1-2007

Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age

Danielle K. Citron
Boston University School of Law

Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age

Danielle Keats Citron

University of Maryland
School of Law

ARTICLES

RESERVOIRS OF DANGER: THE EVOLUTION OF PUBLIC AND PRIVATE LAW AT THE DAWN OF THE INFORMATION AGE

DANIELLE KEATS CITRON*

TABLE OF CONTENTS

* Assistant Professor of Law, University of Maryland School of Law. Many thanks to Richard Boldt, Maxwell Chibundu, Lisa Fairfax, Don Gifford, Oscar Gray, Keith Hylton, Bob Kaczorowski, Greg Keating, Helen Norton, Peter Quint, Max Stearns, David Super, Michael Van Alstine, and Ben Zipursky for their thoughtful comments on this Article. This Article also benefited from the excellent research assistance of Jonathan Bliley, Pamela Bluh, Jenny Deines, Sue McCarty, Janet Sinder, and Jenny Smith. I am indebted to Dean Karen Rothenberg and the University of Maryland School of Law for their support of this research.

ABSTRACT

A defining problem of the Information Age is securing computer databases of ultrasensitive personal information. These reservoirs of data fuel our Internet economy but endanger individuals when their information escapes into the hands of cyber-criminals. This juxtaposition of opportunities for rapid economic growth and novel dangers recalls similar challenges society and law faced at the outset of the Industrial Age. Then, reservoirs collected water to power textile mills: the water was harmless in repose but wrought havoc when it escaped. After initially resisting Rylands v. Fletcher*'s strict-liability standard as undermining economic development, American courts and scholars embraced it once the economy*

matured and catastrophes such as the Johnstown Flood made those hazards impossible to ignore.

Public choice analysis suggests that a meaningful public law response to insecure databases is as unlikely now as it was in the early Industrial Age. The Industrial Age's experience can, however, help guide us to an appropriate private law remedy for the new risks and new types of harm of the early Information Age. Just as the Industrial Revolution's maturation tipped the balance in favor of early tort theorists arguing that America needed, and could afford, a Rylands *solution, so too the Information Revolution's deep roots in American society and many strains of contemporary tort theory support strict liability for bursting cyber-reservoirs of personal data instead of a negligence regime overmatched by fast-changing technology. More broadly, the early Industrial Age offers valuable lessons for addressing other important Information Age problems.*

I. INTRODUCTION

The emerging technologies of our Information Age will redefine accidents as we know them.[1] The characteristic dangers of this century's information technologies fundamentally differ from those posed by the technologies propelling last century's economy. Whereas twentieth-century technologies largely wrought environmental and bodily harm, a salient issue at the dawn of the Information Age is the release of sensitive personal information from computer databases into the hands of identity predators and corporate thieves.[2] As we head into uncharted territory, we can learn much from the law's response to newly emerging risks at the dawn of the previous economic era.

The dynamics of the early Industrial Age, a time of great potential and peril, parallel those at the advent of the Information Age. Then, as now, technological change brought enormous wealth and comfort to society. Industry thrived as a result of machines powered by water-reservoirs. But

1. *See generally* MARTIN REES, OUR FINAL HOUR: A SCIENTIST'S WARNING: HOW TERROR, ERROR, AND ENVIRONMENTAL DISASTER THREATEN HUMANKIND'S FUTURE IN THIS CENTURY—ON EARTH AND BEYOND (2003) (discussing threats arising in the wake of recent developments in bio-, cyber-, and nanotechnology); Bill Joy, *Why the Future Doesn't Need Us*, WIRED, Apr. 2000, *available at* http://www.wired.com/wired/archive/8.04/joy_pr.html.

2. *See* U.S. FEDERAL TRADE COMM'N, INFORMATION COMPROMISE AND THE RISK OF IDENTITY THEFT: GUIDANCE FOR YOUR BUSINESS (June 2004), *available at* http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.pdf [hereinafter FTC, INFORMATION COMPROMISE]; John Leland & Tom Zeller, Jr., *Technology and Easy Credit Give Identity Thieves an Edge*, N.Y. TIMES, May 30, 2006, at A1; *Senator Clinton Speaks on Privacy Rights to American Constitution Society*, U.S. FED. NEWS, June 16, 2006, *available at* 2006 WLNR 10544222.

when the dams holding those reservoirs failed, the escaping water caused massive property and personal damage different from the interpersonal harms of the previous century.[3] *Rylands v. Fletcher*[4] provided the Industrial Age's strict-liability response to the accidents caused by the valuable reservoirs' escaping water. The history of *Rylands*'s reception in Britain and the United States reflects the tension between that era's desire for economic growth and its concern for security from industrial hazards.[5]

Computer databases are this century's reservoirs. Today, databases of personal identifying information in the private sector ensure the seamless flow of commerce.[6] Social Security numbers ("SSNs") facilitate loans and instant credit. Employers and colleges use SSNs to identify employees and students. Over 1000 companies collect and sell our sensitive personal information.[7] Databases of biometric information—fingerprint, retinal, iris, and facial images—increasingly authenticate retail transactions, secure workplaces, and provide access to corporate computer networks. Much as water reservoirs drove the Industrial Age, computer databases fuel the Internet economy of our Information Age.[8]

Today's cyber-reservoirs are safe so long as the sensitive personal data remains inside. But because such cyber-reservoirs are "treasure chests" for criminals, data-security breaches are increasingly prevalent.[9] When sensitive personal information escapes into the hands of thieves, great havoc can result. Just as the new technologies of the Industrial Age changed the nature of accidents, information technologies present new harms, ranging from identity theft and criminal impersonation to stalking

3. *See* LAWRENCE M. FRIEDMAN, A HISTORY OF AMERICAN LAW 350, 364–65 (3d ed. 2005); Oliver Wendell Holmes, *The Path of the Law*, 10 HARV. L. REV. 457, 467 (1897) (highlighting a shift in the late nineteenth century from wrongs, such as assault and battery, to those involving the "incidents" of industry).

4. Rylands v. Fletcher, (1868) 3 L.R.E. & I. App. 330 (H.L.).

5. *See infra* Part V.B.

6. *See* Leland & Zeller, *supra* note 2.

7. Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 65 (2003). *See also* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 16–26 (2004) (discussing the history of private sector databases).

8. *See* FRIEDMAN, *supra* note 3, at 350–68.

9. *See* Phillip Britt, *Survey: Government Struggles with Data Breaches*, INFO. TODAY, Jan. 1, 2006, at 48 ("Like thieves [who] rob banks because 'that's where the money is,' computer attackers target databases because that's where the data is."); Privacy Rights Clearinghouse, *A Chronology of Data Breaches Since the ChoicePoint Incident*, http://www.privacyrights.org/ar/ChronData Breaches.htm (last visited Aug. 1, 2006) [hereinafter Privacy Rights, *Chronology*].

and corporate espionage.[10] The emerging technologies at the dawn of the Information Age bring great value and new risks to individuals.

We face a dilemma similar to that of the past: striking a balance between the social goals of economic growth and individual safety. Although the hazardous nature of today's valuable cyber-reservoirs are clear, many questions remain. How can the law motivate those collecting sensitive personal data to secure it? What role can, and does, public law play in solving this problem? To what extent should private law operate to promote data security at the dawn of this Information Age? How should private law conceptualize harm in the twenty-first century, a time when an individual's autonomy increasingly depends on the individual's market identity?

In answering these questions, this Article develops three distinct, but interlocking, themes. First, it proposes a *Rylands* strict-liability model to address the hazards of leaking databases and explains why both the public law and negligence-based solutions suggested in the current literature are likely to prove impractical. Second, it explores parallels in the challenges presented by the new technologies at the dawn of the Industrial Age with those at the outset of the Information Age. Third, it looks at the influence economic development has on legal theory across those eras.

Each of these themes is critical to the others. The history of the Industrial Age's reservoirs helps us appreciate that the problem of insecure databases is not an entirely novel one. Analyzing the patterns of economic, intellectual, and legal change at the dawn of the Industrial Age provides a preview of similar conflicts at the outset of the Information Age. The insecure database dilemma also illuminates the changing conception of personal harm that accompanies the genesis of new economic eras.

Part II of this Article describes the massive collection of sensitive personal information in private-sector computer databases and the hazards the release of such data can pose. Part III explores the prospects of a public law solution to today's insecure databases. Although states have made some progress, no comprehensive federal legislation addresses the collection of sensitive personal data held by private industry. Public choice

10. *See* FTC, INFORMATION COMPROMISE, *supra* note 2; Peter P. Swire, *Efficient Confidentiality for Privacy, Security, and Confidential Business Information*, 2003 BROOKINGS-WHARTON PAPERS ON FIN. SERVS. 273, 290, *available at* http://muse.jhu.edu/journals/brookings-wharton_papers_on_financial_services/v2003/2003.1swire.html; Leland & Zeller, *supra* note 2; David Stout, *Veterans Agency to Atone with Free Credit Monitoring*, N.Y. TIMES, June 22, 2006, at A17.

theory suggests that no meaningful law can be expected any time soon. This leaves a significant void to fill.

Part IV explores how economic and moral views come together in finding negligence inadequate to address the insecure database problem. It explores the uncertainty database operators will face in attempting to comply with a negligence standard given the rapidly changing risk environment, which undermines efficient deterrence. Part IV then highlights the significant residual risk of data leaks that will remain even if database operators employ safety precautions. The high utility and high risk of information reservoirs suggest their treatment as an ultrahazardous activity for which negligence is an inefficient cost-spreading and deterrence tool. It concludes by arguing that a negligence regime will be unable to establish norms for reasonable information security practices.

Part V looks to the law's treatment of technological change at the threshold of the Industrial Age to address the novel challenges at the outset of the Information Age. It describes *Rylands v. Fletcher* and surveys the different schools of thought that responded to *Rylands* in England and in the United States. Part V explores how Industrial Age jurists and intellectuals embraced *Rylands* once the economy matured and public anxiety about bursting reservoirs and other industrial hazards intensified.

Part VI argues that the economic and intellectual trends at the outset of the Information Age are aligned in a manner similar to that at the time of *Rylands*'s adoption. *Rylands* provides a powerful metaphor to conceptualize the contributions and the dangers engendered by the new technologies of the Information Age, particularly the insecure cyber-reservoirs of personal data. Part VI argues that just as the Industrial Age recognized new and different harms, the new injuries of the Information Age, namely those involving the compromise of our personal independence and market identity, ought to be recognized and redressed.

II. CYBER-RESERVOIRS OF THE TWENTY-FIRST CENTURY

For the first half of the twentieth century, private and public entities engaged in the time-consuming task of gathering personal information by using paper-filing systems.[11] Computers, however, radically changed the

11. *See* ELTING E. MORISON, MEN, MACHINES, AND MODERN TIMES 54 (1966) (explaining that certain government employees spent their "whole lives" assembling the medical and salary records of U.S. soldiers in paper-filing systems during the early part of the twentieth century); SOLOVE, *supra* note 7, at 14.

speed and breadth of data collection over the past fifty years.[12] Until recently, computers doubled their power about every eighteen months.[13] In June 2006, IBM researchers broke the speed record for silicon-based chips.[14] In the near future, semiconductors operating 250 times faster than those currently in production may become commercially available.[15]

Just as data processing has rapidly advanced, so has the storage of information.[16] In the past two years, the country's largest databases have tripled in size,[17] while data collection costs have fallen by half.[18] ChoicePoint, an information broker, collects and sells the personal information of over 220 million adults—an amount equivalent to "21 million miles, if printed out on copy paper carefully laid end to end," or roughly 77 trips around the moon.[19] As Microsoft founder Bill Gates recently remarked of our Information Age, "we're always in a time of utter change, maybe even accelerating change."[20]

Given the speed and efficiency of storing digital data, nearly all businesses maintain cyber-records.[21] This Part surveys the ultrasensitive digital data collected by information brokers, colleges, private employers,

12. ROBERT O'HARROW, JR., NO PLACE TO HIDE 4–5 (2005).

13. Nathan Myhrvold, *Moore's Law Corollary: Pixel Power*, N.Y. TIMES, June 7, 2006, at G3.

14. Laurie J. Flynn, *Researchers Say New Chip Breaks Speed Record*, N.Y. TIMES, June 20, 2006, at C7.

15. *See id.*; Press Release, IBM, IBM and Georgia Tech Break Silicon Speed Record (June 20, 2006), http://www-03.ibm.com/press/us/en/pressrelease/19843.wss (explaining that the recent breakthrough will "redefine[] the performance limits of silicon-based semiconductors" and that IBM will be working closely with academic and industry partners to deliver a new generation of high-performance, energy-efficient microprocessing).

16. Daniel B. Prieto, *Data Mine*, NEW REPUBLIC, Dec. 19, 2005, at 17. *See also* John Markoff & Saul Hansell, *Hiding in Plain Sight, Google Seeks an Expansion of Power*, N.Y. TIMES, June 14, 2006, at A1 (describing Google as a leader in the effort to build a network of supercomputers that can process more data and searches at speeds constrained only by the speed of light).

17. *See* J. Nicholas Hoover, *High–Stakes Data Mining*, INFO.WEEK, May 22, 2006, at 21, 23.

18. Jon William Toigo, *Data—The Squeeze Is on—Today's Digital Data Explosion Is the Stuff of Legend*, NETWORK COMPUTING, Nov. 24, 2005, at S3. *See also* JEFFREY W. SEIFERT, CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, REPORT NO. RL31798, DATA MINING AND HOMELAND SECURITY: AN OVERVIEW 2 (Jan. 27, 2006), *available at* http://www.fas.org/sgp/crs/intel/RL31798.pdf (noting that the decreased cost of data storage has contributed to the nation's increasing interest in data mining).

19. O'HARROW, *supra* note 12, at 145. *See also* Joseph Menn, *ChoicePoint Is Fined for Data Breach*, L.A. TIMES, Jan. 27, 2006, at C1 (noting that ChoicePoint stores 19 billion records).

20. John Markoff, *Gates's Lieutenants Look Ahead, Hoping to Avoid Other Companies' Mistakes*, N.Y. TIMES, June 17, 2006, at C1.

21. U.S. GOV'T ACCOUNTABILITY OFFICE, SOC. SEC. NUMBERS: MORE COULD BE DONE TO PROTECT SSNS, GAO REP. NO. GAO-06-586T, TESTIMONY BEFORE THE SUBCOMM. ON SOC. SEC., COMM. ON WAYS AND MEANS, H.R. 3 (Mar. 30, 2006) (statement of Cynthia M. Fagnoni, Managing Director of Education, Workforce, and Income Security Issues), *available at* http://www.gao.gov/new.items/d06586t.pdf [hereinafter GAO, MORE COULD BE DONE].

and biometric vendors.[22] Section A describes the widespread use and storage of SSNs. Section B explores how private-sector databases will increasingly amass fingerprint, iris, and retinal images to secure workplaces, computer systems, and retail transactions. Section C highlights the risks that the release of such personal data entails.

A. SOCIAL SECURITY NUMBERS

The SSN stands as our de facto national identifier.[23] According to the Federal Trade Commission ("FTC"), it would be "almost impossible" to conduct business without storing the SSNs of customers, employees, or students in computer databases.[24] Companies employ SSNs to track customer transactions.[25] Employers use SSNs to perform background checks, report payroll taxes, and identify employees.[26] Universities and colleges collect the SSNs of students and alumni.[27] Third-party vendors

22. This Article focuses on the collection of sensitive personal information by the large section of the private sector that is likely to remain unregulated by federal law. *See infra* text accompanying notes 98–108.

23. BRUCE SCHNEIER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD 114 (2003); SOLOVE, *supra* note 7, at 116. Federal law requires the collection of SSNs for the administration of the federal personal income tax, Medicaid, Child Support Enforcement programs, and to ensure compliance with the USA Patriot Act. U.S. GOV'T ACCOUNTABILITY OFFICE, SOC. SEC. NUMBERS: FEDERAL AND STATE LAWS RESTRICT USE OF SSNS, YET GAPS REMAIN, GAO REP. NO. GAO-05-1016T, at 6, 9–10 & n.14, 11, 20–21 (Sept. 15, 2005) (statement of Barbara D. Bovbjerg, Director of Education, Workforce, and Income Security Issues), *available at* http://www.gao.gov/new.items/d051016t.pdf. *See also* 26 U.S.C. § 6109(a) (2000) (income tax); USA Patriot Act of 2001, 31 U.S.C. § 5318A(b)(3)(B) (Supp. II 2002); 42 U.S.C.A. § 666(a)(13)(B) (West Supp. 2006) (child support); 42 U.S.C. § 1320b–7(a)(1), (b)(2) (2000) (Medicaid). Although federal law restricts the public disclosure of SSNs by credit reporting agencies, banks, and health care providers, no federal legislation addresses the collection and disclosure of SSNs by employers, retailers, and information resellers. *See* Privacy Rights Clearinghouse, *My Social Security Number: How Secure Is It?* (Jan. 2006), http://www.privacyrights.org/fs/fs10-ssn.htm; *infra* text accompanying notes 73–76.

