. Ohio 2007) (holding that a duty of care was owed and breached, but paying for credit monitoring is not an injury); Ponder v. Pfizer, 522 F. Supp. 2d 793 (M.D. La. 2007). *But cf.* Stollenwerk v. Tri-West Healthcare Alliance, 254 Fed. Appx. 664 (9th Cir. 2007) (reinstating an identity theft victim suit even with only circumstantial evidence of causation, but holding

though many businesses suffering breaches have chosen on a voluntary basis to provide their customers with credit monitoring services to reduce the risk of harm from identity theft.[7]

Analyzing SBNLs from a regulatory impact perspective shows that they impose high compliance costs on relatively few businesses while providing only weak incentives to most businesses to make major changes in the security of their information systems. SBNLs were modeled after "community right to know" (CRTK) laws, which were developed in order to improve the efficacy of environmental laws.[8] CRTK laws can enhance the impact of other regulation—such as mandatory minimum levels of computer security for businesses that handle sensitive consumer information or a right to statutory damages for breaches of the privacy of personal information—but alone cannot provide a coherent regulatory framework.[9] The narrow, targeted approach taken in SBNLs may be justified in political terms as a tactic calculated to generate widespread American public support for stronger information privacy laws, or as the broadest form of computer security law that could actually be enacted in America today. If this is the case, however, then there is a large gap between what may have been politically expedient and what would be socially or economically optimal.

If SBNLs are having an impact on corporate behavior, that impact appears to be modest even among many of the most sophisticated companies. In 2009, a report was published of a review of the "risk factors" sections of the 10-K filings of publicly listed Fortune 500 companies as a means of assessing the recognition within those companies of privacy and data security issues.[10] The study concluded that even many Fortune 500 companies do not appear to appreciate fully the financial and reputational risks posed by fail-

---

that credit monitoring victims cannot proceed); Am. Fed'n of Gov't Employees v. Hawley, 2008 U.S. Dist. LEXIS 25308 (D.D.C. Mar. 31, 2008) (holding that damages for distress may be permitted under Privacy Act after TSA lost TSA employees' personal information).

7. *E.g.*, Jenn Abelson, *Breach of Data at TJX is Called the Biggest Ever*, BOSTON GLOBE, Mar. 29, 2007, at A1. In that instance, TJX offered credit monitoring for customers whose driver's license numbers were exposed in a security breach. *Id.*

8. *Compare* Emergency Planning and Community Right to Know Act of 1986, 42 U.S.C. §§ 11001-11050 (2009) *with* CAL. CIV. CODE §§ 1798.28, 1798.80-.84 (2009).

9. NEIL GUNNINGHAM & PETER GRABOSKY, SMART REGULATION: DESIGNING ENVIRONMENTAL POLICY 65 (1998).

10. In 2008, Hiscox and consulting firm NetDilligence surveyed 60 US organizations in different sectors including healthcare, retail, and financial services; and ranging in annual revenue from tens of millions to billions. Hiscox, Data Privacy and Corporate America: Who's Recognizing the Risk? (Apr. 2009), http://www.hiscox.com/Downloads/d2899def-619c-4147-bbe4-3a85426a44c4.pdf.

ures to secure databases of sensitive personal information.[11] With regard to the use of encryption, which California's and many other state's SBNLs recognize as a safe harbor that can reduce or eliminate the need to provide notices following a security breach, the white paper reported on a separate study of sixty U.S. companies. That study found that only seven percent had implemented end-to-end encryption of sensitive data; forty-two percent of the companies investigated had suffered a data breach, and of those only twelve percent had encryption in place for data at rest; forty-seven percent of the companies had not fully implemented laptop encryption; and twenty-nine percent of the companies had not fully implemented back-up tape encryption.[12] While no similar data exists for small and medium-sized enterprises, it would be reasonable to expect that management attention to security breach risks and use of encryption technologies would be even lower among such companies.

This Article will evaluate the provisions of California's pioneering SBNL in light of "better regulation" or "smart regulation"[13] criteria in order to highlight the costs of taking a narrowly focused, piecemeal approach and the benefits of taking a more comprehensive perspective to the problems of identity theft and information security. Just as the basic structure of SBNLs was borrowed from environmental law, this Article will borrow from decades of analysis of the impact of environmental regulation to evaluate the likely impact of SBNLs. Just as environmental laws can be used to reduce externalities created through the mismanagement of common pool resources found in the natural environment, information security laws can be used to reduce externalities created through the mismanagement of common pool resources found in the virtual environment. If the analogy to environmental law is well drawn and the problem of identity theft is recognized as only a symptom of larger underlying systemic problems—including inadequate information system security[14]—then a narrow, piecemeal regulatory strategy will be no substitute for an integrated, multi-faceted regulatory strategy.[15]

---

11. *Id.* at 3.

12. *Id.* at 11.

13. See *infra* Part II for an explanation of what constitutes "better regulation" or "smart regulation."

14. Identity theft may be a symptom of other problems as well. *See*, *e.g.*, Ranum & Schneier, *supra* note 2 ("What we really need are laws prohibiting financial institutions from granting credit to someone using your name with only a minimum of authentication.").

15. GUNNINGHAM & GRABOSKY, *supra* note 9, at 15 ("The central thesis of this book is that recruiting a range of regulatory actors to implement complementary combinations of policy instruments, tailored to specific environmental goals and circumstances, will produce more effective and efficient regulatory outcomes."); *see also* DANIEL J. FIORINO, THE NEW ENVIRONMENTAL REGULATION 217-18 (2006) (noting that the new environmental regula-

To provide a framework within which the provisions of SBNLs can be analyzed, Part II of this Article provides a general overview of academic and political "better regulation" initiatives undertaken in recent decades. While the Clinton Administration's emphasis on "reinventing government" was displaced by the Bush Administration's emphasis on "deregulation" in the United States, outside the United States interest in "smart regulation" strategies continued to grow during the 2000s and are likely to enjoy a new vogue under the Obama Administration. In Part III, California's pioneering SBNL is analyzed in light of better regulation principles, which spotlights some obvious shortcomings of the legislation. The business, technological, and regulatory challenges posed by any effort to reduce the volume of security breaches are analyzed in Part IV. Given the enormity of those challenges, it should come as no surprise that a regulatory scheme as limited in scope as SBNLs is having only a modest impact on the information security policies of database owners. Because information security problems are complex and multi-faceted, they may defy any attempt to resolve them with simple solutions. If achieving a significant reduction in the volume of data breaches is taken seriously as a policy goal, then there may be no alternative but to face the challenges of developing and enacting not just "better" SBNLs, but a better general "information security" regime.

## II. WHAT MAKES "BETTER" REGULATION BETTER?

In 1992, Ian Ayres and Jon Braithwaite described many of the basic principles now recognized as essential elements of "better" or "smart" regulation in their book RESPONSIVE REGULATION.[16] They approached the theoretical goal of transcending the artificial constraints of the "regulation versus deregulation" political conflict by focusing on an apparent paradox observed in attempts to assess the effectiveness of regulation: while it would come as no surprise to anyone that lax regulatory regimes engender low levels of compliance, merely reversing strategy and adopting a harsh regulatory regime is unlikely to raise levels of compliance.[17] Ayres and Braithwaite argued that deploying an integrated array of strategies, beginning with collaborative engagement and ending with termination of business activity, would achieve the best regulatory outcomes.[18] With such a strategy, regulators respond diffe-

---

tion would be a more adaptable, performance based-learning system achieved by combining higher order fundamental decisions with lower order, incremental decisions).

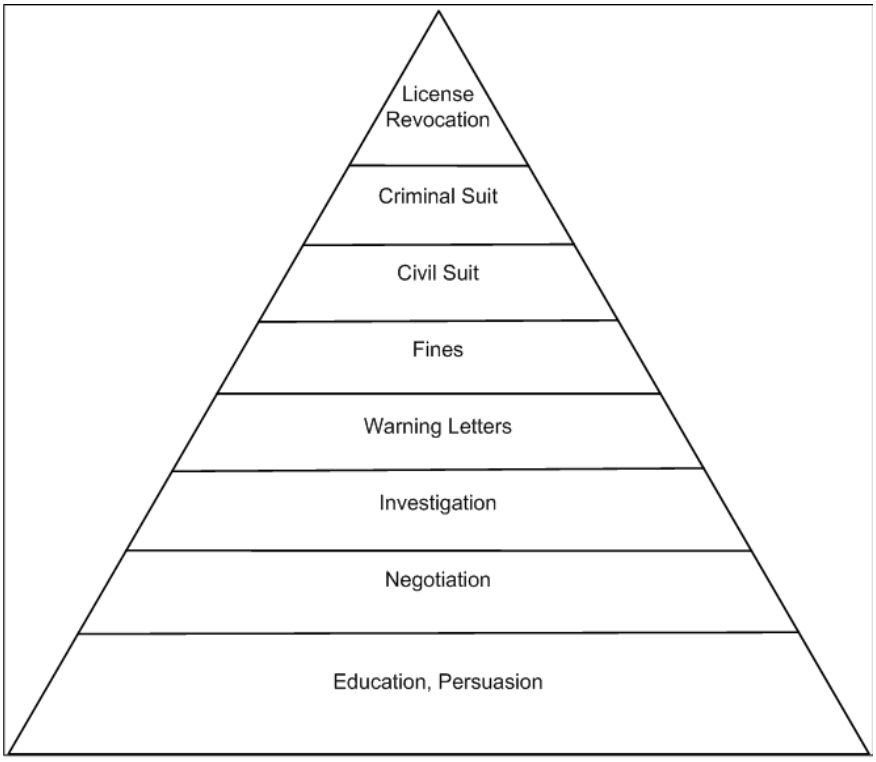
16. IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE (1992).