24. FTC, INFORMATION COMPROMISE, *supra* note 2.

25. *See Hearing Before the H. Energy Commerce Reps. and Subcomm. on Commerce, Trade and Consumer Protection*, 109th Cong. (2006) (statement of H.R. Lively, President and CEO for the American Financial Services Association), *available at* http://energycommerce.house.gov/108/Hearings/05112006hearing1871/Lively.pdf [hereinafter Lively Testimony].

26. Lively Testimony, *supra* note 25 (explaining that SSNs are used to track employees in high-security positions); FREDERICK S. LANE III, THE NAKED EMPLOYEE: HOW TECHNOLOGY IS COMPROMISING WORKPLACE PRIVACY 28 (2003); *Employees Sue over Data Theft*, N.Y. TIMES, July 5, 2006, at C2 (describing a class-action lawsuit filed by employees of the Union Pacific Corporation for the company's use of SSNs to identify its employees).

27. Greg Sandoval, *University Server in Hackers' Hands for a Year*, ZDNET NEWS, May 21, 2006, http://news.zdnet.com/2100-1009_22-6074739.html; Privacy Rights Clearinghouse, *supra* note 23. Although publicly funded schools governed by the Privacy Act of 1974 must tell students how their SSNs will be used, private institutes face few restrictions in their use of student and alumni SSNs. Privacy Rights Clearinghouse, *supra* note 23.

often store SSNs and other personal data on behalf of businesses.[28]

An entire industry has emerged—data brokerage—that sells SSNs of millions of individuals.[29] Information brokers gather SSNs from public and private sources without individuals' knowledge or consent.[30] Moreover, data brokers typically refuse individual requests to remove personal information from their databases.[31]

B. BIOMETRIC DATA

Images of the human body's characteristics—a fingerprint, iris, retina, voice, and face—will increasingly be stored in databases to identify individuals and authenticate transactions.[32] Some predict that soon "no one will need pockets" to store credit cards or keys because "[w]hen you need

28. Thomas J. Smedinghoff, *The New Law of Information Security: What Companies Need to Do Now*, COMPUTER & INTERNET LAW., Nov. 2005, at 9, 16. S*ee also* GAO, MORE COULD BE DONE, *supra* note 21, at 3–4 (explaining that 90% of businesses outsource the storage of personal data, such as SSNs, to third-party contractors).

29. *See* SOLOVE, *supra* note 7, at 19; Jonathan Krim, *Net Aids Access to Sensitive ID Data*, WASH. POST, Apr. 4, 2005, at A1 (describing numerous companies that sell SSNs for as low as thirty-five dollars on websites such as www.secret-info.com). One such firm, "SixChannels," explains that it continuously gathers the personal data of consumers from a variety of sources, including title companies, credit bureaus, tax liens, and judgments. SixChannels, Next Generation Multichannel Marketing Solutions, Frequently Asked Questions, http://www.sixchannels.net/faq.asp (last visited Aug. 1, 2006).

30. *See* SOLOVE, *supra* note 7, at 81, 84 (explaining that "[i]nformation collection is duplicitous, clandestine, and often coerced"); Stephanie Kirchgaessner & Bob Sherwood, *Companies Selling Personal Information Have Been Allowed to Operate Relatively Free of Regulation*, FIN. TIMES (U.K.), May 20, 2005, at 17 (discussing how data brokers acquire individuals' names and addresses from credit agencies and supplement that information with data culled from public records); McClurg, *supra* note 7, at 65; Leigh Webb, *Personal Information—Asset or Risk?*, IDENTITY THEFT 911 NEWSLETTER, Apr. 2006, at 1, *available at* http://www.identitytheft911-sunj.com/content.do?sp=323 (explaining that because of the increase in instances of personal data collection, often without the consumer's consent, more and more people are falling victim to identity theft).

31. *E.g.*, Kirchgaessner & Sherwood, *supra* note 30, at 17 (noting that LexisNexis permits consumers to opt out of its database only in limited circumstances, despite the industry's previous commitment to permit such opt outs whenever a consumer requested them); *Your Privacy for Sale*, CONSUMER REP., Oct. 2006, *available at* http://www.consumerreports.org/cro/personal-finance/data-privacy-10-06/a-steady-customer/1006_privacy_ov6_1.htm [hereinafter *Your Privacy*] (noting that the Pentagon refuses requests to opt out of its vast database). *See also* O'HARROW, *supra* note 12, at 138 (explaining that information broker ChoicePoint apparently does not allow individuals to opt out of its databases). When Consumer Reports investigators asked data brokers to permit them access to their own personal information, the data brokers informed them that they could not see everything that was routinely sold to businesses. *Your Privacy*, *supra*.

32. *See* Gang Wei & Dongge Li, *Biometrics: Applications, Challenges and the Future*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 135, 136 (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006); Alex Halperin, *Biometrics: Payments at Your Fingerprints*, BUS. WK. ONLINE, Mar. 28, 2006, http://www.businessweek.com/technology/content/mar2006/tc20060328_901806.htm?campaign_id=search.

to open a door or make a purchase, chances are you'll do it with a fingerprint, a voice command, or a computer scan of your eyeball."[33]

Databases store an image of an individual's biometric information, such as a picture of a person's thumbprint or a mathematical formula of that image, called a template.[34] The biometric system operates by matching an individual's fingerprint, for example, with the image or template stored in the database.[35] Computer databases today store a considerable amount of biometric data.[36] A biometric provider, Pay By Touch, holds the biometric templates of over two million individuals who use their fingerprints to pay for gas and groceries.[37] Elementary schools,[38] airports,[39] health clubs,[40] workplaces,[41] and even Disney's theme parks collect iris scans and

33. Halperin, *supra* note 32.

34. *See* Ishwar K. Sethi, *Biometrics: Overview and Application*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION, *supra* note 32, at 117, 120–22. In certain biometric systems, individuals do not provide their biometric information for storage in a database but instead carry cards, known as Smart Cards, with their biometric data stored inside. *Id.* at 121. Such systems match biometric data contained in a card to the individual's characteristic, such as a fingerprint or iris. *Id. See also* Kevin Coughlin, *Security in the Blink of an Eye*, STAR-LEDGER, Jan. 4, 2006, at 43 (describing the use of Smart Cards at airports).

35. Wei & Li, *supra* note 32, at 137 (explaining that biometric systems either identify an individual by matching the person's sample to the many samples in the database or verify an individual's identity by matching the sample to the template or image in the database with that name).

36. *See* JOHN D. WOODWARD, JR., NICHOLAS M. ORLANS & PETER T. HIGGINS, BIOMETRICS 329–52 (2003); Roger Allan, *Biometrics Wields a Double-Edged Sword*, ELECTRONIC DESIGN, June 30, 2005, at 77, *available at* http://www.elecdesign.com/Articles/ArticleID/10605/10605.html (describing massive databases of biometric data maintained by banking, security, and medical organizations). Technology sold by Identix Incorporated currently allows businesses to store up to twenty million fingerprints in a single computer database. *See* IDENTIX, ABIS® SYSTEM FREQUENTLY ASKED QUESTIONS—VERSION 4.1, para. 12 (2005), *available at* http://www.identix.com/support/downloads/ABIS%204-1%20FAQs%20Draft2_Customer%20Version_Final.pdf. Comnetix Inc. stores biometric image scans indefinitely and, for government users, can submit scans to the national fingerprint database for quick checks against criminal records. John Breeden II, *Biometrics Look Ready for Prime Time*, GOV'T COMPUTER NEWS, Feb. 6, 2006, at 36, *available at* 2006 WLNR 2849844.

37. Halperin, *supra* note 32. One hundred seventy-six Bi-Lo grocery stores in Georgia, North Carolina, South Carolina, and Tennessee use fingerprint systems to allow customers to cash paychecks. O'HARROW, *supra* note 12, at 174–75.

38. Halperin, *supra* note 32; Greg Toppo, *Eye Scans: A High-Tech Hall Pass?*, USA TODAY, Feb. 23, 2006, at 12B (discussing the recent implementation of iris-scan technology as a security measure at a New Jersey elementary school).

39. Coughlin, *supra* note 34; Elizabeth Fernandez, *Fast-track Security Check OK'd for Airports*, S.F. CHRON., Apr. 21, 2006, at B3 (discussing the Transportation Security Administration's recent approval of a plan to use fingerprint and iris scans to screen preregistered passengers at airport security checkpoints at twenty airports).

40. Michael Sisk, *Biometric Systems Replace the Lost Card Key*, CRAIN'S N.Y. BUS., May 1, 2006, at 17.

41. Joan Engebretson, *How Security Dealers Really Feel About Biometrics*, SEC. DISTRIBUTING & MARKETING., Mar. 13, 2006, *available at* http://www.sdmmag.com/copyright/faf86047124f9010VgnVCM100000f932a8c0_?. One in four companies surveyed by Deloitte in 2006 plans to employ

fingerprints of individuals to secure access to their physical plants.[42] Businesses allow customers to pay by scanning their fingerprints.[43] Companies, like Morpheus Technologies and ChoicePoint, plan to create "central clearinghouses" of biometric information for commercial use.[44] As the use of biometric systems spreads, the amount of biometric information stored in databases will increase exponentially.[45]

C. THE RISKS OF STORING PERSONAL IDENTIFYING INFORMATION IN DATABASES

Databases filled with large caches of personal information are prime targets of cyber-criminals.[46] The Internet provides hackers access to an organization's databases of personal information.[47] More than 75% of companies surveyed by Deloitte in the first half of 2006 reported that they had suffered a data-security breach from outside intruders, up from 26% in 2005.[48] Furthermore, employees were responsible for 50% of all data leaks reported.[49]

---

biometric security measures over the next eighteen months to authenticate employees. DELOITTE, 2006 GLOBAL SECURITY STUDY 9 (2006), *available at* http://www.deloitte.com/dtt/cda/doc/content/dtt_lssecuritystudy_053006.pdf.

42. David Wyld, *Biometrics at the Disney Gates*, SECUREID NEWS, Mar. 2, 2006, http://www.secureidnews.com/library/2006/03/02/biometrics-at-the-disney-gates/.

43. Brian J. Rogal, *Biometrics: Getting in Touch with a Growing Trend*, CREDIT CARD MGMT., Feb. 1, 2006, at 26. Credit unions have "started deploying electronic fingerprint systems at kiosks to allow members to do business remotely." O'HARROW, *supra* note 12, at 176. *See* Jonathan Curiel, *The Last Days of Privacy*, S.F. CHRON., June 25, 2006, at E1 (discussing the present consideration by the banking industry of widespread implementation of biometric technology in ATMs in the United States).

44. O'HARROW, *supra* note 12, at 171; C. Maxine Most, *Biometrics and Financial Services—Show Me the Money!*, DIGITAL ID WORLD, Jan./Feb. 2004, at 20, *available at* http://magazine.digitalidworld.com/Jan04/Page20.pdf.

45. *See* Dan Frommer, *The Tell-Tale Heart*, FORBES.COM, Feb. 16, 2006, http://www.forbes.com/technology/2006/02/16/ibm-aladdin-biometric-cx_df_0216biometric.html (predicting that the annual sales of biometric security devices will grow from its present level of $2.2 billion to $6 billion by 2010). *See also* William Abernathy & Lee Tien, *Biometrics: Who's Watching You?*, http://www.eff.org/Privacy/Surveillance/biometrics/ (last visited Aug. 2, 2006) (stating that an effective biometric system "must compare captured biometric data to a biometric database").

46. *See* Jarrett Banks, *Identity Theft Suits Gain Popularity with Plaintiffs*, CORP. LEGAL TIMES, July 2005, at 32.

47. Michael E. Whitman, *Enemy at the Gate: Threats to Information Security*, COMM. OF THE ACM, Aug. 2003, at 91, 92–93 (explaining different means by which the Internet opens organizations using it to attack of their computer networks). *See also* Siobhan Gorman, *Hacker Attacks Hitting Pentagon*, BALTIMORE SUN, July 2, 2006, at 1A (describing thousands of successful penetrations of the Pentagon's computer networks and noting the obsolescence of NSA's methods to safeguard data).

48. Dean Foust, *ID Theft: More Hype Than Harm*, BUS. WK., July 3, 2006, at 34.

49. DELOITTE, PROTECTING THE DIGITAL ASSETS: THE 2006 TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS SECURITY SURVEY 7 (2006), *available at* http://www.deloitte.com/dtt/cda/doc/content/dtt_DR_ProtectingDigitalAssets_062106.pdf.

Consider a sample of the data-security breaches from January 2005 to July 2006. Computer hackers accessed the databases of forty-five colleges and universities, resulting in the release of 1.8 million students' SSNs.[50] Thieves obtained the SSNs and credit card information of over 41 million customers.[51] Dishonest employees accessed personal data of 1.7 million coworkers and clients.[52]

The public sector has had its share of information leaks as well. In May 2006, a Veterans Administration employee downloaded the SSNs of as many as 26.5 million veterans onto a laptop, which was stolen from the employee's home.[53] In all, nearly one out of every four households in the United States has been the victim of identity theft.[54]

1. The Hazards of Escaping SSNs

Identity theft is a glaring consequence of the release of SSNs from today's cyber-reservoirs.[55] An SSN, along with a person's name and birth date, authenticates an individual in the marketplace.[56] With that information, a thief obtains "virtual keys" to a victim's finances.[57] An identity thief can empty bank accounts, obtain credit cards, secure loans, open lines of credit, connect telephone services, and enroll in government benefits in a victim's name.[58] Identity thieves also commit crimes in their

50. *See* Privacy Rights, *Chronology*, *supra* note 9. *See also* Stefanie Olsen, *Man Charged with Hacking USC Database*, CNET NEWS.COM, Apr. 20, 2006, http://news.com.com/Man+charged+with+hacking+USC+database/2100-7350_3-6063470.html?tag=nl (describing a hacker's successful penetration of a USC database containing 275,000 applicants' SSNs). "Universities are becoming bigger and bigger targets to the hacker community because they are large institutions" with vast collections of SSNs. *Id.*

51. *See* Privacy Rights, *Chronology*, *supra* note 9 (describing data-security breaches at Guess.com and DSW Inc., among others).

52. *See id.*

53. *See* Stout, *supra* note 10.

54. *See* FEDERAL TRADE COMMISSION, IDENTITY THEFT SURVEY REPORT 3, 13 (Sept. 2003), *available at* http://www.consumer.gov/idtheft/pdf/synovatereport.pdf. *See also* Christine Dugas, *Federal Survey: Identity Theft Hits 1 in 4 U.S. Households*, USA TODAY, Sept. 4, 2003, at 10B.

55. *See* Barbara Kiviat, *Who's Got Your Number?*, TIME, July 17, 2006, at 68 (explaining that "[t]he quickest way to become a victim of identity theft is to let your [SSN] fall into the wrong hands").

56. *See* Swire, *supra* note 10, at 290.

57. O'HARROW, *supra* note 12, at 79; Swire, *supra* note 10, at 290.

58. Leland & Zeller, *supra* note 2; Privacy Rights Clearinghouse, *supra* note 23. *See also* Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, ¶ 15 (2004), *available at* http://stlr.stanford.edu/STLR/Articles/04_STLR_2/contents_f.htm (noting that identity theft is an "enabling crime" that permits criminals to commit other crimes by assuming the victim's identity). This past year, identity thieves used the SSNs and birth dates of three million people to "open new lines of credit, secure loans, [and] flip property" in the victim's name. *See* Leland & Zeller, *supra* note 2.

victims' names.[59] A victim of criminal impersonation risks arrest and a criminal record for an identity thief's transgressions.[60]

Identity-theft victims suffer significant emotional and financial harm.[61] Victims devote an average of $1000 in out-of-pocket expenses and over 600 hours of personal time to clean up their credit reports.[62] When lost income is included, the average victim loses $16,971.[63]

The release of sensitive personal information can also be deadly. *Remsburg v. Docusearch, Inc*.[64] involved an information broker that sold a woman's SSN and employment information to a stalker who used it to find the woman and kill her.[65] Although *Remsburg* did not involve a computer-security breach, it illustrates the risk of physical harm that can result from the escape of sensitive personal data.[66]

2. The Impending Dangers of Released Biometric Data

The release of biometric information from a database will engender serious harm as criminals can use such data to impersonate individuals.[67]

59. *See* Valetk, *supra* note 58, ¶¶ 31–32.