17. *Id.* at 19-20, 25.

18. *Id.* at 40.

rently depending on whether the regulated entity manifests voluntary compliance or refuses to cooperate.[19] As shown in Figure 1, this integrated approach to regulation is often illustrated as a "regulatory pyramid" with the mildest and most commonly used regulatory responses at the base and the most severe and infrequently used responses at the apex.

**Figure 1: Regulatory Pyramid**




Around the same time that Ayres and Braithwaite were writing about responsive regulation, President Clinton established the National Performance Review, an ambitious effort to streamline government, reduce top-down bureaucracy and reliance on command-and-control regulations, and introduce new government policies and procedures modeled on private sector institutions.[20] In the United Kingdom, similar policies were put in place

19. *Id.* at 35.

20. Remarks by President Clinton Announcing the Initiative to Streamline Government, Mar. 3, 1993, http://govinfo.library.unt.edu/npr/library/speeches/030393.html; National Performance Review, Creating a Government that Works Better and Costs Less (1993); Congressional Research Service, Implementation of National Performance Review Recommendations (Oct. 27, 1993). Many of these ideas were captured in David Osborne and Ted Gaebler's influential book on reinventing government. *See generally* DAVID OS-

following the Labour Party's victory in 1997, with the creation of the Better Regulation Task Force.[21] The Better Regulation Task Force's mission was to ensure that regulation in the United Kingdom complied with the five Principles of Good Regulation:

> *Proportionate*: Regulators should only intervene when necessary. Remedies should be appropriate to the risk posed, and costs identified and minimized;
>
> *Accountable*: Regulators must be able to justify decisions, and be subject to public scrutiny;
>
> *Consistent*: Government rules and standards must be joined up and implemented fairly;
>
> *Transparent*: Regulators should be open, and keep regulations simple and user friendly; [and]
>
> *Targeted*: Regulation should be focused on the problem and minimize side effects.[22]

In 1998, Neil Gunningham and Peter Grabosky provided a systematic account of "smart" regulation, which they defined as the use of appropriate combinations of policy instruments to achieve a goal.[23] They reaffirmed Ayres and Braithwaite's insight that progress in increasing the effectiveness of regulation requires moving beyond the "regulation-deregulation" dichotomy. They also suggested that a consensus was then emerging in support of the use of non-governmental actors (which may be businesses or non-commercial third parties, depending on the context) as "quasi-regulators" in combination with private incentives and traditional government regulation as the most efficient method of achieving policy goals.[24] Smart regulation therefore requires comparative analysis of the strengths and weaknesses of different policy instruments, and the design of governance institutions tailored to the context in which the targeted social problem arose. The various policy instruments or "tools of government" that might be used to achieve a smart

---

BORNE & TED GAEBLER, REINVENTING GOVERNMENT: HOW THE ENTREPRENEURIAL SPIRIT IS TRANSFORMING THE PUBLIC SECTOR (1993).

21. Better Regulation Commission, Frequently Asked Questions, http://archive.cabinetoffice.gov.uk/brc/faqs.html (last visited June 6, 2009).

22. Better Regulation Task Force, *Principles of Good Regulation* (1998) (revised 2000), http://archive.cabinetoffice.gov.uk/brc/publications/principlesentry.html (emphasis added).

23. GUNNINGHAM & GRABOSKY, *supra* note 9, at 15 (1998).

24. *Id.* at 11-15.

regulation strategy include: direct provision of goods and services by government; direct regulation to achieve social or economic goals; government contracting with private-sector entities; government grants, loans, and loan guarantees; government-sponsored insurance programs; tax incentives; fees and charges; liability laws; and provision of goods or services by quasi-public agencies or government corporations, or through voucher programs.[25] In order to move beyond the simple regulation-deregulation dichotomy, the parties involved must not be limited to government and business, but should include public interest groups, industry associations, independent third-party certification or rating agencies, professionals (including lawyers, accountants, and consultants), and third-party businesses such as private-sector insurance companies.[26]

Although the United States was a leader in developing "smart regulation" strategies under the Clinton Administration, these developments largely came to a halt at the federal level in 2000 when the Bush Administration chose not to build on them, but to return to the "deregulation" branch of the old regulation-deregulation dichotomy.[27] By contrast, exploring new forms of governance has emerged as a major strategy of European Union political leaders and regulators since the launch of the "Lisbon Strategy" in 2000.[28] The Lisbon Strategy was intended to make Europe "the most competitive and dynamic knowledge-based economy in the world capable of sustainable economic growth with more and better jobs and greater social cohesion."[29] The Mandelkern Group was established by the Council of the European Union as a high-level consultative group to develop a "better regulation" strategy for the European Union.[30] In 2001, this was followed by a white paper outlining how the European Union's better regulation strategy would be implemented by requiring the Commission to conduct impact assessments before new legislation is introduced, simplifying existing European regulations, conducting public consultations for all Commission initiatives, and considering alternatives to conventional regulation such as self-regulation or co-regulation.[31]

---

25. LESTER SALAMON, THE TOOLS OF GOVERNMENT: A GUIDE TO THE NEW GOVERNANCE 21 (2002).

26. GUNNINGHAM & GRABOSKY, *supra* note 9, at 93-134.

27. FIORINO, *supra* note 15, at 60, 213-14.

28. Lisbon European Council 23 and 24 March 2000 Presidency Conclusions, EUR. PARL. DOC. PE 289.667 (2000), *available at* http://www.europarl.europa.eu/summits/lis1_en.htm.

29. *Id.* at 12.

30. MANDELKERN GROUP, MANDELKERN GROUP ON BETTER REGULATION, FINAL REPORT 8 (2001), http://ec.europa.eu/governance/better_regulation/documents/mandelkern_report.pdf.

31. *White Paper on European Governance*, COM (2001) 428 final (July 25, 2001).

In order for "smart regulation" to work, however, legislatures and regulators must accurately assess the risks associated with the use of different policy instruments, and the global financial crisis that erupted in 2008 starkly illustrates how difficult that can be.[32] The United Kingdom may have gone further than other countries in embracing "smart" or "light touch" regulation,[33] as evidenced by a 2005 report issued by the Better Regulation Task Force entitled "Regulation-Less is More."[34] During the global financial crisis, the United Kingdom has suffered some of the most severe economic reverses of any country, in large part as a result of financial and real estate bubbles fueled by lax regulation of financial markets.[35] One possible explanation for the apparent failure of "smart" or "light touch" regulation of financial markets in London might be found in the academic literature on behavioral adaptation and risk compensation.[36] However, the analysis of issues such as the optimal regulatory strategy for dealing with systemic risk in global financial markets is beyond the scope of this Article.[37]

The notion of "better regulation" emerged as a result of frustration with the social costs of both unregulated markets and traditional command-and-control regulation, but it requires a high degree of foresight and competence on the part of lawmakers and regulators to succeed. In order to achieve "bet-

---

32. *Curbs on Risky Banking Proposed*, BBC NEWS, Mar. 18, 2009, http://news.bbc.co.uk/2/hi/business/7948791.stm (reporting that the UK financial crisis was due to failure of "light touch" regulation used by Financial Services Authority since 1997).

33. Beginning in the late 1990s, the United Kingdom Labour Government often advocated "light touch" regulation as an intermediate position between deregulation and traditional regulation. *See*, *e.g.*, David Gow & Mark Atkinson, *Blair Plans War on Red Tape*, THE GUARDIAN (LONDON), Nov, 3, 1999, *available at* http://www.guardian.co.uk/business/1999/nov/03/7/.

34. Better Regulation Task Force, Regulation – Less is More (2005), *available at* http://archive.cabinetoffice.gov.uk/brc/upload/assets/www.brc.gov.uk/lessismore.pdf.

35. David Smith, *Gordon Brown Says: London Is Not "Reykjavik on the Thames,"* THE TIMES, Feb. 1, 2009, *available at* http://business.timesonline.co.uk/tol/business/economics/article5627301.ece. Following liberalization of Iceland's banking system in 2003, its main commercial banks grew rapidly by taking foreign deposits and making foreign loans. Following the failure of Lehman Brothers in September 2008, those banks failed, causing the collapse of Iceland's financial system in October 2008. *See generally Iceland: Cracks in the Crust*, ECONOMIST, Dec. 13, 2008, at 11; Media Eghbal, *Global Financial Crisis: Recession Bits into Western Europe*, EUROMONITOR INT'L, Jan. 12, 2009, http://www.euromonitor.com/The_global_financial_crisis_recession_bites_into_Western_Europe.

36. James Hedlund, *Risky Business: Safety Regulations, Risk Compensation, and Individual Behavior*, 6 INJURY PREVENTION 82 (2000).

37. Not all "light touch" regulation ideas are bad ideas. For example, the United Kingdom government created the Child Trust Fund to help children learn about savings and investment by the time they turn 18 by creating investment accounts of £250 at birth for all children born after 2002. Child Trust Fund, http://www.childtrustfund.gov.uk/ (last visited July 9, 2009).

ter regulation," the institutions to be regulated must be analyzed, and appropriate policy instruments must be selected and then harmonized into an integrated framework. Lawmakers and regulators must grasp the logic of established social relations, review a wide spectrum of different policy instruments and incentive systems, be prepared to delegate selected oversight functions to self-regulatory programs, take steps to promote constructive dialogue between regulator and regulated entity, and finally design and implement targeted enforcement programs. Imposing such high standards on lawmakers and regulators may appear unrealistic, especially when contrasted with the relative simplicity of "deregulation" as a reform agenda. In many areas of public policy, however, the shortcomings of both unregulated markets and direct regulation have also been clearly demonstrated.[38] In order to achieve complex, novel social goals such as a significant reduction in security breaches, better regulation strategies may turn out to be like democracy, which Churchill famously noted was "the worst form of government except for all those other forms that have been tried from time to time."[39]

## III. CALIFORNIA'S SECURITY BREACH NOTIFICATION LAW

On April 5, 2002, the Stephen P. Teale Data Center, one of California's two general-purpose data centers, suffered a security breach that was not discovered until May 7, 2002, and state employees were not notified until May 21, 2002.[40] In response, California legislators enacted Senate Bill 1386, which requires that any state agency, person, or business in California disclose that a security breach had occurred to those whose computerized information had been accessed.[41] These notices to individuals whose personal information is exposed by the breach may be delayed if necessary to avoid impeding a criminal investigation.[42] The legislative findings provided in support of Senate Bill 1386 included findings that the risk to the privacy and financial security of individuals as a result of widespread collection of personal information was growing; that the personal information needed to accomplish identity theft exists in many forms and is widely used for a variety of legitimate purposes; identity theft is one of the fastest growing crimes committed in California, which imposes substantial costs on both California consumers and business-

38. *See* FIORINO, *supra* note 15, at 1-25.

39. Winston Churchill, Speech at the House of Commons (Nov. 11, 1947).

40. Personal Information: Disclosure; Breach of Security: Hearing on S.B. 1386 Before the Assem. Comm. on the Judiciary, 2002 Leg. (2002).

41. S.B. 1386, 2002 Leg., Reg. Sess. (Cal. 2002), codified at CAL. CIV. CODE § 1798.82.

42. *Id.*

es; and that rapid notice to consumers that a security breach has occurred may help consumers to minimize the damage that occurs from identity theft.[43]

The legislative history of California's security breach notification law reveals several interesting features. First, that a huge security breach exposed California state payroll data but weeks passed before the victims were notified suggests that legislators were interested not only in reducing the risk of such breaches in the future, but also in getting even: compliance with SBNLs can "shame" companies with bad security. This feature may intensify other incentives pushing companies handling large volumes of sensitive personal data to improve their security.[44] The shaming function of SBNLs is direct and concrete, while any incentive they provide to improve security is indirect and uncertain.

In one way, SBNLs conform to the "smart regulation" model of Gunningham and Grabowsky because enforcement of the laws is delegated to non-governmental parties.[45] The delegation is fraught with peril, however, because it is not made to an independent third party or quasi-governmental agency,[46] but made directly to the regulated entity itself, with no government audit or examination function to assess compliance levels. Even when public resources are committed to policing compliance, "slippage" problems may arise when regulators make ad hoc, inconsistent exceptions in enforcement.[47] When no public resources are committed to policing compliance, then slippage may become the norm.[48]

So while on the surface SBNLs appear to create a huge compliance obligation across the entire U.S. economy, touching all businesses that handle

---

43. S.B. 1386 § 1, 2001-02 Leg., Reg. Sess. (Cal. 2002).

44. Posting of Bruce Schneier to Schneier on Security Blog, Identity-Theft Disclosure Laws, http://www.schneier.com/blog/archives/2006/04/identitytheft_d.html (Apr. 26, 2006 08:11 EST).

45. GUNNINGHAM & GRABOSKY, *supra* note 9, at 93-134.

46. Government corporations such as Freddie Mac and Fannie Mae, or the American National Standards Institute are examples of private organizations that act as quasi-governmental agencies. *See* About Fannie Mae: Our Charter, http://www.fanniemae.com/aboutfm/charter.jhtml; Freddie Mac: Company Profile, http://www.freddiemac.com/corporate/company_profile/; Introduction to ANSI, http://www.ansi.org/about_ansi/introduction/introduction.aspx.

47. PETER MENELL, ENVIRONMENTAL LAW, at xiii (2002).

48. This would not be the case if enforcement resources are supplied by a different regulatory regime. For example, the obligations of publicly listed companies under the Sarbanes-Oxley Act to maintain effective internal controls may contribute to higher levels of compliance with SBNLs than those among non-public companies. *See* 18 U.S.C. § 1514(a) (2006). Analysis of the relationship between SBNLs and Sarbanes-Oxley Act is beyond the scope of this Article.

sensitive personal information, in reality large-scale non-compliance with SBNLs is not only possible but entirely predictable.[49] This is because rational actors are presumed to be deterred by legal prohibitions when the cost of the violation exceeds the benefits they expect to derive from the violation.[50] Because SBNLs do not commit any significant public resources to increase the probability of apprehension and conviction for failures to report breaches, the expected value of apprehension and conviction for many businesses will be equal to zero.

SBNLs draw on several legislative models from environmental law and other forms of social and economic regulation, including "community right to know legislation," "technology-forcing legislation," and strict liability in tort law. "Community right to know" legislation is one of the most important models used. When "information-forcing" legislation, such as CRTK laws that force companies to divulge information they would rather not,[51] is used in combination with direct regulation and other environmental laws to establish a duty to reduce pollution, together they can increase transparency and the effectiveness of government enforcement efforts by providing more avenues for non-governmental organizations such as public interest groups to participate in enforcement processes.[52]

Within the context of environmental law, the shortcomings of CRTK statutes are well known. The most obvious is the problem of requiring regulatory subjects to turn over information that they know will be used to impose sanctions against them in an adversarial relationship with regulators.[53] Even if the mandatory disclosures are made at great cost to the regulated entities, it remains unclear whether information relevant to achieving the underlying policy goal has been provided. In the case of SBNLs, a wealth of information has been disclosed about hundreds of security breaches, but it remains unclear how helpful this information is in analyzing the causes of iden-

---

49. AYRES & BRAITHWAITE, *supra* note 16, at 19 ("A strategy based on persuasion and self-regulation will be exploited when actors are motivated by economic rationality.").

50. ANTHONY OGUS, REGULATION: LEGAL FORM AND ECONOMIC THEORY 91 (2d ed. 2004) (providing the formula for deterrence with criminal law as $pD > U$ where $p$ is the perceived probability of apprehension and conviction, $D$ the costs incurred as a result of apprehension and conviction, and $U$ the benefits of violating the law).

51. *See* Bradley C. Karkkainen, *Information-forcing Regulation and Environmental Governance*, *in* LAW AND NEW GOVERNANCE IN THE EU AND US 298 (Gráinne de Búrca & Joanne Scott eds., 2006) (explaining information-forcing penalties as those that induce disclosure of asymmetrically held information).

52. GUNNINGHAM & GRABOSKY, *supra* note 9, at 63.

53. ROBERT A. KAGAN, ADVERSARIAL LEGALISM: THE AMERICAN WAY OF LAW 241 (2001); Mary Lyndon, *Information Economics and Chemical Toxicity: Designing Laws to Produce and Use Data*, 87 MICH. L. REV. 1795, 1826-28 (1989).

tity theft, or how representative it is of security breaches occurring throughout the American economy, because there are no estimates of who is not disclosing.

SBNLs also incorporate elements of "technology-forcing legislation" by creating an exemption from the duty to provide security breach notices for "encrypted," sensitive personal information.[54] This safe harbor for encrypted data may operate like a "best available technology" requirement in environmental law, where agency guidelines for effluent limitation require the use of "best available technology economically achievable."[55] Such technology-based environmental standards have been widely criticized on many grounds: regulators pressuring industry to adopt new technologies may fail to anticipate correctly future market developments, or how rapidly industries will be able to adapt; rules that are intended to create mandatory minimums or regulatory floors turn into regulatory ceilings that inhibit innovation; they focus on "end-of-pipe" control technologies,[56] diverting attention away from production processes where problems could be completely eliminated; and they compartmentalize regulation, making an integrated, systemic approach to dealing with social problems impossible.[57] The encryption safe harbor in SBNLs appears to be suffering from all these shortcomings. Years after the first SBNL was enacted, encryption technology is still not widely used by or-

---

54. *E.g.*, CAL. CIV. CODE § 1798.29(a) (2009).

55. *See*, *e.g.*, Clean Water Act, 33 U.S.C. § 1311(b)(1)(A) (2006). Agency guidelines for effluent limitation initially had to require the use of "best available technology economically achievable"; this standard was later revised to require the use of "best practicable control technology currently available." *Compare id. with* 33 U.S.C. § 1311(b)(1)(A) (1977).