60. *See* BOB SULLIVAN, YOUR EVIL TWIN: BEHIND THE IDENTITY THEFT EPIDEMIC 42 (2004) (describing examples of victims of criminal identity theft who faced arrest and jail time before clearing their names). A false criminal record is virtually impossible to erase because officials of criminal records databases are reluctant to remove information from such databases. *Id.*

61. *Data Breaches and Identity Theft: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. 4 (2005) (prepared statement of Deborah Platt Majoras, Chairman of the FTC), *available at* http://commerce.senate.gov/pdf/ftc.pdf [hereinafter Majoras Statement] ("Identity theft causes significant economic and emotional injury."); O'HARROW, *supra* note 12, at 78; Identity Theft Resolution Center, Rutgers University, *Identity Theft Overview: Part III—Emotional Considerations*, 2003, *available at* http://www.identitytheft911-sunj.com/articles/article.ext?sp=27.

62. Prieto, *supra* note 16.

63. Heather M. Howard, Note, *The Negligent Enablement of Imposter Fraud: A Common-sense Common Law Claim*, 54 DUKE L.J. 1263, 1268 (2005). Victims also risk losing stolen bank funds in excess of the FDIC's insurance limit as the FDIC only insures up to $100,000 of a bank customer's funds. *See* Federal Deposit Insurance Co., FDIC: Insuring Your Deposits, http://www.fdic.gov (last visited Aug. 2, 2006).

64. Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1005–06 (N.H. 2003).

65. *Id.* at 1006–08 (finding an information broker liable for the stalker's criminal actions because the information broker's conduct created "'an especial temptation and opportunity for criminal misconduct'" (quoting Walls v. Oxford Mgmt. Co., 633 A.2d 103, 106 (N.H. 1993))).

66. *See also Your Privacy*, *supra* note 31 (citing a lawsuit alleging that a former coworker of Stanford Douglas obtained his home address from a data broker and later killed him).

67. *See* Bruce Barton et al., *The Emerging Cyber Risks of Biometrics*, RISK MGMT. MAG., Oct. 2005, at 26, 28, *available at* http://www.rmmag.com/ShowArticle.cfm?AID=2896; Frommer, *supra* note 45 (explaining that "any biometric database runs the risk of being hacked" to steal the information inside). The 2006 *Biometrics and Privacy* report, issued by the world's largest biometrics consulting group, warns that the storage of biometric information in databases runs a "high" degree of risk of theft to gain unauthorized access to a biometric system. Int'l Biometric Group, Biometric Research Report

Cyber-criminals can reverse engineer biometric templates into images in order to create replicas, such as a gelatin copy of a person's thumbprint or a contact lens of the person's iris.[68] That prosthetic device can fool, or "spoof," a biometric scanner.[69]

With the replica, a thief gains access to everything available to the victim, such as computer networks, workplace, and retail accounts. A cyber-criminal can commit corporate espionage and steal unpatented research and development.[70] Identity theft can also be perpetrated.[71] As

Series, Biometrics and Privacy, 2006 Research Report Series 3–8 (unpublished report on file with author) [hereinafter Int'l Biometric].

68. Sethi, *supra* note 34, at 131–32; Wei & Li, *supra* note 32, at 143. Although many biometric vendors would have the public believe that reverse engineering is not possible, that is simply untrue. Sethi, *supra* note 34, at 131–32. For example, in 2002, an Australian computer science student reverse engineered a fingerprint system as part of his honors thesis. *Id.* Moreover, a 2003 study showed that sample images can be regenerated from face recognition templates. ANDY ADLER, SAMPLE IMAGES CAN BE INDEPENDENTLY RESTORED FROM FACE RECOGNITION TEMPLATES (2003), *available at* http://www.site.uottawa.ca/~adler/publications/2003/adler-2003-fr-templates.pdf. *See also* Int'l Biometric, *supra* note 67, at 35 (discussing regeneration of face recognition templates).

69. *See* Tom Sanders, *Biometrics Struggles to Go Mainstream*, COMPUTING UK, Feb. 17, 2006, *available at* http://www.computing.co.uk/vnunet/news/2150496/biometrics-struggle-mainstream; Sethi, *supra* note 34, at 131. Prosthetic fingerprint samples can trick nearly all biometric scanners except high-end models employing thermal sensors. *See id.* at 131–32. These sensors ensure that the sample comes from a live human being. *Id.* Thermal-sensing machines, however, are not fool-proof as its "liveness" testing system can be breached and shut down. *See* TechTarget Expert Answer Center, Expert Knowledgebase, Joel Dubin, Penetrating a Biometric Security System, Sept. 21, 2005, http://expertanswercenter.techtarget.com/eac/knowledgebaseAnswer/0,295199,sid63_gci1142719,00.html. The significant cost of thermal-sensor scanners also suggests that such machines will not be employed when biometric systems are implemented on a grand scale. *See* ELECTRONIC PRIVACY INFO. CTR., COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER, BEFORE THE DEP'T OF THE TREASURY, IN THE MATTER OF FACT ACT BIOMETRIC STUDY, FILE NO. R41105 (Apr. 1, 2004) (submitted by Chris Jay Hoofnagle, Associate Director & W. Neal Hartzog, IPIOP Clerk), *available at* http://www.epic.org/privacy/biometrics/factabiometrics.html.

70. *See* DELOITTE, *supra* note 41, at 9.

71. A thief's use of an individual's biometric data to commit identity theft will create enormous problems for victims seeking to prove the theft, as all identity-theft victims face a certain amount of difficulty in proving that fraudulent expenses are not their own. *See* Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 107 (2001). But the likely assumption that one's fingerprint does not lie compounds that difficulty for an individual who suffers financial theft as a result of the leak of the individual's biometric. *See* Duncan Graham-Rowe, *Privacy and Prejudice: Whose ID Is It Anyway?*, NEW SCIENTIST, Sept. 17, 2005, at 20. Moreover, an individual's retina scan provides insight into certain medical conditions, such as high blood pressure and AIDS, placing an individual at risk for discrimination by employers. Sethi, *supra* note 34, at 125. The image of a fingerprint, if restored from the template, could reveal that an individual suffers from certain genetic disorders. DAVIDE MALTONI ET AL., HANDBOOK OF FINGERPRINT RECOGNITION 46 (2003). The Americans with Disabilities Act ("ADA"), 42 U.S.C. § 12112(a) (2000), would prohibit any discrimination on the basis of an employee's medical disability. ADA, however, defines disabilities so narrowly that many serious health conditions are not covered by its protections, perhaps including high blood pressure. *See id.* § 12102(2) (defining disability as a condition that substantially limits one or more major life activities); Murphy v. United Parcel Serv., Inc., 527 U.S. 516, 519 (1999) (stating

Bruce Schneier notes, once someone steals the biometric image of your thumb, "it remains stolen for life; there's no getting it back."[72]

The amount of personal identifying information stored in databases maintained by the private sector is astounding. Once cyber-data escapes into the hands of hackers and dishonest employees, individuals and businesses suffer significant harm. This extreme risk cries out for a solution, and the next part explores whether public law can provide it.

III. THE FEASIBILITY OF A PUBLIC LAW SOLUTION FOR INSECURE CYBER-RESERVOIRS

To date, the private sector's collection of sensitive personal information remains largely unregulated by federal law. While federal legislation governs the security of personal data stored by federal agencies,[73] similar federal restrictions apply only to a narrow set of private entities, such as financial institutions,[74] credit agencies,[75] and health care providers.[76]

---

that because a terminated employee's life activities suffered no substantial limits *when the employee took medication* for high blood pressure, the employee was not "disabled" within the meaning of ADA because under ADA, disability is properly assessed in light of any mitigating measures employed).

72. BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 144 (2000). As biometric technology develops universal biometric templates capable of recognition in any system, a thief will be able to use a victim's biometric data to access any database on which the victim's template resides. *See* Int'l Biometric, *supra* note 67, at 1.

73. *See* Federal Information Security Management Act, 44 U.S.C. § 3544(a)(1)(A) (Supp. III 2003) (requiring security measures to protect information collected and maintained by federal agencies and all information systems used or operated by or for federal agencies). The Privacy Act of 1974, 5 U.S.C. § 552a(d) (2000), also regulates the collection and use of records by federal agencies, giving individuals the right to access and correct information in such records.

74. See Title V of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. §§ 6801–6809 (2000), which prohibits financial institutions from disclosing a consumer's personal information to an unaffiliated third party without giving the consumer the opportunity to opt out of the disclosure. *See also* 65 Fed. Reg. 33,646 (May 24, 2000) (promulgated pursuant to the GLBA). GLBA also requires financial institutions to implement "appropriate" physical, technical, and procedural safeguards to protect customer information. 15 U.S.C. § 6801(b). The FTC has set forth standards governing the safeguarding of consumer information stored digitally. *See* Standards for Safeguarding Customer Information, 16 C.F.R. § 314.1–.5 (2006). *See also* 67 Fed. Reg. 36,484 (May 23, 2002) (discussing standards for safeguarding information).

75. See The Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), 15 U.S.C. § 1681g(a)(1)(A) (Supp. III 2003), which includes a number of provisions designed to increase the protection of sensitive consumer information, including SSNs.

76. *See* Health Insurance Portability & Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1320d-2 (2000). *See also* 45 C.F.R. pt. 164 (2005) (prescribing security and privacy regulations pursuant to HIPAA).

In response to the recent escalation of data-security breaches in the private sector, the FTC has broadened its enforcement authority over unfair trade practices to include any private entity's failure to provide "appropriate" information security.[77] To that end, the FTC has reached a number of consent decrees with companies whose information-security lapses led to the release of personal data.[78] The FTC also recently established a Division of Privacy and Identity Protection to enhance consumer outreach and enforcement.[79] Notwithstanding these encouraging developments, the FTC has limited resources to devote to the problem of leaking personal cyber-data.[80] Of the hundreds of documented data-security breaches from February 2005 through September 2006,[81] the FTC could apparently pursue only six.[82]

Some states have stepped in to fill the gaps in enforcement. California stands at the vanguard of this trend. Under California law, companies must employ "reasonable" information-security measures to protect sensitive consumer data[83] and must notify consumers if their personal information is

77. *E.g.*, FTC Complaint, *In re* BJ's Wholesale Club, Inc., Case No. 042 3160 (2005), *available at* http://www.ftc.gov/os/caselist/0423160/0423160.htm. *See also* News Release, U.S. Federal Trade Comm'n, ChoicePoint Settles Data Security Breach Charges (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.htm [hereinafter FTC ChoicePoint].

78. *See, e.g.*, FTC ChoicePoint, *supra* note 77 (requiring ChoicePoint to establish a comprehensive information security program designed to protect sensitive personal information it collects about consumers and to audit its security practices every two years).

79. *Social Security Numbers in Commerce: Reconciling Beneficial Uses with Threats to Privacy*: *Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 109th Cong. (2006) (statement of Jon Leibowitz, Comm'r of the U.S. Federal Trade Comm'n) [hereinafter Leibowitz Statement].

80. SOLOVE, *supra* note 7, at 73.

81. *See* Privacy Rights, *Chronology*, *supra* note 9.

82. *See* News Release, U.S. Federal Trade Comm'n, Real Estate Services Company Settles Privacy and Security Charge (May 10, 2006), *available at* http://www.ftc.gov/opa/2006/05/nationstitle.htm; News Release, U.S. Federal Trade Comm'n, CardSystems Solutions Settles FTC Charges (Feb. 23, 2006), *available at* http://www.ftc.gov/opa/2006/02/cardsystems_r.htm; News Release, U.S. Federal Trade Comm'n, DSW Inc. Settles FTC Charges (Dec. 1, 2005), *available at* http://www.ftc.gov/opa/2005/12/dsw.htm; News Release, U.S. Federal Trade Comm'n, Mortgage Company Settles Information Security Charges (Sept. 28, 2005), *available at* http://www.ftc.gov/opa/2005/09/Superior.htm; *supra* text accompanying notes 77–78 (discussing the FTC's settlement with ChoicePoint and BJ's Wholesale Club). *See also* Leibowitz Statement, *supra* note 79, at 15 (explaining that since 2001 the FTC has brought thirteen cases challenging businesses that failed to take reasonable steps to protect sensitive consumer information).

83. CAL. CIV. CODE § 1798.81.5(b) (West 2006). *See also* ARK. CODE ANN. § 4-110-104(b) (Supp. 2005) (requiring reasonable measures to protect sensitive consumer data); R.I. GEN. LAWS § 11-49.2-2(2), (3) (Supp. 2005) (same); NEV. REV. STAT. ANN. § 597.970(1) (LexisNexis Supp. 2004) (requiring businesses to encrypt electronic transmissions that contain consumers' personal information when those transmissions are sent outside the firm).

leaked.[84] Following California's lead, twenty-two states now have some sort of consumer-notification rules.[85] In twenty-five states, consumers may freeze their credit reports.[86] A smaller number of states limit the display or retention of consumer SSNs on access cards and mailings.[87]

As the recent data-security breaches attest, the patchwork of state and federal laws has not effectively addressed database security. Some members of Congress agree that the insecure database problem requires a public law solution.[88] In the past year, members of the House and Senate

84. CAL. CIV. CODE § 1798.82 (West Supp. 2006).

85. ARK. CODE ANN. § 4-110-105 (Supp. 2005); CONN. GEN. STAT. ANN. § 36a-701b (West Supp. 2006); DEL. CODE. ANN. tit. 6, § 12B-102 (2005); GA. CODE ANN. § 10-1-912 (Supp. 2006); 815 ILL. COMP. STAT. ANN. 530/10 (West Supp. 2006); IND. CODE ANN. § 4-1-11-5 (LexisNexis Supp. 2005) (applying only to state agencies); LA. REV. STAT. ANN. § 51:3074 (Supp. 2006); ME. REV. STAT. ANN. tit. 10, § 1348 (Supp. 2005); MINN. STAT. ANN. § 325E.61 (West Supp. 2006); MONT. CODE ANN. § 30-14-1704 (2005) (effective Mar. 1, 2006); NEV. REV. STAT. ANN. § 603A.220 (LexisNexis Supp. 2005); N.J. STAT. ANN. § 56:8-163 (West Supp. 2006); N.Y. GEN. BUS. LAW § 899-aa (McKinney Supp. 2006); N.C. GEN. STAT. § 75-65 (2005); N.D. CENT. CODE § 51-30-02 (Supp. 2005); OHIO REV. CODE ANN. §§ 1347.12, 1349.19 (LexisNexis Supp. 2006); 73 PA. CONS. STAT. ANN. § 2303 (West Supp. 2006); R.I. GEN. LAWS § 11-49.2-3 (Supp. 2005); TENN. CODE ANN. § 47-18-2107 (Supp. 2005); TEX. BUS. & COM. CODE ANN. § 48.103 (Vernon Supp. 2006); WASH. REV. CODE ANN. § 19.255.010 (West Supp. 2006).

86. Those states allow consumers to freely freeze their credit reports without any preconditions except Illinois, Kansas, South Dakota, Texas, Vermont, and Washington, which only permit identity-theft victims to freeze their credit reports. CAL. CIV. CODE § 1785.11.2 (West Supp. 2006); COLO. REV. STAT. ANN. § 12-14.3-106.6 (West Supp. 2005); CONN. GEN. STAT. ANN. § 36a-701a (West Supp. 2006); DEL. CODE ANN. tit. 6, § 2203 (2006); 815 ILL. COMP. STAT. ANN. 505/2MM (West Supp. 2006); LA. REV. STAT. ANN. § 9:3571.1M (Supp. 2006); ME. REV. STAT. ANN. tit. 10, § 1313-C (Supp. 2005); NEV. REV. STAT. ANN. § 598C.300 (LexisNexis Supp. 2005); N.J. STAT. ANN. § 56:11-46 (West Supp. 2006); N.C. GEN. STAT. § 75-63 (2005); TEX. BUS. & COM. CODE ANN. § 20.034 (Vernon Supp. 2006); VT. STAT. ANN. tit. 9, § 2480h (Supp. 2005); WASH. REV. CODE ANN. § 19.182.170 (West Supp. 2006); 75 Del. Laws Ch. 328 (2006); 2006 Fla. Laws Ch. 2006–124, 1 (effective July 1, 2006) (to be codified at FLA. STAT. § 501.005); 2006 Haw. Rev. Stat. Ann. Adv. Legis. Serv. 138 (LexisNexis) (effective Jan. 1, 2007); Act of Apr. 19, 2006, 2006 Kan. Sess. Laws Ch. 149 § 12 (effective Jan. 1, 2007); 2006 Ky. Acts Ch. 42, § 3 (to be codified at KY. REV. STAT. ANN. § 367); 2006 Minn. Laws Ch. 233 (effective Aug. 1, 2006); 2006 N.H. Laws Ch. 208 (effective Jan. 1, 2007); Act of June 7, 2006, 2006 N.Y. Laws 63 (effective Nov. 1, 2006); Oklahoma Consumer Report Security Freeze Act, 2006 Okla. Sess. Laws Ch. 283 (effective Jan. 1, 2007) (to be codified at OKLA. STAT. tit. 24, § 149); Consumer Empowerment and Identity Theft Prevention Act of 2006, 2006 R.I. Pub. Laws 568 (effective Jan. 1, 2007) (to be codified at R.I. GEN. LAWS § 6-48-5); Consumer Credit Protection Act, 2006 Utah Laws Ch. 344 (effective Sept. 1, 2008) (to be codified at UTAH CODE ANN. § 13-42-201); 2005 Wis. Sess. Laws 140 (effective Jan. 1, 2007) (to be codified at WIS. STAT. § 100.54(2)); S.B. 180, 81st Leg. (S.D. 2006).

87. ARK. CODE ANN. § 4-86-107 (Supp. 2005) (effective Jan. 1, 2007); MD. CODE ANN., COM. LAW § 14-3402 (LexisNexis 2005); MINN. STAT. ANN. § 325E.59 (West Supp. 2006); MONT. CODE ANN. § 30-14-1722 (2005); N.C. GEN. STAT. § 75-62 (2005); OHIO REV. CODE ANN. §1349.17 (LexisNexis 2002); VA. CODE ANN. § 59.1-443.2 (Supp. 2005).

88. *See* S. 1332, 109th Cong. § 2 (2005) (describing databases of personal information as prime targets of hackers, identity thieves, rogue employees, and other criminals, who misuse such data and cause "serious or irreparable harm to an individual's livelihood" and hurt businesses).

have proposed a flurry of legislation. Some proposals are modest, only seeking to regulate the sale of SSNs by information brokers.[89] Other proposals go further in regulating the private sector's digital reservoirs of personal identifying information.

Senator Charles Schumer's proposed Comprehensive Identity Theft Protection Act, for example, would establish an Office of Identity Theft in the FTC charged with protecting sensitive personal information collected by businesses.[90] Under the Schumer proposal, the FTC would promulgate regulations regarding the information-security practices of commercial entities.[91] The proposal would require covered entities to provide notice of data-security breaches, give consumers greater control over the use of their sensitive personal information, and limit the display of SSNs.[92] The Schumer proposal accords with the views of noted privacy experts.[93]

If the Schumer proposal or another like it becomes law, the FTC would likely follow the standards it has set for the financial services industry's storage of customer information under the Gramm-Leach-Bliley Act ("GLBA Safeguards Rule").[94] In recent testimony before a House subcommittee, the FTC's Chairman urged Congress to extend its GLBA

89. *E.g.*, Information Protection and Security Act, S. 500, 109th Cong. §§ 2(b), 3(a)(2) (2005) (directing the FTC to promulgate regulations governing the conduct of information brokers and the protection of data held by such brokers without preempting any state law that would provide greater consumer protection); Privacy Act of 2005, S. 116, 109th Cong. § 101 (2005) (rendering it unlawful for commercial entities to sell personal identifying information without the individual's notice and opportunity to restrict disclosure); Social Security On-line Privacy Protection Act, H.R. 82, 109th Cong. § 2 (2005) (preventing interactive computer services from disclosing SSNs or other personally identifiable information without consent). *See also* Anne Broache, *Congress May Slap Restrictions on SSN Use*, CNET NEWS.COM, May 12, 2006, http://news.com.com/2100-7348_3-6071441.html (noting that at least three pieces of pending legislation in the House and Senate would restrict the use and sale of SSNs).

90. S. 768, 109th Cong. § 3 (2005).

91. *Id.* §§ 3, 5 (ordering the FTC to promulgate regulations governing the sale, maintenance, collection, or transfer of sensitive personal information, including a requirement that all commercial entities take reasonable steps to prevent unauthorized access to sensitive personal information they collect, sell, or transfer). Legislation proposed by Senators Specter, Leahy, and Feingold similarly would require all businesses storing personally identifiable data of over 10,000 individuals to implement a comprehensive data privacy security program. S. 1332, 109th Cong. §§ 401(b), 402 (2005).

92. S. 768, § 3.

93. *See* SOLOVE, *supra* note 7, at 104–05; Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 368–79. *See generally* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995). The Schumer proposal brings together many of the state-level innovations discussed in notes 83–87, *supra*.

94. Standards for Safeguarding Customer Information, 16 C.F.R. pt. 314 (2006).

Safeguards Rule to all private entities storing personal information.[95] The GLBA Safeguards Rule requires financial institutions to design comprehensive information-security programs suited to the consumer data they store.[96] The FTC gives financial institutions the responsibility and discretion to develop and update their security systems to meet today's rapidly changing risk environment.[97]

Although a comprehensive public law solution like the Schumer bill would contribute much to addressing the bursting cyber-reservoirs of the Information Age, such legislation is unlikely to pass. In November 2005, partisan disagreement killed a bill that would have required information brokers to notify consumers about data-security breaches where the broker determined that a breach raised a "significant risk" of identity theft.[98] Many Democrats refused to support a similar bill because it would have "watered down" current state consumer-notification rules by allowing the broker to decide whether a breach warranted disclosure and because it failed to offer consumers the right to access and correct their personal information held by information brokers.[99]

Strong interest-group opposition to comprehensive data-security legislation also might preclude a public law solution. As conceived by public choice theory, Congress is a marketplace where legislation is "sold" by lawmakers and "bought" by beneficiaries of such legislation.[100] Lawmakers provide legislative benefits to groups when it "best serves their

95. Leibowitz Statement, *supra* note 79, at 10 n.25.

96. 16 C.F.R. § 314.3.

97. *See* U.S. FEDERAL TRADE COMM'N, FINAL REPORT OF THE FTC ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY § 3.5 (May 15, 2000), *available at* http://www.ftc.gov/acoas/papers/finalreport.htm; Smedinghoff, *supra* note 28, at 9, 13 (explaining that the FTC and technologists alike agree that information security is a process, not a product, and thus it does not, and cannot, literally dictate what security measures are required); News Release, U.S. Federal Trade Comm'n, FTC Testifies on Security Issues in Global Information-based Economy (Mar. 16, 2006), *available at* http://www.ftc.gov/opa/2006/03/globalitsecurity.htm.

98. Identity Theft Resolution Center, Rutgers University, *House Commerce Passes 'Partisan' Bill, but Bachus Seeks Consensus*, Nov. 2005, *available at* http://www.identitytheft911-sunj.com/articles/article.ext?sp=74 (discussing H.R. 3997, 109th Cong. (2005)). That bill received support by the information brokerage industry, which argued that consumers would not want to be bombarded with notices every time a breach occurred. *Id.*

99. *See* David Lazarus, *Data Theft Bill a Step Backward*, S.F. CHRON., Nov. 6, 2005, at J1 (discussing H.R. 4127, 109th Cong. (2005)).

100. William M. Landes & Richard A. Posner, *The Independent Judiciary in an Interest-group Perspective*, 18 J.L. & ECON. 875, 877 (1975). *See also* Maxwell L. Stearns, *The Public Choice Case Against the Item Veto*, 49 WASH. & LEE L. REV. 385, 400 (1992).

goals, including their primary objective of being re-elected."[101] Members of the larger public, however, tend not to organize and present their demands to lawmakers because they are plagued by free-rider problems—each member knows that an individual contribution will have an imperceptible impact on the group's activity and thus will be inclined to let others make a contribution instead.[102] The efforts of well-organized groups usually prevail over the interests of the larger public because those groups often succeed in distancing the legislator's self-interest from those of the public.[103]

Interest groups may indeed succeed in convincing lawmakers that data-security legislation would undermine their reelection efforts. In May 2006, lobbyists representing the financial services industry, pension planners, and others voiced their opposition to bills limiting the storage of SSNs.[104] Business groups argued that SSNs are critical to financial transactions and "internal security operations," such as employee background checks.[105]

Congress also has an interest in the collection of personal information, as its members use databases containing voters' personal data in

101. Stearns, *supra* note 100, at 400. *See also* ROBERT D. COOTER, THE STRATEGIC CONSTITUTION 67 (2000) (explaining that politicians in a democracy are concerned with the number of votes lobbyists can deliver).

102. MANCUR OLSON, JR., THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS 64 (1965); Herbert Hovenkamp, *Legislation, Well-being, and Public Choice*, 57 U. CHI. L. REV. 63, 87 (1990); Stearns, *supra* note 100, at 401.

103. Cynthia R. Farina & Jeffrey J. Rachlinski, *Foreword: Post-Public Choice?*, 87 CORNELL L. REV. 267, 268 (2002); Saul Levmore, *From Cynicism to Positive Theory in Public Choice*, 87 CORNELL L. REV. 375 , 375 (2002).

104. *See Hearing Before the Subcomm. on Commerce, Trade and Consumer Protection of the H. Comm. on Energy and Commerce*, 109th Cong. 2, 11–13 (2006) (prepared statement of Oliver Ireland on behalf of the Financial Services Coordinating Council), *available at* http://energycommerce.house.gov/108/Hearings/05112006hearing1871/Ireland.pdf [hereinafter Ireland Statement]; Lively Testimony, *supra* note 25; *Social Security Numbers in Commerce: Reconciling Beneficial Uses with Threats to Privacy: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 109th Cong. 5 (2006) (prepared statement of Susan McDonald, President of Pension Benefit Information), *available at* http://energycommerce.house.gov/108/Hearings/05112006hearing1871/McDonald.pdf; *Social Security Numbers in Commerce: Reconciling Beneficial Uses with Threats to Privacy: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 109th Cong. (2006) (prepared statement of Lauren B. Steinfeld, Chief Privacy Officer of the University of Pennsylvania), *available at* http://energycommerce.house.gov/108/Hearings/05112006hearing1871/Steinfeld.pdf. *Cf.* Leland & Zeller, *supra* note 2 (describing strong business opposition to proposed state laws permitting consumers to freeze their credit reports that led to the defeat of proposed legislation in many states).

105. *E.g.*, Ireland Statement, *supra* note 104, at 11.

campaigns.[106] For example, data broker Aristotle International sold voter information to nearly half of the 535 members of Congress in recent years.[107] Because reelection campaigns depend on databases of personal information to court voters, lawmakers may be less inclined to support legislation that would curtail such data collection.[108] As a result, a public solution, although beneficial, may be unlikely in the near future.

To be sure, even in the absence of comprehensive legislation, victims of data-security breaches can sue for negligence. The following part, however, explains why that, too, constitutes an inadequate response to the dangers posed by the insecure cyber-reservoirs of personal data.

IV. NEGLIGENCE LIABILITY AS A POTENTIAL RESPONSE TO THE RELEASE OF SENSITIVE DATA

Several commentators propose a negligence solution for today's insecure databases.[109] Victims of recent data-security breaches are currently pursuing negligence cases against database operators. Those lawsuits allege that database operators failed to reasonably secure sensitive personal information in violation of state statutory law and common law principles.[110]

Cases such as *Kline v. 1500 Massachusetts Avenue Apartment Corp.* support the notion that database operators have a duty to safeguard sensitive data from intruders.[111] In *Kline*, a criminal assaulted the plaintiff

106. Prieto, *supra* note 16, at 18. Indeed, the Republican National Committee maintains a Voter Vault database, which allows party activists to track and solicit voters. Peter Wallsten & Tom Hamburger, *The GOP Knows You Don't Like Anchovies*, L.A. TIMES, June 25, 2006, at M1.

107. Prieto, *supra* note 16, at 18.

108. Members of Congress could exempt themselves from any restrictions on the use of voters' cyber-data. That possibility would not diminish the impact that strong interest-group opposition to a comprehensive legislative solution like the Schumer proposal would have on Members' of Congress reluctance to pass such legislation given their self-interest in reelection.

109. *E.g.*, Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 311 (2005) (suggesting a negligence solution for the release of SSNs); Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1557 (2005) (proposing a cause of action against software manufacturers whose software enables cyber-criminals to access information databases).

110. *See, e.g.*, First Amended Complaint for Declaratory and Injunctive Relief at 2, Parke v. Cardsystems Solutions, Inc., No. CGC-05-442624 (Sup. Ct. Cal. July 5, 2005) (alleging that the defendant failed to adequately secure sensitive personal data of over 40 million California residents, thus allowing hackers to steal plaintiffs' SSNs) (currently pending). *See also supra* note 85 and accompanying text (discussing states that require private entities to employ reasonable security measures over sensitive personal data).

111. Kline v. 1500 Mass. Ave. Apartment Corp., 439 F.2d 477, 480–81 (D.C. Cir. 1970).

tenant in the plaintiff's apartment building's hallway.[112] The court held that the defendant landlord had a duty to reasonably protect the plaintiff from a third party's criminal acts because only the landlord had control over, and the ability to secure, the building's common areas.[113]

Indeed, plaintiffs have successfully argued for an extension of the *Kline* rule to employers whose collections of sensitive data have been stolen by third parties. In *Bell v. Michigan Council 25 of the American Federation of State, County, & Municipal Employees, Local 1023*, for example, a labor union official brought home a list of union members' SSNs.[114] An identity thief somehow obtained the list from the official's home.[115] The court found that the labor union had a duty to protect its members' sensitive personal data from a third party's criminal acts given the fiduciary relationship between them and the foreseeability of identity theft.[116] Thus, negligence lawsuits like *Bell* can operate on their own or as a companion to a public law solution.[117]

When viewed from both an economic and moral perspective, however, it is clear that a negligence regime is inadequate to address the problem of hazardous information reservoirs. Jurists and scholars have long debated the goals of negligence—law-and-economics theorists conceptualize negligence under a cost-benefit analysis,[118] whereas other scholars view negligence through a moral lens.[119] In the discussion that follows, I demonstrate that both approaches converge to the conclusion that

112. *Id.* at 480.

113. *Id.* at 481, 483–84.

114. Bell v. Mich. Council 25 of the Am. Fed'n of State, County, & Mun. Employees, Local 1023, No. 246684, 2005 WL 356306, at *1 (Mich. Ct. App. Feb. 15, 2005).

115. *Id.* at *1.

116. *Id.* at *3–4. *See also* Johnson, *supra* note 109, at 273–34 (arguing for the extension of the *Kline* rule to database operators based on the fiduciary relationship between the operator and the operator's customers). *But see* Thomas J. Smedinghoff, *The Developing U.S. Legal Standard for Cybersecurity*, 4 SEDONA CONF. J. 109, 115 (2003) (suggesting that foreseeability is the cornerstone of liability for database breaches).

117. If Congress adopts a comprehensive bill like the Schumer proposal and the FTC follows its current practices, tort regulation would complement the FTC's performance-based standards, which tell entities what they must accomplish but leave them to decide what technology to use to satisfy the regulation at least cost. *See* Susan Rose-Ackerman, *Tort Law in the Regulatory State*, *in* TORT LAW AND THE PUBLIC INTEREST: COMPETITION, INNOVATION, AND CONSUMER WELFARE 80, 91, 95–96 (Peter H. Schuck ed., 1991). This analysis presumes that state law would not be preempted by federal legislation. The Schumer bill and other similar comprehensive proposals signal Congress's intent not to preempt state laws, a view which is consistent with Congress's vow to leave states free to act on data-security issues in FACTA and GLBA. *See* Identity Theft Resolution Center, *supra* note 98.

118. *E.g.*, Richard A. Posner, *A Theory of Negligence*, 1 J. LEG. STUD. 29, 32–34 (1972).

119. *E.g.*, 3 FOWLER V. HARPER, FLEMING JAMES, JR. & OSCAR S. GRAY, THE LAW OF TORTS 131–32 (2d ed. 1986).

negligence is a suboptimal regime in addressing this important issue of legal policy.