56. Environmental law technology standards that have been criticized for focusing on downstream "end-of-pipe" technologies instead of upstream changes in productive processes include: Best Practicable Technology (BPT) and Best Available Technology (BAT) requirements from the Federal Clean Water Act, 33 U.S.C. § 1311 (1977); Best Available Control Technology (BACT), the standard applied to new pollution emitting facilities under the federal Clean Air Act, 42 U.S.C. § 7475(a)(4) (2006); Best Conventional Technology (BCT) requirements from the federal Clean Water Act, 33 U.S.C. § 1311(b)(2)(E) (2009); Best Demonstrated Available Technology (BDAT), the federal Clean Air Act standard for new stationary sources of pollution, 42 U.S.C. § 7411(a)(1) (2000); and Lowest Achievable Emission Rate (LAER), the federal Clean Air Act standard for new stationary sources nonattainment areas. 42 U.S.C. § 7501(3) (2000). FIORINO, *supra* note 15, at 73; ENVIRONMENTAL LAW INSTITUTE, BARRIERS TO ENVIRONMENTAL TECHNOLOGY INNOVATION AND USE 8 (1998).

57. STEPHEN G. BREYER, REGULATION AND ITS REFORM 106 (1982); GUNNINGHAM & GRABOSKY, *supra* note 9, at 39; OGUS, *supra* note 50, at 209 (describing regulation based on technology-forcing standards as "specification standards" rather than "performance standards"); Richard B. Stewart, *Economic Incentives for Environmental Protection: Opportunities and Obstacles*, *in* ENVIRONMENTAL LAW, THE ECONOMY AND SUSTAINABLE DEVELOPMENT 185 (Richard L. Revesz, Philippe Sands & Richard B. Stewart eds., 2000).

ganizations with large databases containing sensitive personal information; companies can enjoy the benefit of the safe harbor by the use of weak encryption technologies without adopting a systemic, risk management-based approach to information security; and they focus attention on the adoption of a single security technology to mitigate harm rather than the overall process of securing a system or networks of systems.

Encryption appears to have a glamour that other security technologies may lack, making references to it even more likely to distract from the underlying problems:

> Too many engineers consider cryptography to be a sort of magic security dust that they can sprinkle over their hardware or software, and which will imbue those products with the mythical property of "security." Too many consumers read product claims like "encrypted" and believe in that same magic security dust. Reviewers are no better, comparing things like key lengths and on that basis, pronouncing one product to be more secure than another.
>
> Security is only as strong as the weakest link, and the mathematics of cryptography is almost never the weakest link . . . . Security is a broad stockade: it's the things around the cryptography that make the cryptography effective.[58]

While many legislators, product vendors and businesses seem to hope that encryption will be the "silver bullet" that can solve information security problems, encryption has at least two fundamental limitations as a security technology.[59] First, encryption can protect data at rest and in motion but cannot protect data while the data is actually being processed. Second, encryption is only as secure as the weakest link in the system within which it is deployed.[60]

SBNLs have also borrowed a regulatory model from modern tort law: strict liability.[61] The legal theory of liability without fault for releasing products into the stream of commerce that are later found to be defective was first set forth in a concurrence by Justice Traynor in the famous exploding Coke bottle case.[62] The California SBNL establishes a form of strict liability

58. BRUCE SCHNEIER, PRACTICAL CRYPTOGRAPHY, at xviii (2003) (cited in JOHN R. CHRISTIANSEN, AN INTEGRATED STANDARD OF CARE FOR HEALTHCARE INFORMATION SECURITY: HIPAA, RISK MANAGEMENT AND BEYOND (2005)).

59. DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY 309 (1999).

60. *Id.*

61. *See generally* DAN B. DOBBS, THE LAW OF TORTS 969-1046 (2000).

62. Escola v. Coca-Cola Bottling Co., 150 P.2d 436, 462 (Cal. 1944) (Traynor, J., concurring).

for database owners by requiring that they "shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data"[63] without any reference to any fault on the part of the database owner in contributing to the breach. As a result, database owners may be liable for harm caused by problems with the data-processing services they provide incidental to the provision of other goods or services, a clear departure from the common-law standard of care for services. In the absence of express contract terms to the contrary, services are normally provided with an implied warranty of "workmanlike services." This warranty resembles a negligence standard of care, while the warranty of merchantability, which is implied in transactions involving tangible goods, resembles a strict liability standard.[64]

Many states that used the California law as a model modified this provision to require notice only if there was a substantial risk that the breach might result in harm to the individuals whose personal information was exposed.[65] For example, Connecticut enacted a SBNL in 2006 which provides that "notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed."[66] But even these "risk-based" notification requirements adjust the database owner's duty based on the risk to the person whose information was exposed, and they do not take account of whether the database owner suffered the breach despite having implemented current industry best practices.

A stronger incentive for database owners to implement information security best practices could have been created by diminishing the liability of the

---

> Even if there is no negligence, however, public policy demands that responsibility be fixed wherever it will most effectively reduce the hazards to life and health inherent in defective products that reach the market . . . . The injury from a defective product does not become a matter of indifference because the defect arises from causes other than the negligence of the manufacturer.

*Id.*

63. CAL. CIV. CODE § 1798.29(a) (2009).

64. DOUGLAS WHALEY, PROBLEMS AND MATERIALS ON THE SALE AND LEASE OF GOODS 183 (5th ed. 2008).

65. *See generally* Michael E. Jones, *Data Breaches: Recent Developments in the Public and Private Sectors*, 3 J.L. & POL'Y FOR INFO. SOC'Y 555 (2007) (distinguishing different SBNLs with regard to whether they use "acquisition-based triggers" and "risk-based triggers" for notification).

66. CONN. GEN. STAT. § 36a-701b(b) (2008).

database owner whenever it had taken all feasible steps to prevent the security breach from occurring. The "end-of-pipe" perspective on the problem, which emphasizes mitigating damages after the problem has occurred instead of reducing the risk that the problem will occur in the first place, is also reflected in the California Office of Privacy Protection's RECOMMENDED PRACTICES FOR NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION.[67]

In separate legislation enacted in 2004, California recognized a general duty of database owners to secure sensitive personal information by requiring that any "business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[68] This legislation does not provide any guidance with regard to what might constitute "reasonable security procedures," nor does it refer to the SBNL enacted earlier, although a plausible interpretation of the two statutes suggests that encryption of sensitive data should meet the reasonable security procedure standard.[69] Outside the context of California's statutory duty to implement and maintain reasonable security procedures and practices, other regulations have provided more guidance with regard to what might constitute reasonable security procedures, and they may prove helpful in interpreting the California duty to implement reasonable security procedures.[70] These include the Federal Information Security Management Act,[71] the Gramm-Leach-Bliley Act Safeguards Rule,[72] and the Health Insurance Portability and Accountability Act Security Rule.[73]

Security breach notification laws do not take into account precautions taken by database owners before any breach occurs. As a result, an organization with a sophisticated information security policy that is subject to more vicious attacks than other organizations may suffer a breach and bear the same liability as organizations with a complete disregard for information se-

---

67. *See* CALIFORNIA OFFICE OF PRIVACY PROTECTION, CAL. DEP'T OF CONSUMER AFFAIRS, Recommended PRACTICES FOR NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION (2008), *available at* http://www.oispp.ca.gov/consumer_privacy/pdf/secbreach.pdf.

68. CAL. CIV. CODE § 1798.81.5(b) (2009).

69. Chad Pinson, *New Legal Frontier: Mass Information Loss and Security Breach*, 11 SMU SCI. & TECH. L. REV. 27, 39 (2007).

70. *See generally* WINN & WRIGHT, *supra* note 5, at § 17.

71. Pub. L. 107-347, 116 Stat. 2946 (codified as 44 U.S.C. §§ 3541-3549 (2006)).

72. Standards for Safeguarding Customer Information, 16 C.F.R. §§ 314.1-.5 (2009).

73. 45 C.F.R. §§ 160, 162, 164; *see also* WINN & WRIGHT, *supra* note 5, at § 14.03[P][2].

curity issues. The problem may be even worse than that: because enforcement of SBNLs depends almost entirely on self-regulation by owners of databases, then as a practical matter, organizations with good enough security policies to realize that they have a problem are exposed to much greater liability than organizations that are truly clueless. In other words, because SBNLs implicitly require database owners to be sophisticated enough to recognize that problems exist, they do not have any mechanisms for dealing with smaller, less sophisticated organizations that do not even realize they are suffering security breaches.

Liability for security breaches covered by SBNLs can be measured by the cost of providing notices and other remedial actions such as offering credit report monitoring services. In 2005, the Gartner Group estimated that the direct cost of a security breach of a single customer record is from $90 up to $1,500.[74] In 2007, the U.S. Government Accountability Office found that the total cost of a single breach averaged $1.4 million.[75] In 2009, the Ponemon Institute reported that the average cost of data breaches had reached $6.3 million, or $197 per record breached, although the report did not explain how this cost was divided among notices, remediation, compensation to victims and other costs associated with a data breach.[76]

That database owners should be held to a strict liability standard rather than a negligence standard with regard to security breaches is even more surprising, given that the licensors of the database software they use have generally been able to avoid any liability for inadequate security. Michael Scott observed:

---

74. JOHN PESCATORE & AVIVAH LITAN, DATA PROTECTION IS LESS COSTLY THAN DATA BREACHES 2 (2005), *available at* http://www3.villanova.edu/gartner/research/130900/130911/130911.pdf.

75. U.S. GOV'T ACCOUNTABILITY OFFICE, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN, GAO 07-737 (2007), at 34, *available at* http://www.gao.gov/new.items/d07737.pdf.

> There are also the costs associated with actual notifications—potentially including printing, postage, legal, investigative, and public relations expenses. Although comprehensive data on these costs do not exist, a 2006 Ponemon Institute survey of companies experiencing a data breach found that 31 companies that responded incurred an average of $1.4 million per breach, or $54 per record breached, for costs related to mailing notification letters, call center expenses, courtesy discounts or services, and legal fees.

*Id.*

76. THE PONEMON INSTITUTE, 2008 ANNUAL STUDY: U.S. ENTERPRISE ENCRYPTION TRENDS 2 (2008), *available at* http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008_Annual_Study_US_Encryption_Trends_280308.pdf.

> Software vulnerabilities cost businesses and consumers tens of billions of dollars each year. Every day brings news of freshly discovered security flaws in major software products. While Microsoft, due to its prominence in the operating system market, gets the brunt of the criticism for these flaws, there are many other companies whose software is also targeted for security-related complaints. Yet, software vendors have traditionally refused to take responsibility for the security of their software, and have used various risk allocation provisions of the Uniform Commercial Code (U.C.C.) to shift the risk of insecure software to the licensee. There were a few early cases in which licensees sought to have courts hold vendors liable for distributing defective software. These cases were unsuccessful.[77]

The exemption of software developers from liability for inadequate security is due to a variety of factors. Decades ago, software development was seen as a service rather than a product.[78] More recently, courts have been reluctant to apply products liability concepts to software on the grounds that it is not a tangible product.[79] In addition, vendors that market products to assist database owners with SBNL compliance are generally selling products to assist in monitoring vulnerabilities and generating reports, not products to remove vulnerabilities.[80] So companies with databases of sensitive personal information cannot simply shift their exposure under SBNLs by contract to other enterprises such as database software vendors, who appear to be in a much better position to reduce the incidence of security breaches.

California's pioneering SBNL was a radical innovation that is influencing privacy and information legislation around the world.[81] It creates an important new consumer right to receive information in an area in which consumers formerly had no entitlement at all. While the SBNL may have achieved its drafters' goals of imposing a modest sanction on database owners who fail to safeguard the sensitive personal information of their customers, its value as a

---

77. Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 426 (2008) (citations omitted).

78. *Id.* at 461.

79. *Id.* at 464; RESTATEMENT (THIRD) OF TORTS § 19, cmt. d, Reporter's Note (1998).

80. *See*, *e.g.*, Agiliance Product Overview, http://www.agiliance.com/products/overview.html (last visited May 30, 2009).

81. *See, e.g.*, *Commission Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC, Directive 2002/58/EC, and Regulation (EC) No. 2006/2004*, COM (2007) 698 final (Nov. 13, 2007), *available at* http://ec.europa.eu/information_society/policy/ecomm/doc/library/proposals/dir_citizens_rights_en.pdf; AUSTRALIAN LAW REFORM COMMISSION, Introducing a mandatory data breach notification scheme (Aug. 11, 2008), available at http://www.alrc.gov.au/media/2008/mbn6.pdf.

model for information security law reforms is uncertain at best. Due to its limited scope, ex post focus on notice of problems rather than an ex ante focus on effective solutions, failure to provide concrete incentives to product developers to reduce risks at a systemic level, and lack of any public enforcement system, California's SBNL provides only limited, distorted incentives to database owners to act decisively to reduce the volume of security breaches.

## IV. CHALLENGES OF REDUCING SECURITY BREACHES

Looking at SBNLs as a bundle of information-forcing, technology-forcing and strict liability rules, it is clear that they suffer from serious structural flaws. This form of regulation might be adequate, however, if it were applied to an easier problem than improving security for collections of sensitive personal information. As with the causes of pollution in the natural environment, the causes of bad information security are too complex to rectify with such flawed legislative strategies. Just as it has become apparent in environmental law that pollution is a symptom of the larger problem of unsustainable economic development, it should also be apparent that security breaches are symptoms of larger technical and institutional problems.

In part, the technical problems are caused by the fact that applications are being developed and deployed without adequate attention to security faster than information security solutions can be created and applied.[82] The problem of low returns for investments in information security emerged decades ago when computing became a popular phenomenon, and computer systems were no longer isolated in cold rooms with access denied to all but a select few.[83] Less sophisticated users of information technology products are not in a good position to appreciate the risks caused by lack of attention to computer security, and they are easily frustrated by any diminution in func-

---

82. In January 2009, the SANS (SysAdmin, Audit, Network, Security) Institute announced that

> experts from more than 30 US and international cyber security organizations jointly released the consensus list of the 25 most dangerous programming errors that lead to security bugs and that enable cyber espionage and cyber crime. Shockingly, most of these errors are not well understood by programmers; their avoidance is not widely taught by computer science programs; and their presence is frequently not tested by organizations developing software for sale.

Bob Martin, Experts Announce Agreement on the 25 Most Dangerous Programming Errors - And How to Fix Them, http://www.sans.org/top25errors/ (last visited May 30, 2009).

83. Lewis University, A Brief History of Information Security, *available at* http://www.lewisu.edu/academics/msinfosec/history.htm (last visited June 25, 2009).

tion associated with increased security.[84] Information asymmetries between producers and consumers of information technology products and services, and strong network effects that can easily produce a "first mover" effect,[85] have resulted in chronic failures in information technology product markets evidenced by the externalization of many of the costs of bad security onto third parties.[86] These market failures are exacerbated in part by underinvestment in basic information security research because basic research has many of the features of a public good.[87] In addition, to the extent that information security is created with products and services distributed within networked markets, adoption of those products and services will be hindered whenever end users fear their use may fragment existing networks through lack of standardization or because competition among different standards fails to produce a single dominant standard strong enough to create a new network.[88]

This institutional problem grows out of conflicts among the current social norms of business administration and legislative mandates that require significant changes in those norms. Most businesses have not yet modified their organizational norms to integrate "operational risk"[89] or "information assurance"[90] policies systematically into all management systems.[91] Until the 2008 financial crisis, many American consumers appeared to think access to

84. NATIONAL RESEARCH COUNCIL ET AL., TRUST IN CYBERSPACE 182 (Fred Schneider ed., 1999).

85. First-mover advantages are created when an organization has a technological lead on its competitors, can block competitors' access to certain assets, and its customers have high switching costs. Marvin B. Leiberman & and David B. Montgomery, *First-Mover Advantages*, 9 STRATEGIC MGMT. J. 41, 41-58 (Summer 1988). First-mover advantages frequently arise in markets defined by networks. CARL SHAPIRO AND & HAL R. VARIAN, INFORMATION RULES 168-69 (1999).

86. NATIONAL RESEARCH COUNCIL ET AL., *supra* note 84, at 251.

87. *Id.* at 244.

88. SHAPIRO & VARIAN, *supra* note 85, at 168-69.

89. Operational risk was originally defined to capture all sources of risk other than market risk and credit risk. Rob Jameson, *Operational Risk: Getting the Measure of the Beast*, RISK, Nov. 1998, at 38. See *infra* Part IV for further discussion of the definition of operational risk.

90. Information assurance is defined by the National Security Agency as the "protection of information systems against unauthorized access to, or modification of, information, whether in storage, processing or transit, and protection against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats." National Security Agency, Frequently Asked Questions: Terms and Acronyms, http://www.nsa.gov/about/faqs/terms_acronyms.shtml (last visited May 30, 2009).

91. David Farmer, *Operational Risk Management and the Risk Governance Challenge*, GT NEWS (May 20, 2008), *available at* http://www.gtnews.com/article/7268.cfm ("While regulatory developments, such as Basel II and Sarbanes Oxley, have accelerated the implementation of enterprise risk management frameworks, operational risk management remains relatively unchanged with many organisations steaming ahead like the Titanic.").

credit was a more fundamental human right than information privacy and were happily complicit in the commodification of their sensitive personal information because it reduced barriers to obtaining the credit necessary to consume at will.[92] Most vendors of information assurance products and services have little or no incentive to make the social norm reform dimension of the problem clear because, at least in the short term, they can often sell more of their products if they can convince their customers that their product provides a technological "silver bullet" to solve their problems.

In some economic sectors, traditional direct regulation has been used to pressure businesses to overcome social norms of inattention to operational risk. For example, during safety and soundness examinations of regulated depository institutions, bank examiners consider market risk, credit risk, and operational risk.[93] Even though operational risk has traditionally received less attention than market and credit risk,[94] it has nevertheless received more attention in financial services industries than in most other industries. In the Basel Committee on Banking Supervision, International Convergence of Capital Measurement and Capital Standards (Basel II Guidelines), "operational risk" is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."[95] One reason operation risk management is less well developed than market or credit risk management for financial institutions is the dearth of publicly available operational risk data.

> This is in direct contrast to market risk and credit risk, for which data are widely available . . . . Although operational risk was originally defined to capture all sources of risk other than market risk and credit risk, several more specific definitions of operational risk

92. *See generally* LENDOL CALDER, FINANCING THE AMERICAN DREAM: DEBT, CREDIT, AND THE MAKING OF A CONSUMER SOCIETY 1890-1940 (1999) (discussing the centrality of easy credit to American popular culture since colonial times).

93. 2-37 Banking Law § 37.04.

94. Philip Alexander, *Risk Management Bites Back*, BANKER, Oct. 1, 2008, *available at* http://www.thebanker.com/news/fullstory.php/aid/6049/Risk_Management_bites_back_.html ("Many practitioners suggest that . . . operational risk [management] has been the poor relation of [other forms of risk management].").