A. THE UNCERTAINTY DILEMMA

The rapidly changing nature of information technologies may create uncertainty as to what a negligence regime entails, blunting its efficiency from a law-and-economics perspective.[120] Under the Judge Learned Hand formula, an actor is negligent if the marginal cost of avoiding an accident is less than the cost of the accident, given the likelihood of the accident's occurrence.[121] Negligence operates optimally when parties can anticipate the law's requirements in a particular circumstance.[122]

The negligence doctrine, however, may not operate optimally when a party is uncertain about the law's requirements.[123] In the face of uncertainty about how negligence will be applied due to rapidly developing technologies, actors may modify their behavior to a greater extent than required by law in order to decrease their chance of liability.[124] Even if the result is economic waste, actors might adopt excessive, and perhaps

120. The question of whether a fault-based system or a strict-liability standard is most economically efficient has been long and carefully debated by prominent scholars and jurists. *See, e.g.*, GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 263, 312 (1970); RICHARD EPSTEIN, TORTS 91–107 (1999); RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 177–92 (6th ed. 2003); Izhak Englard, *The System Builders: A Critical Appraisal of Modern American Tort Theory*, 9 J. LEG. STUD. 27, 51–56 (1980) (comparing the theories of Calabresi and Posner). Although this Article does not endeavor to tackle that abstract question, that debate may be given greater meaning in light of this concrete policy application of efficiency considerations to today's insecure database problem.

121. United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947) (ruling that "if the probability be called P; the injury, L; and the burden, B, liability [in a negligence regime] depends upon whether B is less than L multiplied by P: i.e., whether B < PL."). For a contemporary invocation of the Hand Formula, see *Cross v. Berg Lumber Co.*, 7 P.3d 922, 936 n.3 (Wyo. 2000). Some reject an economic view of optimal deterrence, instead asking whether the social benefits gained by reducing the risk of injury outweigh the social costs incurred to reduce the risk. KENNETH S. ABRAHAM, THE FORMS AND FUNCTIONS OF TORT LAW 15–16 (2d ed. 2002).

122. *See* ABRAHAM, *supra* note 121, at 16; STEVEN SHAVELL, ECONOMIC ANALYSIS OF LAW 46–47, 59 (2004) (explaining that when a due-care level is chosen by courts to equal the socially optimal level of care, the injurers will be led to exercise due care); Kenneth S. Abraham, *The Trouble with Negligence*, 54 VAND. L. REV. 1187, 1222 (2001).

123. *See* Richard Craswell & John E. Calfee, *Deterrence and Uncertain Legal Standards*, 2 J.L. ECON. & ORG. 279, 279–80 (1986).

124. Guiseppe Dari-Mattiacci, *Errors and the Functioning of Tort Liability*, 13 SUP. CT. ECON. REV. 165, 169, 186 (2005) (explaining how uncertainty in liability rules and damages often yield higher levels of precaution); Jason Scott Johnston, *Uncertainty, Chaos, and the Torts Process: An Economic Analysis of Legal Form*, 76 CORNELL L. REV. 341, 359 (1991).

inefficient, precautions in a negligence regime in order to bolster their claim to have exercised due care should litigation arise.[125]

Due to the rapidly changing threats to information security, database operators will likely be uncertain as to what constitutes optimal care. Cyber-intruders employ increasingly innovative techniques to bypass security measures and steal personal data,[126] thereby requiring an ever-changing information-security response to new threats, vulnerabilities, and technologies.[127] A database operator's uncertainty about the contours of due care may prompt it to take too much precaution. Such overcompliance with the law risks inhibiting socially useful data collection.[128]

B. RESIDUAL RISK

A negligence regime will fail to address the significant leaks that will occur despite database operators' exercise of due care over personal data. Security breaches are an inevitable byproduct of collecting sensitive

125. *See* Craswell & Calfee, *supra* note 123, at 299; Mark F. Grady, *A New Positive Economic Theory of Negligence*, 92 YALE L.J. 799, 809–12 (1983).

126. *See* SYMANTEC, COMPREHENSIVE THREAT MANAGEMENT: A SYMANTEC SOLUTION FOR MODERN-DAY ATTACK PROTECTION 4–5 (2006), http://wp.bitpipe.com/resource/org_939987896_418/10510712_CTM_wp_edp.pdf?site_cd=fbs (explaining that hacker motivation to make money, coupled with a lower bar for developing malicious software, has steadily increased the number of threats to computer security); THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 8 (Feb. 2003), *available at* http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf [hereinafter NATIONAL STRATEGY]; Smedinghoff, *supra* note 28, at 17. Due to the plethora of tools used by hackers, there has been a "precipitous drop in the time that it takes for a new threat to be developed." SYMANTEC, *supra*, at 5. *See also* DAVID SANCHO, ROOTKITS: THE NEW WAVE OF INVISIBLE MALWARE IS HERE (2005), http://www.trendmicro.com/NR/rdonlyres/388874B6-C27C-4354-9078-42771EABEBB1/18503/rootkitwp.pdf (explaining the emergence of rootkits technology used by malware developers to infiltrate computers that is difficult to detect with antiviral software); Joris Evers, *Office Hit by Another Security Problem*, CNET NEWS.COM, June 22, 2006, http://news.zdnet.com/Office+hit+by+another+security+problem/2100-1009_22-6087161.html (explaining a weakness in software that allows cyber-attackers to access sensitive information).

127. *See* NATIONAL STRATEGY, *supra* note 126, at 5, 8–9; Smedinghoff, *supra* note 28, at 17 (explaining that information security is a "moving target").

128. Uncertainty in the negligence standard also compounds the challenges faced by jurors assessing the care taken by a defendant in its information-security practices. While lay juries ordinarily have difficulty assessing negligence in complicated technical cases, juries may have an especially challenging time assessing a database operator's care over its security system given the rapid changes in technologies and new risks, which will cause experts to present diverging, yet convincing, views. *See* STEPHEN BREYER, ECONOMIC REASONING AND JUDICIAL REVIEW, AEI-BROOKINGS JOINT CENTER 2003 DISTINGUISHED LECTURE 12 (Dec. 4, 2003) (2004) (noting the difficulty courts have in assessing the "outer bounds of what is reasonable in technical subject matter areas" such as those involving computers where the parties offer warring expert testimony). Although judges serve as gatekeepers over the admissibility of technical expert testimony under *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 147 (1999), jurors will still wrestle with the clashing views of computer security experts whose testimony is deemed admissible.

personal information in computer databases.[129] No amount of due care will prevent significant amounts of sensitive data from escaping into the hands of cyber-criminals. Such data leaks constitute the predictable residual risks of information reservoirs.

Consequently, negligence will not efficiently manage the residual risks of hazardous databases. Negligence would neither induce database operators to change their activity level nor discourage marginal actors from collecting sensitive information because such operators need not pay for the accident costs of their residual risk.[130]

The high levels of residual risk suggest treating cyber-reservoirs as ultrahazardous activities—those with significant social utility and significant risk—that warrant strict liability.[131] As Judge Richard Posner has explained, ultrahazardous activities often involve something "new" that society has "little experience" securing, where neither the injurer nor victim

129. *See* LAWRENCE A. GORDON ET AL., COMPUTER SECURITY INSTITUTE, 2005 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 11 (2005), *available at* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf (explaining that "[t]echnical computer security measures such as use of passwords, biometrics, anti-virus software and intrusion detection systems cannot totally reduce an organization's risk of computer security breaches and the associated financial losses"); PHOENIX TRUSTCONNECTOR, THE TRUSTED-CONNECTION LANDSCAPE 1 (Sept. 1, 2005), http://research.telephonyonline.com/detail/RES/1126533537_228.html&src=TRM_TOPN (explaining that despite firewalls, intrusion detection systems, and user authentication tools, information systems are being successfully penetrated due to rapid growth of malicious software and innovative hackers); John Dobberstein, *Crime Online: State Businesses, Law Enforcement Officials and Other Groups Are Trying to Stop Hackers and Cyber Terrorists*, TULSA WORLD, July 23, 2006, at E1 (citing survey results establishing that passwords, biometrics, anti-virus software, and intrusion detection systems "cannot totally reduce an organization's risk of computer security breaches"); Smedinghoff, *supra* note 28, at 19 (noting that "[a]t some level, security breaches may be inevitable").

130. *See* SHAVELL, *supra* note 122, at 46.

131. Today's hazardous cyber-reservoirs would fall outside the current *Restatement*'s description of abnormally dangerous activities. *See, e.g.*, RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL HARM § 20 (Proposed Final Draft No. 1, Apr. 6, 2005) (abnormally dangerous activities must involve "a . . . risk of *physical* harm" (emphasis added)); Rosenblatt v. Exxon Co., U.S.A., 642 A.2d 180, 188 (Md. 1994) (declining to extend the doctrine of strict liability to embrace economic harm). Nonetheless, information reservoirs share the defining characteristics of the *Restatement*'s abnormally dangerous activities such as blasting and water reservoirs—high utility and high risk. In Kenneth Abraham's view, abnormally dangerous activities are governed by strict liability so as to protect victims who "are unlikely to know much about" the activity and cannot protect themselves against its risks. ABRAHAM, *supra* note 121, at 169. This rationale applies to information reservoirs as individuals whose data is collected by data brokers know little about where their data resides and can do nothing to prevent database operators from amassing their sensitive data. Although hazardous information reservoirs do not fall within the *Restatement* prescription of an abnormally dangerous activity, a strong argument exists for extending that definition of abnormally dangerous activities to include bursting cyber-reservoirs. In revisiting the *Restatement* view of abnormally dangerous activities, the American Law Institute ought to consider compensable harm in the twenty-first century to include injuries to our market identity caused by the release of sensitive personal data. *See infra* Part IV.D. (discussing the need for a change in our conception of harm in the Information Age).

can prevent the accident by taking greater care.[132] This characterized water reservoirs in nineteenth-century England.[133] Strict liability creates an incentive for actors engaging in ultrahazardous activities to "cut back on the scale of the activity . . . to slow its spread while more is learned about conducting it safely."[134]

Classifying database collection as an ultrahazardous activity is a logical extension of Posner's analysis. Just as no clear safety standard governing the building and maintenance of water reservoirs had emerged in the 1850s, a stable set of information-security practices has not yet materialized today.[135] Individuals can do nothing to ensure their information remains safely inside an entity's database, especially those who have no idea that their data resides there. Database operators, too, are limited in what they can do to protect cyber-reservoirs from significant leaks given the "inevitability" of data-security breaches, even with seemingly responsible levels of precaution against such breaches.[136]

In this analysis, strict liability has the potential to encourage a change in activity level respecting the storage of sensitive personal information, unless and until more information allows operators to better assess optimal precaution levels and to respond to the persistent problem of residual risk.[137] Because strict liability would force database operators to internalize the full costs of their activities, marginally productive database operators might refrain from maintaining cyber-reservoirs of personal data. Strict liability also may decrease the collection of ultrasensitive data among those who are at greatest risk of security breaches. Moreover, as insurance markets develop in this emerging area, database operators that continue collecting sensitive information will be better positioned to assess the cost

132. Ind. Harbor Belt R.R. v. Am. Cyanamid Co., 916 F.2d 1174, 1177 (7th Cir. 1990) (Posner, J.); POSNER, *supra* note 120, at 180 (citing A.W.B. Simpson, *Legal Liability for Bursting Reservoirs: The Historical Context of* Rylands v. Fletcher, 13 J. LEGAL STUD. 209 (1984)).

133. POSNER, *supra* note 120, at 180.

134. *Id.*

135. *See supra* Part IV.A–B (discussing cyber-security).

136. *See* Smedinghoff, *supra* note 28, at 19.

137. For example, employers storing employee SSNs for tax reporting can discontinue using them as a form of employee identification. *See Stolen Social Security Number Records Prompt Lawsuit Against Union Pacific*, 29 U.S. RAIL NEWS 111 (2006) (describing a complaint asserting that a data-security breach resulted from a company's use of employee SSNs for identification and arguing that the employer should only have used SSNs for tax reporting). Organizations can also disconnect databases containing ultrasensitive information from the Internet to prevent hacking. Additionally, organizations can store biometric information on Smart Cards, which permit individuals to carry their biometrics on a card, instead of in centralized databases subject to theft. *See* Int'l Biometric, *supra* note 67, at 22, 24; Sethi, *supra* note 34, at 120–21.

of residual risk and the extent to which they can spread the cost of such risk onto consumers.[138]

Negligence lawsuits also fail to efficiently spread the costs of such residual harm. Law-and-economics scholars suggest that a liability regime should efficiently allocate the risk of unavoidable accident costs.[139] This is only true when it is less costly for the industry to bear the cost of all accidents than for individual victims to purchase insurance.[140] In the context of cyber-reservoirs, the most efficient cost-spreader is the database operator who need only buy one cyber-security insurance policy as opposed to the millions of identity-theft insurance policies that would be purchased by consumers.[141] The cost-spreading advantages of database operators resemble those of defective-product manufacturers who sit in the best position to obtain insurance and distribute its costs "among the public as a cost of doing business" as opposed to only injured individuals.[142]

138. *See* Jon D. Hanson & Kyle D. Logue, *The First-party Insurance Externality: An Economic Justification for Enterprise Liability*, 76 CORNELL L. REV. 129, 135, 137–38 (1991).

139. *E.g.*, *id.*; John E. Calfee & Clifford Winston, *Economic Aspects of Liability Rules and Liability Insurance*, *in* LIABILITY: PERSPECTIVES AND POLICY 16, 16 (Robert E. Litan & Clifford Winston eds., 1988).

140. *See* POSNER, *supra* note 120, at 181.

141. *See infra* note 239 (discussing the availability of cyber-risk insurance to database operators that covers third-party losses due to leaks of sensitive data and identity-theft insurance available to individuals). When the demand for a good is inelastic, a seller's ability to pass on the cost of insurance to consumers is strong. Emerging technologies that offer highly valued services in thin markets, meaning that there are few substitutes, including massive computer databases containing sensitive information, are paradigmatic illustrations of markets characterized by inelastic demand. For a discussion of the concept of elasticity, see RICHARD A. IPPOLITO, ECONOMICS FOR LAWYERS 131–39 (2005); PAUL A. SAMUELSON & WILLIAM D. NORDHAUS, ECONOMICS 64–70 (16th ed. 1998).

142. Escola v. Coca Cola Bottling Co. of Fresno, 150 P.2d 436, 441 (Cal. 1944) (Traynor, J., concurring). The maintenance of hazardous information reservoirs parallels the manufacture of defective products in other ways as well. Just as a person injured by a product is "not ordinarily in a position to refute . . . evidence [about a manufacturing process] or identify the cause of the defect," *id.*, here, too, individuals will have great difficulty identifying the flaws in a database operator's security system and proving a database operator's negligence. And like the consumer who lacks the skill to investigate the soundness of a product, individuals have no knowledge about where their data resides, let alone the ability to assess the security provided their personal data. See generally KENNETH S. ABRAHAM, DISTRIBUTING RISK: INSURANCE, LEGAL THEORY, AND PUBLIC POLICY 64–100 (1986) and Kenneth S. Abraham, *Liability Insurance and Accident Prevention: The Evolution of an Idea*, 64 MD. L. REV. 573 (2005) for insightful discussions of liability insurance.

C. ABSENCE OF CLEAR NORMS

Scholars espousing a moral view conceive of negligence as setting forth norms to guide future behavior.[143] A preexisting norm of safe cyber-security practices, however, cannot be established given the ever-changing tactics, and increasing sophistication, of those seeking to bypass cyber-security measures to steal valuable personal data and the rapid proliferation of computer network vulnerabilities.[144] Because information security is a "moving target," negligence litigation cannot signal to database operators reasonable cyber-security practices to follow.[145] As Kenneth Abraham argues, "[i]n the absence of independent, pre-existing norms of behavior, the very idea of negligence is shaky."[146]

In sum, the Information Age's insecure cyber-reservoirs require a different solution given the deficiencies of a negligence regime. As Mark Geistfeld explains, "[w]henever negligence liability loses its deterrence advantage," strict liability better addresses "risk reduction and injury compensation."[147] The following part explores the law's treatment of the valuable yet highly risky technologies of another era—the Industrial Age—and the *Rylands* model of strict liability for entities gathering substances that do serious mischief upon their escape. It lays the groundwork for adopting *Rylands* to manage the harm of the Information Age's hazardous cyber-reservoirs.