95. BASEL COMMITTEE ON BANKING SUPERVISION, INTERNATIONAL CONVERGENCE OF CAPITAL MEASUREMENT AND CAPITAL STANDARDS 134 (2004), *available at* http://www.bis.org/publ/bcbs107.pdf; *see also* BASEL COMMITTEE ON BANKING SUPERVISION, SOUND PRACTICES FOR THE MANAGEMENT AND SUPERVISION OF OPERATIONAL RISK (2003), *available at* http://www.bis.org/publ/bcbs96.pdf.

> have become well known, [most notably, the definition in the Basel II Guidelines].[96]

Effective management of operational risk is integral to the business of banking and to institutions' roles as financial intermediaries. Although operational risk is not a new risk, deregulation and globalization of financial services—together with the growing sophistication of financial technology, new business activities and delivery channels—are making the operational risk profiles of institutions (i.e. the level of operational risk across an institution's activities and risk categories) more complex.[97]

Outside of industries where outside auditors are required to examine how operational risks are handled, there has been much less management attention to operational risk issues, although there is evidence this may slowly be changing. Panjer notes:

> Operational risk has only in recent years been identified as something that should be actively measured and managed in a company in order to meet its objectives for stakeholders, including shareholders, customers, and management . . . . Operational risk is becoming a major part of corporate governance of companies.[98]

Just as with regulated financial institutions, the operational risk profiles of businesses throughout the economy are increasing in complexity as the use of information technology becomes pervasive within business administration systems.[99] After the Sarbanes-Oxley Act[100] imposed new obligations on executives of publicly listed companies to maintain effective internal controls, publicly listed companies in the United States are now under an obligation similar to that of regulated financial institutions to manage operational risk.[101] Yet American businesses that are not publicly listed companies may have few concrete incentives to sort out competing vendor claims, identify current best practices, and embark on a program of rigorously implementing best

96. HARRY H. PANJER, OPERATIONAL RISKS: MODELING ANALYTICS 3, 5 (2006).

97. Internet Ratings-Based Systems for Corporate Credit and Operational Risk Advanced Measurement Approaches for Regulatory Capital, 68 Fed. Reg. 45949 (Aug. 4, 2003).

98. PANJER, *supra* note 96, at 3, 5.

99. GUY BUNKER & GARETH FRASER-KING, DATA LEAKS FOR DUMMIES 10-20 (2009).

100. 18 U.S.C. § 1514(a) (2009).

101. Analysis of Sarbanes-Oxley internal control requirements is beyond the scope of this Article. *See generally* HAROLD S. BLOOMENTHAL, SARBANES-OXLEY ACT IN PERSPECTIVE (2003).

practices.[102] According to a 2005 survey cited by the Better Business Bureau, small businesses in America generally do not understand the true economic impact of information security exposures or the nature of the threats they need to manage against, and they tend to be much more reactive than proactive in their thinking about information security.[103] The volume of security breaches reported by major enterprises and government agencies in recent years indicates that small businesses are not the only organizations that are not dealing effectively with information assurance challenges.[104]

For any business of any size not currently required to focus on operational risk, the cost of adopting for the first time a systematic approach to operational risk management can be enormous, while the rewards may be remote and uncertain. The academic literature on "business process reengineering" (BPR) has exhaustively documented the costs and benefits of achieving lasting change in organization values as a strategy for improving a firm's competitive position.[105] While the central focus of BPR is identifying and strengthening the value-creating activities within a firm,[106] BPR also normally includes a shift to adaptive management processes that provide a framework within which comprehensive risk management becomes feasible.[107]

Few businesses will undertake a process as difficult, expensive and uncertain as BPR without a powerful external trigger.[108] In order for SBNLs to provide such a trigger ex ante, the cost of compliance would have to appear to managers to be greater than the cost of enforcement sanctions discounted

---

102. *See*, *e.g.*, Anthony Savvas, *UK Security Bodies Form Security Awareness Forum*, COMPUTER WKLY, Feb. 13, 2008 ("According to the Forum, one of the biggest problems facing organisations and individuals is a lack of information security awareness, with people either not knowing about, ignoring or circumventing security processes and technical countermeasures.").

103. Better Business Bureau, Small Business Mistakes and Vulnerabilities, http://www.bbb.org/us/corporate-engagement/small-business-mistakes/ (last visited May 30, 2009).

104. *See*, *e.g.*, Brian Krebs, *Security Fix - Data Breach Reports up 69 Percent in 2008*, WASH. POST, June 30, 2008, http://voices.washingtonpost.com/securityfix/2008/06/data_breach_reports_up_69_perc_1.html; Andrew Sparrow, *'Inexcusable' Security Breaches Still Occurring, Says Information Commissioner*, THE GUARDIAN, Apr. 22, 2008, *available at* http://www.guardian.co.uk/politics/2008/apr/22/whitehall.voluntarysector/.

105. *See generally* MICHAEL HAMMER & JAMES CHAMPY, REENGINEERING THE CORPORATION (1993).

106. MICHAEL PORTER, COMPETITIVE ADVANTAGE (1985).

107. Enid Mumford, *Risky Ideas in the Risk Society*, 11 J. INFO. TECH. 321-31 (1996). Adaptive management systems, also known as PDCA [Plan-Do-Check-Act] Cycles, are discussed further *infra* Part V.

108. HAMMER & CHAMPY, *supra* note 105, at 149-50.

by the probability of enforcement action. If the managers of most businesses, especially those that are not public companies, believe the probability that unreported security breaches will be detected is negligible, then the cost of compliance will always be higher than the cost of sanctions. By contrast, SBNLs may provide a significant trigger ex post for BPR in companies that suffer a data breach that attracts widespread attention, whether through voluntary disclosure or otherwise, because of the reputational harm caused by disclosure. While dozens or even hundreds of American businesses that have suffered data breaches that resulted in widespread public controversy and criticism may have undertaken BPR in order to achieve lasting changes in organization norms and lasting improvements in information security, it is unclear how many of the hundreds of thousands of American businesses that have not suffered such public humiliations have been similarly motivated.

One reason that SBNLs create weak incentives for change in business social norms is that they apply to enterprises in all sectors of the economy but do not designate a regulatory authority or provide any mechanisms for consistent, vigorous enforcement. Law reforms similar in substance to SBNLs targeting specific industry sectors and supported by strong government funded enforcement efforts might have much greater impact within those industries. For example, in 2005, federal bank and thrift regulatory agencies jointly issued regulations requiring depository institutions in the United States to provide notice of security breaches to their customers.[109] Depository institutions cannot operate without a license, which is granted subject to an ongoing duty to submit to ongoing government examinations.[110] Financial regulators communicate their regulatory proprieties by providing management of depository institutions with updated examination guidelines containing detailed explanations of their standards and then conducting examinations based on those new standards. If financial regulators believe security breach notices are important, they have all the regulatory levers they need to cause depository institutions to become scrupulously attentive to the problems of detecting security breaches and sending notices. By contrast, general business and commercial activities are regulated by private law, and the rights and obligations of the parties are normally enforced through private litigation. As a result, there is no regulatory authority in the U.S. with a clear mandate to investigate information security risk management policies or enter into negotiations with management of most American

109. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (Mar. 29, 2005).

110. RICHARD SCOTT CARNELL, JONATHAN R. MACEY, & GEOFFREY P. MILLER, THE LAW OF BANKING AND FINANCIAL INSTITUTIONS 73-74 (4th ed. 2009).

businesses regarding necessary changes to achieve compliance with SBNLs.[111]

Within the market for information security products, self-regulatory institutions are not yet well enough developed to take the place of direct government regulation. Information security is a new industry dealing with new problems that continue to evolve at a rapid pace. The most concrete, applied information about improving information security is generally provided to businesses by product and service vendors trying to sell something, creating a potential conflict of interest between teacher and student. In more mature industries, a wide range of public and private institutions normally exist that can offer more disinterested information and training to businesses. These include the Better Business Bureau, local chambers of commerce, various trade associations, and in agriculture, agricultural extension offices maintained with public funds. In markets for information security products and services, these "third sector" institutions are fewer, and those that exist are much less mature. Smart regulation advocates would predict that investment of public resources in educational outreach organizations together with investment in enforcement is likely to have a much greater impact on compliance than investment in either enforcement or educational outreach alone.[112]

While there are no national statistics on the use of encryption products by American businesses, anecdotal information suggests that sales of encryption software and business use of encryption technologies have increased only slowly since the first SBNL was enacted in 2003.[113] This suggests that the "safe harbor" in SBNLs for enterprises that encrypted sensitive data before any breach occurred has either provided very weak incentives to invest in encryption technologies, or that the "total cost of ownership" of encryption technologies may be higher than legislators believed when they created the safe harbor. If the cost of using encryption technologies in a manner that significantly reduces the risk of harm when a security breach occurs is higher than legislators realized, it may be because few business software applications

111. The Federal Trade Commission has been making tentative steps in that direction, but lacks a clear statutory basis for doing so. For discussion of Federal Trade Commission (FTC) information security enforcement actions see WINN & WRIGHT, *supra* note 5, § 17.06[E]. *See also* Michael D. Scott, *The FTC, The Unfairness Doctrine and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 173 (2008).