V. LESSONS FROM THE DAWN OF ANOTHER AGE: STRICT LIABILITY UNDER *RYLANDS V. FLETCHER*

Oliver Wendell Holmes offered strict liability as a solution when negligence could not deter unsafe practices: "the safest way to secure care is to throw the risk upon the person who decides what precautions shall be

143. *See* Abraham, *supra* note 122, at 1191; Robert E. Keeton, *Is There a Place for Negligence in Modern Tort Law?*, 53 VA. L. REV. 886, 889–90 (1967) (explaining that adjudications of negligence "place [a] mark of legal disapproval, with all its practical consequences, on identifiable types of conduct [that] may influence the attitudes and future behavior" of others); Benjamin C. Zipursky, *Civil Recourse, Not Corrective Justice*, 91 GEO. L.J. 695, 743 (2003) (explaining that the norms of tort law are "directive and conduct-oriented: they enjoin persons from treating others in certain ways and from interfering with others' interests in certain ways," serving as "guidance rules").

144. *See* NATIONAL STRATEGY, *supra* note 126, at 8; SYMANTEC, *supra* note 126, at 4–5 (explaining that hacker motivation to make money, coupled with a lower bar for developing malicious software, has steadily increased the number of threats to computer security).

145. *See* Smedinghoff, *supra* note 28, at 17.

146. Abraham, *supra* note 122, at 1203, 1223.

147. Mark Geistfeld, *Negligence, Compensation, and the Coherence of Tort Law*, 91 GEO. L.J. 585, 618 (2003).

taken."[148] Holmes highlighted *Rylands* as a model for redressing the dangers of rapidly changing technologies at the dawn of the Industrial Age.[149] Holmes's words have great significance as we find ourselves in a time of accelerating technological change in this Information Age.

This part explores *Rylands* and the classic accounts of that decision in the Industrial Age. Many of the debates surrounding *Rylands* purport to be about justice but in fact reflect the economic necessities of the era.[150] At the time of *Rylands*, Britain had sustained a generation of economic expansion largely associated with industrialization.[151] Great technological progress catapulted the British standard of living well above that of any other nation.[152] America, on the other hand, had just begun its industrial journey in the 1860s.[153] Nevertheless, many of the arguments against the application of *Rylands* in the United States receded as the country's economy strengthened and as the risks of bursting reservoirs and other industrial hazards escalated.[154]

148. O.W. HOLMES, JR., THE COMMON LAW 117 (Boston, Little, Brown, & Co. 1881); Abraham, *supra* note 122, at 1222 (explaining that "flaws in the negligence standard should make us much more willing to consider proposals for no-fault alternatives to liability for negligence"). Although Holmes is widely regarded as a proponent of negligence and a foe of strict liability, Holmes approved of strict liability for the foreseeable risks of high risk and high social utility activities such as the maintenance of reservoirs. *See The Theory of Torts*, 7 AM. L. REV. 652, 653, 663 (1873) (wherein Holmes discusses the justifications for strict liability vis-à-vis *Rylands v. Fletcher*); DAVID ROSENBERG, THE HIDDEN HOLMES: HIS THEORY OF TORTS IN HISTORY 9 (1995) (noting that many scholars overlooked Holmes's approval of *Rylands*).

149. *The Theory of Torts*, *supra* note 148, at 653, 663.

150. *See* FRIEDMAN, *supra* note 3, at 356–66, 519. *See also* MORTON J. HORWITZ, THE TRANSFORMATION OF AMERICAN LAW 1870–1960: THE CRISIS OF LEGAL ORTHODOXY 142 (1992) (discussing how social and economic necessities influence legal decisions).

151. BENJAMIN M. FRIEDMAN, THE MORAL CONSEQUENCES OF ECONOMIC GROWTH 224 (2005).

152. *Id.* at 54.

153. *See id.*

154. *See infra* notes 208–16. The evolving law of water rights in the nineteenth century similarly illustrates the profound role played by economic concerns in the shaping of law. *See* MORTON J. HORWITZ, THE TRANSFORMATION OF AMERICAN LAW 1780–1860, at 34–35 (1977). In the early nineteenth century, courts viewed land not as a productive asset but as a private estate to be enjoyed for its own sake, finding any nonconsensual interference with the natural flow of water illegal. *Id.* at 36. As industrialization began to take root, however, courts eroded the restrictive common law rules to permit extensive, uncompensated use of water for business purposes. *Id.* at 36–37. As the economy strengthened during the second quarter of the nineteenth century, courts began to strike a balance between competing land uses, only freeing economically desirable but injurious activities from legal liability if they were exercised with due care. *Id.* at 102.

A. THE *RYLANDS V. FLETCHER* MODEL

Rylands v. Fletcher stands as a prominent example of strict liability in the Industrial Age.[155] John Rylands, a textile mill owner in Lancaster, England, hired a contractor to build a reservoir because he needed an additional source of water for his steam-powered mill.[156] In 1860, the reservoir failed and the water escaped into an abandoned mine shaft that connected with neighboring active coal mines owned by Thomas Fletcher.[157] The reservoir water flooded the interlocking maze of tunnels, forcing Fletcher to abandon his coal mines.[158]

Fletcher sued Rylands in the Court of the Exchequer, where he lost.[159] Fletcher then appealed to the Exchequer Chamber and won.[160] Although Rylands might have been held liable for the negligence of his contractors who built the reservoir,[161] the Exchequer Chamber judges held him liable regardless of fault.[162] The House of Lords affirmed.[163] Lord Chancellor held that a person who "brings on his land and collects and keeps there anything likely to do mischief if it escapes" must pay for all of the damage that "is the natural consequence of its escape."[164]

This century's problem of escaping cyber-data is analogous to *Rylands*'s nineteenth-century response to collected substances that do mischief upon their escape. Some might suggest that the intervention of a third party, such as a hacker, would not fall within the "natural consequences" contemplated by *Rylands*. *Rylands* itself, however, involved an intervening actor—the contractor who negligently built the reservoir. More importantly, it is the collection of massive amounts of sensitive digital information in databases that creates the opportunity for leaks and misbehavior by third parties in much the same way that the collection of water in reservoirs rendered the water inside vulnerable to negligent construction of the dam or gravity itself. A third party's criminal acts are the natural consequences of maintaining information reservoirs in much the

155. *See* Rylands v. Fletcher, (1868) 3 L.R.E. & I. App. 330, 338–40 (H.L.); Kenneth S. Abraham, Rylands v. Fletcher*: Tort Law's Conscience*, *in* TORTS STORIES 207, 207 (Robert L. Rabin & Stephen D. Sugarman eds., 2003).

156. Fletcher v. Rylands, (1865) 159 Eng. Rep. 737, 739–40 (Exch.).

157. *Id.*

158. Simpson, *supra* note 132, at 241–42.

159. *Fletcher*, 159 Eng. Rep. at 743–47.

160. Fletcher v. Rylands, (1866) 1 L.R. Exch. 265, 279 (Exch.).

161. 3 HARPER ET AL., *supra* note 119, at 191.

162. *Fletcher*, 1 L.R. Exch. at 279.

163. Rylands v. Fletcher, (1868) 3 L.R.E. & I. App. 330, 338–40, 342 (H.L.).

164. *Id.* (quoting *Fletcher*, 1 L.R. Exch. at 279).

same way that flooding due to gravity or negligence naturally accompanied water reservoirs.

Thus, for analytic purposes, leaks due to hacking are akin to the pull of gravity on water reservoirs. Any possible resistance to applying *Rylands* to cases involving the criminal acts of third parties on the grounds that the criminal actor ought to be found and pursued for the victim's damages is seemingly inapplicable here given the illusive nature of criminal hackers who mask their identities and strike from unidentifiable distances. The criminal acts of computer hackers constitute the "natural consequences" of amassing sensitive databases given the statistical certainty that such computer hackers will breach computer databases to steal sensitive personal data.[165] Furthermore, I offer the *Rylands* model as a metaphor to conceptualize the utility and the risks of information reservoirs at the dawn of the Information Age, not as a direct doctrinal fit.[166]

The following sections will explore the intellectual reactions to *Rylands* and the substantive merits of applying a formulation minted at the dawn of one economic era to the problems of another.

B. THE CLASSIC RESPONSES TO *RYLANDS*

In the Industrial Age, commentators grappled with the law's response to accidents caused by the flooding of reservoirs critical to industry. In some respects, their thinking tracked the arc of the economy as it emerged from a fledgling industrializing state to a vibrant industrialized one. In other respects, their views reflected the morality of the times.

In Britain and the United States, intellectuals of the Industrial Age hailed from several different schools of thought, including formalism, utilitarianism, materialism, and economic moralism. This section discusses the British response to *Rylands* and then turns to the American reaction to the decision that followed in the 1870s.[167]

165. *See supra* text accompanying notes 46–72 (discussing the ultrahazardous nature of computer databases).

166. *See infra* text accompanying notes 217–24 (discussing *Rylands* as a powerful metaphor to conceptualize the new cyber-harms of the twenty-first century).

167. *See, e.g.*, Brown v. Collins, 53 N.H. 442, 449–50 (1873) (finding *Rylands* "contrary to American authority, as well as to [the Court's] understanding of legal principles").

1. The British Response

a. Formalists

British formalists stressed the logical consistency of legal opinions.[168] The Lords who heard *Rylands* demonstrated their formalist approach when they professed that the case did not involve a novel proposition.[169] As the Lord Chancellor observed, "the principles on which this case must be determined appear . . . to be extremely simple."[170] The judges promulgated a general rule of strict liability for escaping substances, of which liability for the escape of fire, cattle, or water was an example.[171] Because British courts endorsed strict liability for other things or substances before *Rylands*, the Lords asserted that they were simply upholding prevailing legal principles.[172]

b. Utilitarians

The utilitarians envisioned tort law as a tool of social progress.[173] To them, *Rylands* responded to the "magnitude of the danger" posed by reservoirs and other industrial hazards.[174] The desire to eliminate future accidents, most especially those involving exploding dams, precipitated

168. *See* LOUIS MENAND, THE METAPHYSICAL CLUB 339 (2001); Roscoe Pound, *The End of Law as Developed in Legal Rules and Doctrines*, 27 HARV. L. REV. 195, 204 (1914). "[F]ormalism maintains that because law is internally intelligible, it does not require, nor would it be useful for it to have, the assistance of any external discipline, such as history, economics, social science, or philosophy, as part of its understanding or justification." Ken Kress, *Formalism, Corrective Justice and Tort Law*, 77 IOWA L. REV. i, i (1992).

169. *See* 3 HARPER ET AL., *supra* note 119, at 190; F.H. Newark, *The Boundaries of Nuisance*, 65 L.Q. REV. 480, 487 (1949).

170. Rylands v. Fletcher, (1868) 3 L.R.E. & I. App. 330, 338 (H.L.).

171. *See* Fletcher v. Rylands, (1866) 1 L.R. Exch. 265, 279–81 (Exch.); 3 HARPER ET AL., *supra* note 119, at 191–92. *But cf.* Ezra R. Thayer, *Judicial Legislation: Its Legitimate Function in the Development of the Common Law*, 5 HARV. L. REV. 172, 184–85 (1892) (embracing a scientific approach to tort law, a subspecies of formalism, which questions the extent to which *Rylands* truly follows from established tort law involving fire and escaping cows).

172. *See* Newark, *supra* note 169, at 487. At the time of *Rylands*, the English tradition distinguishing trespass and trespass on the case prevailed, a distinction that is largely extinct in contemporary times. I do not mean to equate the nature of the interest invaded in *Rylands*—land—with that harmed by the release of cyber-data today. Instead, this Article discusses why *Rylands* serves as a powerful metaphor for the release of sensitive personal data from the Information Age's cyber-reservoirs.

173. *See* MENAND, *supra* note 168, at 339 (grouping legal theories that emphasize social consequences of the law under the rubric "utilitarian"); 1 ROSCOE POUND, JURISPRUDENCE 512–13 (1959); Zipursky, *supra* note 143, at 696. Utilitarian judges "fashioned rules" to prevent "future harms." *See* Leon Green, *The Duty Problem in Negligence Cases: II*, 29 COLUM. L. REV. 255, 255–56 (1929).

174. FREDERICK POLLOCK, THE LAW OF TORTS 307 (Phila., Blackstone Publ'g Co. 1887); Frederick Pollock, *Duties of Insuring Safety: The Rule in* Rylands v. Fletcher, 2 L.Q. REV. 52 (1886) [hereinafter Pollock, *Duties*].

Rylands,[175] as did the wish to provide compensation for the injuries they caused.[176]

In 1887, Sir Frederick Pollock explained that British law "takes notice" that certain activities are a source of "extraordinary risk" such that a person who exposes his neighbor to such risks must "insure" his neighbor against harm, even if the activity itself is not wrongful.[177] Pollock noted that because *Rylands* was a "hard rule," it needed strong evidentiary support or "clear grounds of policy."[178] The prevention or compensation, or both, of flooding reservoirs warranted *Rylands*.[179]

2. The American Response

a. Materialists

American materialists envisioned judicial decisions as a measure of, and a tool to promote, industry's health.[180] To some, the affluence of British industry explained and justified the decision,[181] as mill owners could afford to pay for the accidents they caused regardless of fault.[182] But

175. *See* John Murphy, *The Merits of* Rylands v. Fletcher, 24 OXFORD J. LEGAL STUD. 643, 649 (2004) (explaining that three references to alkali works in the Exchequer Chamber's decision in *Rylands* illustrate that concerns of industrial harms were on the forefront of judges' minds). Deadly reservoir failures occurred just before, and during, the *Rylands* decisions, raising the public's fear about the collection of water in reservoirs. Simpson, *supra* note 132, at 244–51 (arguing that well–known dam failures prompted *Rylands*). *See also* ROSCOE POUND, INTERPRETATIONS OF LEGAL HISTORY 109 (1923) (explaining that *Rylands* reflected a social-justice ethic prominent in 1860s England that sought to protect individuals from industrial harm and provided for the public's "general security").

176. *See* POLLOCK, *supra* note 174, at 307; Pollock, *Duties*, *supra* note 174, at 52.

177. POLLOCK, *supra* note 174, at 307.

178. *Id.* at 311.

179. *See id.*; POUND, *supra* note 175, at 109.

180. *See* JOHN FABIAN WITT, THE ACCIDENTAL REPUBLIC: CRIPPLED WORKINGMEN, DESTITUTE WIDOWS, AND THE REMAKING OF AMERICAN LAW 8 (2004).

181. *See* FRANCIS H. BOHLEN, STUDIES IN THE LAW OF TORTS 351 (1926) [hereinafter BOHLEN, STUDIES]; Francis H. Bohlen, *The Rule in* Rylands v. Fletcher*: Part I*, 59 U. PA. L. REV. 298, 303 (1911); Leon Green, *Tort Law Public Law in Disguise*, 38 TEX. L. REV. 1, 5 (1960).

182. *See* BOHLEN, STUDIES, *supra* note 181, at 368–69 ("What may appear desirable in an ancient and highly organized society whose natural resources have been gradually and fully developed may be utterly inappropriate and harmful in a newly settled country whose natural resources still require exploitation."); Green, *supra* note 181, at 5 ("[W]e do know that in England at this time a new and prosperous industry as milling could well afford to bear the risks it imposed on the older and equally if not more important mining industry."); Kenzo Takayanagi, *Liability Without Fault in the Modern Civil and Common Law*, 16 ILL. L. REV. 163, 168 (1921) (attributing the *Rylands* decision to the growth of commerce and the rise of large-scale enterprises that could spread the cost of accidents). Bohlen also suggested, to much criticism, that the judges hearing the case in the House of Lords hailed from or aspired to the landed gentry and thus adopted a rule that would advance the protection of their interests over the commercial interests of the enterprising middle class. BOHLEN, STUDIES, *supra* note 181, at 369. Others have refuted this classist explanation of *Rylands*. *See* POUND, *supra* note 175, at 106–07.

the materialists objected to the application of *Rylands* to 1870s America.[183] They reasoned that the fledgling U.S. industry could not grow if it was saddled with the costs of faultless accidents.[184] In *Brown v. Collins*,[185] Judge Charles Doe of the New Hampshire Supreme Court captured the materialists' concerns, declaring *Rylands* antithetical to "progress and improvement."[186] The materialists explained that *Rylands* would at least slow down the journey toward civilization and economic growth,[187] and, at worst, "bring all economic action to a halt."[188]

b. Utilitarians

American utilitarians, much like their British counterparts, envisioned *Rylands* as a means to combat industrial hazards. *Rylands* would "pressure" industry to "keep in hand" dangerous conditions for the public's safety.[189] Utilitarians looked to Oliver Wendell Holmes who wrote, in 1873, that *Rylands* was a "politic" means to prevent dangers caused by "extra-hazardous" activities,[190] such as reservoirs and other new industrial risks.[191]

See generally Robert Thomas Molloy, Fletcher v. Rylands*: A Reexamination of Juristic Origins*, 9 U. CHI. L. REV. 266 (1942) (explaining that the middle-class backgrounds of some House of Lords judges refutes Bohlen's class thesis).

183. *See* BOHLEN, STUDIES, *supra* note 181, at 369 (explaining the U.S. rejection of *Rylands* as partly attributable to the country's pressing need to encourage material development); Green, *supra* note 181, at 5 (same).

184. FRIEDMAN, *supra* note 3, at 351 (explaining that absolute liability rules like that imposed in *Rylands* were initially rejected in the United States because they risked strangling the economy); W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS 548–49 (5th ed. 1984) (explaining that late-nineteenth-century courts rejected the strict-liability standard because it would be too great a burden on the industrial and commercial development of the country). *But see generally* Gary T. Schwartz, *Tort Law and the Economy in Nineteenth–century America: A Reinterpretation*, 90 YALE L.J. 1717 (1981) (rejecting the thesis that tort law of the nineteenth century adopted a fault-based standard in order to subsidize industry).

185. Brown v. Collins, 53 N.H. 442 (1873).

186. *Id.* at 448. *See also* Losee v. Buchanan, 51 N.Y. 476, 484 (1873) (condemning the strict-liability rule of *Rylands* as incompatible with the development of "factories, machinery, dams, canals and railroads"); Pa. Coal Co. v. Sanderson, 6 A. 453, 459–60 (Pa. 1886) (rejecting *Rylands* as "wholly inapplicable" to the case at bar and noting that the coal industry serves "a great public interest").

187. II SEYMOUR D. THOMPSON, THE LAW OF NEGLIGENCE IN RELATIONS NOT RESTING IN CONTRACT 1234–35 (St. Louis, F.H. Thomas & Co. 1880). *See also* Jed Handelsman Shugerman, Note, *The Floodgates of Strict Liability: Bursting Reservoirs and the Adoption of* Fletcher v. Rylands *in the Gilded Age*, 110 YALE L.J. 333, 348–49, 350 (2000) (explaining that New York and New Hampshire court decisions in the late nineteenth century suggested a concern for economic growth that outweighed the desire to protect urban populations from industrial risks).

188. WITT, *supra* note 180, at 48. *See also* FOWLER VINCENT HARPER, A TREATISE ON THE LAW OF TORTS 338 (1933) (explaining that the early rejection of *Rylands* in the U.S. grew out of concern for the business community).

189. *See* POUND *supra* note 175, at 109–10.

190. Davis v. Rich, 62 N.E. 375, 377 (Mass. 1902) (Holmes, C.J.) ("When knowledge of the damage done or threatened to the public is established, the strict rule of *Rylands v. Fletcher* is not in

Dam tragedies in the 1880s prompted utilitarians to call for the adoption of *Rylands*. In 1889, a dam at an exclusive club in Johnstown, Pennsylvania, broke.[192] Two thousand people died and $17 million in property was destroyed.[193] That year, editors of the *American Law Review*[194] asked "[w]hat is the responsibility of a corporation or person who collects on his land a vast body of water, and does not sufficiently restrain it as to prevent its being turned loose . . . upon the unsuspecting inhabitants below?"[195] The authors argued that *Rylands* offered the "best answer."[196]

c. Economic Moralists

Economic moralists advocated individual self-determination under a *laissez-faire* philosophy of natural justice.[197] For them, *Rylands* offended morality by imposing liability on those not at fault for accidents.[198]

question."); *The Theory of Torts*, *supra* note 148, at 653, 663. As Louis Menand explains, Holmes did not view the law from a monolithic utilitarian lens. MENAND, *supra* note 168, at 341 (explaining that Holmes saw law's development as guided by utility, morality, doctrinal consistency, and historical concerns). *See supra* note 148 and accompanying text (describing scholarly interpretations of Holmes's views on negligence and strict liability).

191. *The Theory of Torts*, *supra* note 148, at 663. Holmes's "extra-hazardous" activities bear a strong connection to contemporary concepts of abnormally dangerous or ultrahazardous activities. *Compare id.* at 653, 666, *with* RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL HARM § 20 (Proposed Final Draft No. 1, Apr. 6, 2005) (stating that abnormally dangerous activities subject the actor to strict liability for physical harm caused by that activity), *and* RESTATEMENT (SECOND) OF TORTS § 520 (1977) (explaining that courts, in determining whether an activity is abnormally dangerous, should consider, among other things, the high degree of risk of harm to the person, land, or chattel and the extent to which the activity is not a matter of common usage). *See supra* note 131 (discussing how a *Rylands* approach to today's insecure cyber-reservoirs might accord with the *Restatement* view).

192. DAVID G. MCCULLOUGH, THE JOHNSTOWN FLOOD 264 (1968); NORMAN SMITH, A HISTORY OF DAMS 177–78 (1971).

193. MCCULLOUGH, *supra* note 192, at 264; SMITH, *supra* note 192, at 177–78.

194. The *American Law Review*, a bimonthly publication, was probably "the most influential legal periodical of the nineteenth century." THOMAS A. WOXLAND & PATTI J. OGDEN, LANDMARKS IN AMERICAN LEGAL PUBLISHING 48 (1990).

195. Note, *The Law of Bursting Reservoirs*, 23 AM. L. REV. 643, 646 (1889).

196. *Id.* at 647. *See also* Ariz. Employers' Liab. Cases, 250 U.S. 400, 432–33 (1919) (Holmes, J., concurring) ("There is no more certain way of securing attention to the safety of the men . . . than by holding the employer liable for accidents. . . . [T]hey probably will happen a good deal less often when the employer knows that he must answer for them if they do."); Robert J. Kaczorowski, *The Common-law Background of Nineteenth-century Tort Law*, 51 OHIO ST. L.J. 1127, 1128 (1990) (explaining that nineteenth-century judges used tort law as a tool to encourage moral behavior, minimize injuries, and promote honesty and fair dealing in economic relationships); Takayanagi, *supra* note 182, at 172.

197. *See* BERNARD SCHWARTZ, THE LAW IN AMERICA 78 (1974) (explaining nineteenth-century tort law's deference to free individual action and decision).

198. *See* WITT, *supra* note 180, at 47 (explaining the view that strict liability unethically fined the "free exercise of the nonnegligent injurer's rights"); James Barr Ames, *Law and Morals*, 22 HARV. L. REV. 97, 99, 103 (1908).

Economic moralists envisioned "man [as] a free agent to be left to his own fortunes" whose autonomy would be compromised if he were charged with harms that could not be avoided by taking due care.[199] *Rylands* also unethically allowed "unmeritorious or even culpable plaintiffs to use the machinery of the court" to collect money from "blameless defendants."[200]

C. *RYLANDS*'S PATH TO ACCEPTANCE IN AMERICA

British formalists and utilitarians upheld *Rylands* in the decades after the decision. The fear of reservoir accidents, coupled with industry's ability to distribute the cost of accidents through insurance, weakened *laissez-faire* arguments favoring a fault-based approach.[201] As John Murphy explains, *Rylands* was "neither immoral nor enterprise-inhibiting."[202]

By contrast, *Rylands*'s chance for acceptance in the United States appeared slight in the 1870s.[203] The protectionist view of the materialists predominated.[204] The economic moralists proclaimed that the "ethical standard of reasonable conduct" had prevailed over "the unmoral standard of acting at one's peril."[205]

But that trend reversed itself at the turn of the twentieth century.[206] At that time, a strong majority of U.S. courts adopted *Rylands*, including many states that had previously rejected it.[207] The materialist objections to *Rylands* receded in the face of America's industrial boom.[208] Hazardous enterprises, though socially valuable, could "pay their way,"[209] much as

199. Green, *supra* note 173, at 255. *See also* YEHOSHUA ARIELI, INDIVIDUALISM AND NATIONALISM IN AMERICAN IDEOLOGY 334 (1964) ("Competitive economic activity was . . . not only the way to progress but the principle of natural justice."); WITT, *supra* note 180, at 46–47.

200. Ames, *supra* note 198, at 103.

201. *See* JOHN G. FLEMING, THE LAW OF TORTS 368 (9th ed. 1998); Murphy, *supra* note 175, at 665.

202. Murphy, *supra* note 175, at 665 (internal footnote omitted). *See also* John H. Wigmore, *Responsibility for Tortious Acts: Its History—III.*, 7 HARV. L. REV. 441, 452–56 (1894) (discussing the progression of tort liability standards from negligence to the no-fault rule of *Rylands*).

203. *See* Shugerman, *supra* note 187, at 338–39 (noting that only three states—Massachusetts, Minnesota, and Pennsylvania—accepted *Rylands* by the end of the 1870s).

204. *See* FRIEDMAN, *supra* note 3, at 365 (stating that *Rylands* was "too much, too soon" for the American economy); KEETON ET AL., *supra* note 184, at 549.

205. Ames, *supra* note 198, at 99.

206. *See* 3 HARPER ET AL., *supra* note 119, at 195 (the "prevailing" twentieth–century view of the rule in *Rylands* was one of acceptance, rather than rejection); Shugerman, *supra* note 187, at 345.

207. Shugerman, *supra* note 187, at 345.

208. *Id. See* KEETON ET AL., *supra* note 184, at 549.

209. KEETON ET AL., *supra* note 184, at 549; Charles O. Gregory, *Trespass to Negligence to Absolute Liability*, 37 VA. L. REV. 359, 382–83 (1951). *See also* Robb v. Carnegie Bros. & Co., 22 A. 649, 651 (Pa. 1891) (holding "the production of iron or steel or glass" while of great public importance

British industry could in the 1860s.[210] A "strong and growing" sentiment queried: "in view of the exigencies of social justice who can best bear the loss?"[211] Utilitarian concerns also contributed to the pro–*Rylands* trend, prompting courts to apply *Rylands* in cases involving crowded urban conditions[212] and industrial hazards.[213]

Oliver Wendell Holmes, in *The Path of the Law*, remarked that the law of torts started with the "old days of isolated, ungeneralized wrongs" like assault, whereas the majority of the torts at the end of the nineteenth century were "incidents of certain well known businesses."[214] Just as the Industrial Age saw a shift from individualized wrongs to generalized perils, the Information Age brings another fundamental shift in the field of accidents, from mass physical injuries to today's cyber-harms. The next part explores why strict liability is as appropriate a response to the new risks posed by today's cyber-reservoirs as it was to the emerging risks of the early Industrial Age.

VI. THE CASE FOR *RYLANDS V. FLETCHER* AND THE CYBER-RESERVOIRS OF THE TWENTY-FIRST CENTURY

Two characteristic trends converged upon *Rylands*'s adoption in Britain and the United States—the maturation of industry and the salience of industry's new hazards. Before those trends came together, fault dominated within tort law.[215] Only after massive reservoir failures, such as the Johnstown Flood, and the strong growth of industry did American courts embrace *Rylands*.

is "the result[] of private enterprise" which "has no right to claim exemption from the natural consequences" of its acts).

210. Green, *supra* note 181, at 5.

211. Pound, *supra* note 168, at 233. *See also* Bridgeman-Russell Co. v. City of Duluth, 197 N.W. 971, 972 (Minn. 1924) (articulating a social justice rationale for the adoption of *Rylands*); Green, *supra* note 181, at 258 (discussing the implications for moral change upon the development of tort law).

212. *E.g.*, Davis v. Rich, 62 N.E. 375, 377 (Mass. 1902) (Holmes, C.J.) (discussing a leaking pipe that created an icy city sidewalk); Gorham v. Gross, 125 Mass. 232, 238–40 (1878) (stating that an employer was strictly liable for a collapsing wall that was negligently constructed by its employee); Wiltse v. City of Red Wing, 109 N.W. 114, 115 (Minn. 1906) (discussing a bursting city reservoir).

213. *E.g.*, Balt. Breweries' Co. v. Ranstead, 28 A. 273, 274 (Md. Ct. App. 1894); Bradford Glycerine Co. v. St. Marys Woolen Mfg. Co., 54 N.E. 528, 531 (Ohio 1899) (discussing exploding nitroglycerine); Green v. Sun Co., 32 Pa. Super. 521, 529–30 (1907) (discussing an oil refinery).

214. Holmes, *supra* note 3, at 467.

215. ABRAHAM, *supra* note 121, at 167 ("*Rylands* was decided against the background late nineteenth-century rule that there was liability only upon proof" of negligence.).

That same pattern emerges today. Some commentators offer negligence to address today's insecure databases.[216] But a strict-liability approach becomes increasingly compelling as the biometrics and information-technology sectors mature, the cyber-risk insurance market grows, data leaks escalate, and incidents of identity theft and corporate espionage compound.

This part argues that *Rylands* serves as a powerful metaphor to enrich our understanding of the new accidents in the Information Age. It offers parallels between the economic conditions at the time of *Rylands*'s adoption and this era, and explores how strict liability would meet the needs of many contemporary theorists as it did for Industrial Age intellectuals. Lastly, this part argues that the characteristic injuries of the Information Age deserve compensation due to our changing understanding of personhood in the twenty-first century.

A. A POWERFUL METAPHOR

Metaphors have long had a profound impact on the way scholars and judges conceptualize problems.[217] Although *Rylands* responded to the damage caused by bursting dams and other similar hazards, it also produced a metaphor for economically valuable, yet risky, technologies—a dynamic reservoir, amassing enormous power that provides great value if kept under control, but, if let loose as is inevitable, could wreak havoc on innocent people not involved in the enterprise.

216. *See supra* notes 109–19 and accompanying text.

217. *See, e.g.*, J.M. BALKIN, CULTURAL SOFTWARE: A THEORY OF IDEOLOGY 247 (1998) (discussing the use of metaphors and their effects); SOLOVE, *supra* note 7, at 27–28, 36–38, 55 (invoking the tyrannical bureaucracy of Franz Kafka's *The Trial* to describe commercial collection of personal data); Shyamkrishna Balganesh, *Common Law Property Metaphors on the Internet: The Real Problem with the Doctrine of Cybertrespass*, 12 MICH. TELECOMM. & TECH. L. REV. 265, 268 (2006) (arguing that the judicial doctrine of cybertrespass resulted from the law's reliance on metaphor); Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 718 (1995) (explaining that the nature of Internet law "depend[s] critically on the legal metaphors" used to describe the Internet and its functions); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 459 (2003) [hereinafter Hunter, *Cyberspace*] (arguing that metaphors are "central to legal thinking" and profoundly influence judicial decisionmaking). *See generally* Dan Hunter, *Reason Is Too Large: Analogy and Precedent in Law*, 50 EMORY L.J. 1197, 1197 (2001) (arguing that "cognitive science models of human thinking explain how analogical reasoning and precedential reasoning operate in law"). *But see* RICHARD A. POSNER, OVERCOMING LAW 523–24 (1995) ("A way of thinking, metaphor, yes, but often of an undisciplined and misleading character.").

The reservoir is a potent image for the collection of sensitive personal data in computer databases.[218] Water is a particularly appropriate analogy to electronic data as both "flow according to the laws of physics."[219] Personal information moves through "information pipelines," providing great value to organizations in this Internet economy.[220] Just as water in a reservoir is safe inside its confines, sensitive personal information is harmless if it remains inert. Now, as then, it is the uncontrolled release of the collected material—today's being personal identifying data—that wreaks havoc.

Much as failed reservoirs permit water to escape onto land, leaking databases release sensitive personal information into cyberspace and into the hands of dishonest employees or hackers. Indeed, land is commonly invoked as a metaphor for cyberspace.[221] Although the virtual world differs from the physical world in many ways, the image of cyberspace as apparently boundless land is compelling when envisioning Internet access to an organization's computer databases. [222] A business's internal computer

218. *See* O'HARROW, *supra* note 12, at 137–38 (recounting privacy expert Chris Hoofnagle's explanation that extraordinary "reservoirs" of cyber-data constitute infrastructure of our surveillance society).

219. *See* Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 538 (2003) (noting that Internet trespass cases, which involve electrical charges, "are all about chasing down electronic 'water' in order to reclaim it").

220. *See* SOLOVE, *supra* note 7, at 3, 19. *See also* Eric Lichtblau & James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES, June 23, 2006, at A1 (quoting an official describing the U.S. Government's search of a massive database containing financial records "turning on every spigot . . . and seeing what water would come out").