112. GUNNINGHAM & GRABOSKY, *supra* note 9, at 50-56, 60-65.

113. While attending the RSA 2009 conference in April 2009, the author asked representatives of half a dozen major vendors of encryption products about trends in the sales of their products. All reported slow but steady increases, and rejected the suggestion that SBNLs had fueled a sharp increase in demand for encryption products.

for processing data already incorporated encryption technologies in 2003, and it has proven difficult to add encryption to software products or information systems without creating new problems.[114] It may also be because it is difficult to make effective use of a single technology such as encryption unless it is embedded in a larger overhaul of management processes and information technology systems characteristic of BPR. For example, in order to achieve significant reductions in the risk of data breaches, an enterprise must normally:

> Create data-protection policies recognizing different levels of security for different types of data and provide ongoing staff training to support its implementation;
>
> Apply those policies by identifying data that requires higher levels of security, and identifying all places where sensitive data has been stored;
>
> Restrict access to sensitive data on an "as needed" basis through the use of access controls and encryption of stored data and data during transmission;
>
> Implement policies governing archived data, including destruction of data that is no longer needed or which may not be preserved;
>
> Take steps to block the storage of sensitive data on portable devices unless access to the data is authorized and the data can be encrypted; [and]
>
> Continuously review and update data-protection policies in light of new threats, new technologies and new business processes.[115]

Market pressures to create, store, and share as much data as possible without regard to security issues are intense, and they certainly appear to be strong enough to overwhelm whatever impact modest law reforms such as SBNLs may have on business incentives to safeguard the sensitive personal information they control. The cost of technologies used to create, store, and share data continues to fall, while the development of new business models offer tangible, immediate rewards for sharing and reuse of sensitive data.[116]

Over the last half century, the use of business information systems has exploded, transforming administrative systems and resulting in the collection, storage and use of unprecedented volumes of data of every conceivable type.

---

114. *See supra* note 113.
115. GUY BUNKER & GARETH FRASER-KING, *supra* note 99, at 26, 375-78.
116. *Id.* at 10-20.

In recent decades, networks connecting separate business information systems have also grown explosively. The main "driver" for this increased business use of data has been the search for short-term competitive advantage, while too often, too little emphasis has been placed on information system security. This is hardly surprising, given the difficulty of securing open computer networks such as the Internet and the absence of a clear liability scheme requiring attention to information security. Regulators trying to force businesses to internalize the costs of better information security face a task equivalent to turning the Queen Mary: achieving even modest improvements in business orientation may require major changes in the way business information systems are developed and used. SBNLs target only one small piece of this larger problem, leaving in place many of the market failures and perverse incentives that fueled the growth of the problem in the first place. If reducing security breaches is a legitimate and important policy goal, then a very different legislative approach may be required to achieve it.

## V. CAN SBNLS GET "BETTER?"

A "better regulation" approach to the challenge of incorporating information security risk assessments into management processes would look for the combination of policy instruments most likely to achieve that result. Ayres and Braithwaite noted that enforcement regimes that are too harsh or too permissive are both likely to fail, while regimes that emphasize public-private collaboration and selectively resort to punitive enforcement strategies in response to evidence of willful non-compliance are generally most likely to achieve positive outcomes.[117] SBNLs provide no framework within which public-private collaboration can take place to improve compliance over time; rather, companies are left to navigate the maze of competing information security product vendor claims with few reliable standards for guidance. SBNLs provide most businesses with few positive incentives to encourage disclosure but many negative incentives to discourage it.[118] Furthermore, SBNLs establish an inequitable strict liability regime because when breaches occur they do not distinguish between companies that implement information security best practices and those that show a reckless disregard for the security of sensitive data. The severity of the sanctions imposed in terms of the cost of providing notices is a function of the volume of data exposed, not the wrongfulness of the conduct that led to the breach, so some companies

117. AYRES & BRAITHWAITE, *supra* note 16, at 40-41.

118. The problem is well recognized with regard to environmental "right-to-know" laws. *See*, *e.g.*, Mary L. Lyndon, *supra* note 53, at 1826-28.

may suffer a sanction that is punitive. In other words, SBNLs completely fail to meet the standard of "responsive regulation."

From the perspective of policy rather than political expediency, what would a "responsive regulation" framework designed to reduce security breaches by improving information security practices at the firm level look like? It would most likely be made up of a variety of policy instruments designed to complement each other, which would likely include strategies to increase voluntary compliance and self-regulation as well as direct regulations providing for some form of ex ante audit or examination functions and ex post public enforcement. For example, Congress might decide to recognize that customers, suppliers and employees of businesses are entitled to expect that sensitive information will be handled responsibly by establishing a legally enforceable duty on the part of database owners to take reasonable precautions to prevent sensitive data from being accessed without authorization. The Federal Trade Commission (FTC) could then be given the authority to issue regulations to clarify essential elements of this new duty such as what constitutes "reasonable precautions" and "sensitive data" and "unauthorized access." Just as independent self-regulatory organizations[119] perform essential functions in the regulation of securities markets and in assessing whether products conform to technical standards,[120] FTC regulations could recognize a role for independent certification authorities in information security markets, and create a presumption that "reasonable precautions" have been taken by businesses whose information security has been certified compliant with a recognized industry standard.

This approach to reducing the incidence and severity of security breaches would solve several problems associated with SBNLs: it would establish the general, foundational duty of information assurance necessary to support the operation of a "right-to-know" regulation; it would end the piecemeal, sectoral approach currently taken to information security regulation in the United States and establish a uniform, minimum standard for all enterprises that handle sensitive data, not just those in regulated industries; and it would not mandate the use of a particular technology but allow the meaning of "reasonable precautions" to be based on risk assessments; and it would grant an agency authority to enforce the duty.

---

119. Under U.S. securities law, the National Association of Securities Dealers and stock exchanges such as the New York Stock Exchange are recognized as "self-regulating organizations" that regulate their members. 15 U.S.C. § 78s (2009); *see also* GUNNINGHAM & GRABOSKY, *supra* note 9, at 65-66.

120. NATIONAL RESEARCH COUNCIL, STANDARDS, CONFORMITY ASSESSMENT, AND TRADE: INTO THE 21ST CENTURY 17 (1995).

Smart regulation is intended to optimize the structure and content of regulation in order to increase its effectiveness. Evidence is clear in other areas of social regulation that this requires an integrated approach to the interplay between legislation, enforcement, and social norms.[121] An integrated approach requires a balanced combination of direct regulation in the form of a statutory duty of information assurance combined with appropriate levels of funding for public investigation and enforcement efforts, indirect regulation in terms of private liability to data subjects for harm caused by security breaches, enforced self-regulation in the form of independent third-party audits of adaptive management systems, and self-regulation in the form of voluntary industry-based standards and education programs. Clarification of the duty and funding for enforcement would begin to tip the balance of the cost of compliance versus probability of enforcement; under such circumstances, caps on liability in private litigation could be justified. Many standards conformity-assessment authorities already exist, and government regulators could play a role in recognizing those whose competence and independence meet minimum standards to overcome information asymmetries between businesses needing conformity certification and certification providers. With widespread use of adaptive management systems to implement comprehensive information technology risk management policies, the nature of business requirements for information assurance products and services might be clarified to the point where greater standardization of information assurance technologies becomes possible. Such standardization would increase competition among vendors and reduce barriers to adoption of comprehensive risk management strategies by less sophisticated, private companies that currently have little or no awareness of information assurance issues. Voluntary industry efforts to provide educational outreach could complement publicly subsidized "information assurance extension office" educational outreach efforts. This integrated approach is based on an ex ante assessment of the causes of the underlying problem of poor information security practices, and it focuses on making large-scale compliance feasible.

Confronted with the complex, multi-polar institutional framework of business information systems, the California legislature asserted jurisdiction over only two parties and crafted a bi-polar solution that resembles the holding of a case more than it resembles modern regulation: California citizens were given a right of notice of problems occurring at businesses serving them. Given the limited impact that SBNLs have had to date in pressuring businesses to make fundamental changes in their information security prac-

121. GUNNINGHAM & GRABOSKY, *supra* note 9, at 56-60.

tices, the most obvious next step for the California legislature is to create a private cause of action to allow California citizens against businesses suffering security breaches that affect their sensitive personal information.[122] Such a change would be completely consistent with the American regulatory style that relies heavily on public and private litigation to achieve regulatory objectives.[123] The social consequences of such a regulatory approach are well known: unpredictable and inconsistent outcomes in different courts, imposition of high litigation costs on regulated entities in addition to compliance costs, defensive posturing by regulated entities in advance of any litigation, erosion of trust, and loss of opportunities for constructive engagement among stakeholders.[124] Given the complexity of the causes of current information-security problems of American businesses and the current shortage of cost-effective solutions to those problems, the costs of a more adversarial strategy seem very likely to outweigh the benefits of a more flexible, collaborative approach.[125]

An adversarial approach to improving the security of business information systems was recently tried with the Fair and Accurate Credit Transactions Act ("FACTA") credit card receipt rule, and the result was a flood of class action lawsuits with the imposition on businesses of major litigation costs, resulting in negligible improvements in information security.[126] In 2003, Congress enacted "technology-forcing" legislation[127] to require retail merchants to modify point-of-sale systems to block out expiration dates and most digits in credit card numbers.[128] A 2007 deadline was set, and a private cause of action together with statutory damages was created.[129] The result has been hundreds of class action lawsuits, and a flood of judicial decisions that produced a bewildering array of results.[130] In response to the tidal wave of

122. *See*, *e.g.*, Sharona Hoffman & Andy Podgurski, *Securing the HIPAA Security Rule*, J. INTERNET L., Feb. 2007, at 6 (advocating a private cause of action for violations of the HIPAA Security Rule).

123. KAGAN, *supra* note 53, at 182.

124. *Id.* at 198-206.

125. William H. Simon, *Toyota Jurisprudence: Legal Theory and Rolling Rule Regimes*, *in* LAW AND NEW GOVERNANCE IN THE EU AND THE US (Gráinne de Búrca & Joanne Scott eds., 2006).

126. WINN & WRIGHT, *supra* note 5, § 14.03[C].

127. *See generally* Alan S. Miller, *Environmental Regulation, Technological Innovation, and Technology-Forcing*, 10 NAT. RESOURCES & ENV'T 64 (1995) (defining "technology-forcing" legislation).

128. 15 U.S.C. § 1681c(g)(1) (2009).

129. 15 U.S.C. § 1681c(g)(3) (2009).

130. *E.g.*, Ramirez v. Midwest Airlines, Inc., 537 F. Supp. 2d 1161 (D. Kan. 2008); Vasquez-Torres v. StubHub, Inc., No. 07-CV-1328-FMC(FFMx), 2008 U.S. Dist. LEXIS 22503 (C.D. Cal. Mar. 4, 2008); Grabein v. 1-800-Flowers.com, Inc., No. 07-22235-CIV-HUCK,

litigation unleashed by the FACTA credit card receipt provisions, Congress enacted the Credit and Debit Card Receipt Clarification Act of 2007 to provide that printing expiration dates on receipts where the account number is otherwise properly truncated does not by itself constitute willful noncompliance, eliminating at least some of ambiguity in the text of the FACTA credit card receipt rule.[131]

By contrast, the recent "Identity Theft Red Flag Guidelines" issued by the FTC and federal financial regulators is an example of a "smart" approach to using regulation to reduce the risk of identity theft.[132] The Red Flags Rules apply to licensed depository institutions and "creditors," which include any entity that regularly extends credit, with regard to accounts used for payment transactions.[133] Under the Red Flags Rules, financial institutions and creditors must develop a written program that identifies and detects the relevant warning signs of identity theft.[134] These may include, for example, unusual account

---

2008 U.S. Dist. LEXIS 11757 (S.D. Fla. Jan. 29, 2008); Dister v. Apple-Bay E., Inc., No. C 07-01377 SBA, 2007 U.S. Dist. LEXIS 95861 (N.D. Cal. Dec. 24, 2007); Azoiani v. Love's Travel Stops & Country Stores, Inc., No. EDCV 07-90 ODW (Opx), 2007 U.S. Dist. LEXIS 96159 (C.D. Cal. Dec. 18, 2007); Follman v. Vill. Squire, Inc., 542 F. Supp. 2d 816 (N.D. Ill. 2007); Ramirez v. MGM Mirage, Inc., 524 F. Supp. 2d 1226 (D. Nev. 2007); Edwards v. Toys "R" Us, 527 F. Supp. 2d 1197 (C.D. Cal. 2007); Follman v. Hospitality Plus of Carpentersville, Inc., 532 F. Supp. 2d 960 (N.D. Ill. 2007); Serna v. Big A Drug Stores, Inc., No. SACV 07-0276 CJC (MLGx), 2007 U.S. Dist. LEXIS 82023 (C.D. Cal. Oct. 9, 2007); Medrano v. Modern Parking, Inc., No. CV 07-2949 PA (AGRx), 2007 U.S. Dist. LEXIS 82024 (C.D. Cal. Sept. 17, 2007); Price v. Lucky Strike Entm't, Inc., No. CV 07-960-ODW(MANx), 2007 U.S. Dist. LEXIS 96072 (C.D. Cal. Aug. 29, 2007); Korman v. Walking Co., 503 F. Supp. 2d 755 (E.D. Pa. 2007); Iosello v. Leiblys, Inc., 502 F. Supp. 2d 782 (N.D. Ill. 2007); Evans v. U-Haul Co. of Cal., No. CV 07-2097-JFW (JCx), 2007 U.S. Dist. LEXIS 82026 (C.D. Cal. Aug. 14, 2007); Torossian v. Vitamin Shoppe Indus., No. CV 07-0523 ODW (SSx), 2007 U.S. Dist. LEXIS 81961 (C.D. Cal. Aug. 6, 2007); Lopez v. KB Toys Retail, Inc., No. CV 07-144-JFW (CWx), 2007 U.S. Dist. LEXIS 82025 (C.D. Cal. July 17, 2007); Najarian v. Charlotte Russe, Inc., No. CV 07-501-RGK (CTx), 2007 U.S. Dist. LEXIS 59879 (C.D. Cal. June 12, 2007); Najarian v. Avis Rent A Car Sys., No. CV 07-588-RGK (Ex), 2007 U.S. Dist. LEXIS 59932 (C.D. Cal. June 11, 2007); Soualian v. Int'l Coffee & Tea LLC, No. CV 07-502-RGK (JCx), 2007 U.S. Dist. LEXIS 44208 (C.D. Cal. June 11, 2007); Spikings v. Cost Plus, Inc., No. CV 06-8125 JFW (AJWx), 2007 U.S. Dist. LEXIS 44214 (C.D. Cal. May 25, 2007); Arcilla v. Adidas Promotional Retail Operations, Inc., 488 F. Supp. 2d 965 (C.D. Cal. 2007); Aeschbacher v. California Pizza Kitchen, Inc., No. CV 07-215-VBF(JWJx), 2007 U.S. Dist. LEXIS 34852 (C.D. Cal. Apr. 3, 2007); Eskandari v. IKEA U.S. Inc., No. SACV 06-1248 JVS (RNBx), 2007 U.S. Dist. LEXIS 23007 (C.D. Cal. Mar. 12, 2007); Tremble v. Town & Country Credit Corp., No. 05 C 2625, 2006 U.S. Dist. LEXIS 1835 (N.D. Ill. Jan. 18, 2006).

131. 15 U.S.C. § 1681n (2009).

132. Banking Agencies and FTC, Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003, 16 C.F.R. § 681.1 (2009).

133. *Id.*

134. *Id.*

activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The program must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program.[135] The program must be managed by the Board of Directors or senior employees of the financial institution or creditor, include appropriate staff training, and provide for oversight of any service providers.[136] In addition to the Red Flags Rules, the regulators also issued guidelines that provide detailed analysis of examples of possible red flags.[137] After the Red Flags Rule was issued, FTC staff engaged in outreach to raise awareness of the rule and to provide training and support to industry associations' own outreach and training efforts.[138] The Red Flags Rule is intended to promote the use of adaptive management systems to reduce the risk of identity theft by changing business administrative systems.

The Red Flags Rule demonstrates that even though the term "better regulation" is not generally used to describe U.S. legislation, many of the tenants of better regulation are well known and can be used effectively in the United States, and that a slide into adversarial legalism—in the form of expanded tort liability and class action litigation—is not a foregone conclusion. So while a comprehensive regulatory framework to provide database owners with stronger incentives to improve information security remains unlikely in the United States, it remains possible that elements of a better regulation legislative approach may be chosen.

## VI. CONCLUSION

Many different factors contribute to the problem of security breaches: explosive growth in the use of information technologies in business administration processes that has outpaced growth in the science and engineering of information security; weaker models for managing operational risk than other forms of risk encountered by businesses; software and information technology vendor success in avoiding liability for the problems caused by their lack of attention to information security; and the commodification of sensitive personal information. SBNLs may be having some impact on some of the

135. *Id.*

136. *Id.*

137. FTC Business Alert, New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft (2008), *available at* http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.pdf.

138. FTC Extended Enforcement Policy: Identity Theft Red Flags Rule, 16 CFR 681.1 (2009), *available at* http://www.ftc.gov/os/2009/04/P095406redflagsextendedenforcement.pdf.

factors contributing to the problem of security breaches, but due to their modest scope, that impact will be no more than modest at best. In addition to their modest scope, SBNLs suffer from some design flaws that will also undermine their effectiveness. Because SBNLs do not provide for audits or public enforcement, many database owners may decide that the expected cost of non-compliance is close to zero and not increase their investment in information security. SBNLs also include information-forcing provisions, which place disclosure obligations on those with powerful incentives to disclose as little as possible, as well as "end-of-pipe" technology-forcing provisions, which often suppress innovation and create perverse incentives to invest in mitigating harms after they occur instead of prevention. They also impose strict liability on organizations that cannot in turn pass that liability on to the information technology producers who are normally in a better position than database owners to fix problems with information security. Adding a private cause of action for individuals whose personal information has been exposed against database owners without guaranteeing database owners a similar right to recover from vendors of products with defective security would create only indirect and relatively weak incentives to improve the security of business information systems.

A "better" approach to security breach regulation would begin with a better understanding of the challenges facing database owners, look for opportunities to promote voluntary collaboration and self-regulation, and minimize confrontation and the taking of defensive measures in order to minimize litigation risks. Some form of direct regulation is likely to be necessary to address free-riding and opportunism by organizations that would otherwise seek to exploit the weak enforcement mechanisms available within voluntary or self-regulatory systems. Although the turn toward "deregulation" that began with the first Bush Administration in the 1980s may now be over, it is unclear whether the political will exists in the United States to enact any information security regulations that do not fit the "adversarial legalism" mold of class action lawsuits to enforce private causes of action. So SBNLs may be the best legal protection that American consumers are offered against breaches of security that expose their sensitive personal information, even if they are not "better" regulation.