221. *E.g.*, WILLIAM J. MITCHELL, CITY OF BITS: SPACE, PLACE, AND THE INFOBAHN 23 (1995) (analogizing the physical world to the world of the Internet); Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73, 82–83 (2003) (arguing that websites look more like real property than ordinary chattel given the land-like descriptions of cyberspace and thus the rules of "real property" offer a "better fit" for the analysis of cyberspace issues); Hunter, *Cyberspace*, *supra* note 217, at 452, 516 (stating that many "treat cyberspace as if it were a physical place. . . . [It] may be inchoate and virtual, but no less real in our minds," rendering attempts to supplant the metaphor tragically "doomed to failure"); Harold Smith Reeves, Comment, *Property in Cyberspace*, 63 U. CHI. L. REV. 761, 762 (1996) ("Current judicial and legislative approaches to Cyberspace rely on a conception of bounded property developed to regulate the ownership of land.").

222. Mark Lemley offers a powerful critique of the "cyberspace as place" metaphor adopted by courts and scholars to justify applying real property laws to Internet law issues. *See generally* Lemley, *supra* note 219, at 521. *But see* Hunter, *Cyberspace*, *supra* note 217, at 452–53, 511–13 (challenging the perceived wisdom of those who conflate the idea that cyberspace has the characteristics of a place because it risks fencing off of the Internet, a tragedy of the "anticommons"). For Lemley, the metaphor should begin the inquiry, not end it. *See* Lemley, *supra* note 219, at 523. Lemley argues that courts ought to consider the context and effect of the proposed rules addressing cyberspace instead of reflexively applying real property rules to cyberspace law issues. *Id.* My analysis endeavors to avoid that blunder, offering the metaphor of water reservoirs to frame my discussion of the historical and theoretical reasons that support the application of *Rylands* to the problem of escaping valuable data.

network houses its proprietary data; the network welcomes visitors to its public areas from the "information superhighway," allowing only a very limited list of people into areas designated for certain employees.[223] Computer databases stand as the network's reservoirs, collecting the valuable personal information kept inside, as well as protecting it from escaping into cyberspace.

The *Rylands* metaphor of the water reservoir enriches our understanding of accidents at the dawn of this Information Age.[224] The following section will explore the historical arguments for the adoption of *Rylands* to current cyber-security breaches.

B. ECONOMIC CONDITIONS

The Information Age's economy shares many parallels with the British economy of the 1860s. At that time, England was a mature, industrialized nation.[225] Industry was booming.[226] Cotton-textile production quadrupled in the years between 1820 and 1850; real income in the late 1840s rose twenty percent above that of the 1830s; and railroads allowed factory owners to sell their goods to distant markets.[227] Industry increasingly was able to pass on accident costs through insurance.[228]

223. In this analysis, I borrow from Mark Lemley's notion that "private and public spaces must coexist on the Internet, just as they do in the physical world." Lemley, *supra* note 219, at 537. *See also* MITCHELL, *supra* note 221, at 23 ("Many of the places in cyberspace are public, like streets and squares; access to them is uncontrolled. Others are private, like mailboxes and houses, and you can enter only if you have the key or can demonstrate that you belong.").

224. In analogizing computer databases to reservoirs of valuable personal data, I do not mean to simply equate cyberspace with real property and databases with reservoirs. *See* Hunter, *Cyberspace*, *supra* note 217, at 487–88 (criticizing judicial decisions that treat a defendant's damage to a plaintiff's computer system as one involving real property, not personal property, due to the oversimplification of all tortious cyber-harm as involving real property law). I use the image of the water reservoir instead to illuminate how contemporary technologies are akin to those in *Rylands*'s time. To that end, I rely on the "interaction" theory of metaphor, which suggests that the combination of the "source" of the comparison and the target to which it is compared results in a "unique agent of meaning" that enriches our conceptualization of the dangers associated with the collection of personal identifying data at this juncture in our economic history. Janet Martin Soskice & Rom Harré, *Metaphor in Science*, *in* FROM A METAPHORICAL POINT OF VIEW: A MULTI-DISCIPLINARY APPROACH TO THE COGNITIVE CONTENT OF METAPHOR 289, 291 (Zdravko Radman ed., 1995).

225. *See* T.S. ASHTON, THE INDUSTRIAL REVOLUTION: 1760–1830, at 114–15 (1968); FRIEDMAN, *supra* note 151, at 53–54. *See also* Christine MacLeod, Britain as Workshop of the World (Feb. 11, 2004), http://www.bbc.co.uk/history/trail/victorian_britain/industry-invention/britain-workshop-world-01.shtml (explaining that by the Great Crystal Palace Exhibition of 1851, Britain was the world's industrial power, producing more than half of the world's iron, coal, and cotton).

226. FRIEDMAN, *supra* note 151, at 53–54.

227. *Id.* at 53–54, 228.

228. Murphy, *supra* note 175, at 665.

Reservoirs, large and small, enriched the British landscape when water from John Rylands's reservoir flooded Thomas Fletcher's coal mines.[229] Although dams appeared in England in the eleventh century,[230] the building of large reservoirs began in earnest in the late 1830s to provide water-power for textile mills.[231] By 1850, mill owners and towns increasingly used reservoirs to generate power and collect water for canals.[232]

At that time, however, no clear safety standard concerning the building and maintenance of reservoirs had been established.[233] As a result, Britain experienced two massive dam failures just before, and during, the *Rylands* decision.[234] Those reservoir failures created "anxiety" about the "menacing" character of large dams.[235]

The vitality and perils of the Information Age's technologies are similar to those of the Industrial Age. Information and biometric technologies, as well as their applications, have grown greatly in the past five years.[236] Information technology startups "no longer require lots of capital" because "they can build cheaply on Net infrastructure that didn't exist 10 years ago."[237] The biometrics market projects sales of $6 billion by 2010, up from $2.2 billion in 2006.[238] Insurance companies now provide cyber-risk insurance that covers third-party losses due to data leaks.[239]

229. *See* Simpson, *supra* note 132, at 217. *See also* SMITH, *supra* note 192, at 170–73 (discussing the construction of dams during the early nineteenth century). *See generally* G.M. BINNIE, EARLY VICTORIAN WATER ENGINEERS (1981).

230. SMITH, *supra* note 192, at 164 (explaining that the first recorded dam in Great Britain was built in 1189). In the eleventh century, however, England had 5624 water mills and it is likely that many were powered "by dams of some sort, small though they must have been." *Id.* at 165.

231. BINNIE, *supra* note 229, at 50.

232. *See* SMITH, *supra* note 192, at 169–80.

233. *See* BINNIE, *supra* note 229, at 50 (explaining that the widespread development of large reservoirs occurred in the late 1830s and 1840s to meet the water-power needs of mill owners); Simpson, *supra* note 132, at 217 (explaining that civil engineers in nineteenth-century England built reservoirs "on the basis of common sense, hunch, and experience, slowly augmented by a body of theoretical knowledge").

234. Simpson, *supra* note 132, at 219–31 (describing the failure of the Bilberry dam in 1852, which killed seventy-eight people and caused massive property damage, and the flooding of the Dale Dyke dam in 1864).

235. *Id.* at 219.

236. *See* Gary Flake, *A Virtual Roundtable: Seven Thought Leaders Sound Off on How Connectivity Is Changing the Planet*, FORTUNE, July 10, 2006, at 104, 106.

237. Justin Hibbard & Heather Green, *The Net: It Feels Like 1998 All over Again*, BUS. WK., May 22, 2006, at 30, 32 (describing $5.6 billion of venture capital investments in Internet startups in the first quarter of 2006).

238. Frommer, *supra* note 45.

239. Lawrence A. Gordon, Martin P. Loeb & Tashfeen Sohail, *A Framework for Using Insurance for Cyber-risk Management*, COMM. OF THE ACM, Mar. 2003, at 81, 81 (explaining that insurance allows firms to "hedge" potential losses from data-security breaches). The leading insurance companies

But in the ten years since the Internet has gained widespread use, a broadly accepted standard for securing today's cyber-reservoirs has not emerged.[240] In the first half of 2006, reports of massive data leaks appeared on a regular basis.[241] Today, public fear about identity theft is rampant and justified.[242]

The risks and rewards of some of today's cyber-reservoirs lack proportionality in much the same way they did for the Industrial Age's reservoirs. In the 1860s, a mill owner's neighbors like Thomas Fletcher shouldered much of the harm when a reservoir failed. Although such neighbors enjoyed the healthy economy fostered by textile mills, their gain paled in the face of the harm caused by a reservoir's flooding.[243]

Today, the burdens and benefits of an information broker's databases are not equitably distributed. Individuals struggle for years with the financial, emotional, and physical repercussions of data leaks inflicted upon them, having enjoyed little personal benefit from a data broker's collection of their data. Just as many suffered greater risk than reward from their neighbors' reservoirs, an individual's benefit from an information broker's collection of personal data is overshadowed by the harm suffered upon the information's release.

The parallels between the cyber-reservoir problem at the dawn of the Information Age and the reservoir problem of the Industrial Age extend beyond the economic conditions of the times. The following section

now carry policies covering third-party risks arising from computer-security breaches, such as losses due to identity theft and an identity-theft victim's mental anguish. *Darwin Enhances Tech//404sm: New Cyber Liability, Technology E&O, and Internet Liability Coverage*, PR NEWSWIRE, Apr. 26, 2006 (describing liability insurance policies that cover unauthorized access, theft, and loss of data due to security breaches); Gregory D.L. Morris, *Into the Breach*, RISK & INS., Apr. 15, 2006, at 82, 82, *available at* http://www.riskandinsurance.com/060415_feature_4.asp (explaining that AIG, Chubb, and others carry data-security insurance covering a vendor's failure to protect personal information).

240. *See generally* MICHAEL LEWIS, THE NEW NEW THING: A SILICON VALLEY STORY (2000) (describing the advent of the Internet); Gordon et al., *supra* note 239, at 81 (explaining that cyber-criminals successfully hacked into networks and databases of companies surveyed despite their near-universal use of security measures).

241. *E.g.*, Terry Frieden, John King, & Marsha Walton, *Source: Theft of Vets' Data Kept Secret for 19 Days*, CNN.COM, May 23, 2006, http://www.cnn.com/2006/US/05/23/vets.data/; *FTC Laptop Theft Puts 110 People at Risk*, REUTERS, June 23, 2006, *available at* http://news.zdnet.com/2100-1009_22-6087218.html; Kiviat, *supra* note 55, at 68. *See also* Privacy Rights, *Chronology*, *supra* note 9 (cataloguing hundreds of data breaches in 2005 and 2006).

242. *See, e.g.*, Kiviat, *supra* note 55, at 68.

243. *See* Keith N. Hylton, *The Theory of Tort Doctrine and the* Restatement (Third) of Torts, 54 VAND. L. REV. 1413, 1435 (2001) ("It would be easy to reach the conclusion that a reservoir externalizes far more non-reciprocated risk than benefit onto adjacent activities.").

explores similarities in the intellectual history of the Industrial Age and that of the Information Age.

C. STRICT LIABILITY AND CONTEMPORARY TORT THEORY

A strict-liability regime can be analyzed from a variety of different contemporary tort theories that share many of the values embraced by thinkers of the Industrial Age. Running through the debates surrounding *Rylands* in the Industrial Age were concerns about loss-spreading, accident prevention, and justice. Many of these intellectual themes recur today, providing profound theoretical support for a strict-liability solution for hazardous information reservoirs.

1. Instrumentalism

Contemporary instrumentalism envisions tort law as a means to pursue policy objectives, such as "accident prevention, wealth maximization, and the widespread distribution of the economic losses resulting from accidents."[244] Efficient deterrence and enterprise liability theories support a strict-liability solution for today's bursting cyber-reservoirs. Both theories embrace the nineteenth-century materialist's preoccupation with industry's ability to shoulder and distribute liability costs, on the one hand, and the utilitarian's concern for safety precautions, on the other. Although both efficient deterrence and enterprise liability theories uphold tort law as an efficient means to prevent accidents, enterprise liability envisions the spreading of accident costs as tort law's primary goal.[245]

a. Efficient Deterrence

The efficient deterrence theory of leading law-and-economics scholar and jurist Guido Calabresi supports a strict-liability approach to hazardous

244. Donald G. Gifford, *The Challenge to the Individual Causation Requirement in Mass Products Torts*, 62 WASH. & LEE L. REV. 873, 881–82 (2005) (footnotes omitted). *See also* John C.P. Goldberg, *The Constitutional Status of Tort Law: Due Process and the Right to a Law for the Redress of Wrongs*, 115 YALE L.J. 524, 583 (2005) (arguing that "[w]hether couched in terms of James-Traynor loss-spreading, Prosserian utilitarian balancing, or Calabresi-Posner efficient deterrence, tort law has, since the late 1930s, been widely understood by academics to be just another way in which government regulates conduct for the public good").

245. *Compare* CALABRESI, *supra* note 120, at 26–28 (discussing three subgoals of accident prevention, including a distributional goal), *and* Guido Calabresi & Jon T. Hirschoff, *Toward a Test for Strict Liability in Torts*, 81 YALE L.J. 1055, 1060, 1084–85 (1972) (noting that the cheapest cost-avoider efficiency test cannot be explained solely in terms of distributional goals although such goals may be served by it), *with* VIRGINIA E. NOLAN & EDMUND URSIN, UNDERSTANDING ENTERPRISE LIABILITY: RETHINKING TORT REFORM FOR THE TWENTY-FIRST CENTURY 175–77 (1995) (arguing that contemporary enterprise liability theory is premised on loss-spreading).

information reservoirs. As Calabresi explains, tort law should minimize the costs of accidents, including the costs of avoiding accidents.[246] Accident costs can be reduced by pursuing three goals. The first goal involves reducing the number and severity of accidents.[247] The second goal concerns the reduction of the societal costs of accidents that are not worth preventing because it costs more to prevent them than to let them occur.[248] The third goal is the reduction of the costs of administering an accident regime.[249] Because these three goals are "not fully consistent" with each other, an efficient liability regime would find the best combination of them, "taking into account what must be given up in order to achieve that reduction."[250]

Under Calabresi's theory, liability should attach to the "cheapest cost avoider"—the party best suited to make the "cost-benefit analysis between accident costs and accident avoidance costs" and to act on that analysis.[251] In unclear cases, courts and juries deciding the identity of the cheapest cost avoider should consider whether "some distributional goals are not best served by one decision rather than the other."[252] The cheapest cost-avoider inquiry focuses on parties who would "actually bear a loss."[253] Calabresi envisions *Rylands* as deciding that the reservoir owner defendant was better suited to compare the benefits and the costs of the risks he took than the neighboring coal mine operator plaintiff.[254]

Database operators constitute the cheapest cost avoiders vis-à-vis individuals whose information sits in a private entity's database. Database operators have distinct informational advantages about the vulnerabilities in their computer networks.[255] Individuals, by contrast, cannot detect and

246. CALABRESI, *supra* note 120, at 26.

247. *Id.* at 26–27.

248. *Id.* at 27–28, 44; Hanson & Logue, *supra* note 138, at 135 (arguing that law-and-economics scholars generally agree that an efficient products liability regime would encourage parties to "prevent all preventable accidents"—the deterrence goal—and would efficiently allocate the risk of unprevented accident costs—the insurance goal).

249. CALABRESI, *supra* note 120, at 28.

250. *Id.* at 29.

251. Calabresi & Hirschoff, *supra* note 245, at 1060 (emphasis omitted). *See also* CALABRESI, *supra* note 120, at 26–29; Steven Shavell, *Strict Liability Versus Negligence*, 9 J. LEGAL STUD. 1, 1–4 (1980) (arguing that strict liability is perfectly efficient where accidents are unilateral or not due to any fault of the victim). Negligence requires courts to examine all possibly relevant circumstances and to make a difficult, expensive, and often unreliable decision about reasonableness.

252. *See* Calabresi & Hirschoff, *supra* note 245, at 1083.

253. *Id.* at 1070. This focus on the actual loss-bearer does not mean that the liability rules differ between those who are insured and those who are uninsured. *Id.* at 1070 n.54. Instead, in devising a rule appropriate to a particular category of individuals, "the availability of insurance and other means of externalizing costs should be taken into account." *Id.*

254. *See id.* at 1066.

255. *See* Swire, *supra* note 10, at 286.

understand the security offered by information brokers, employers, colleges, or biometric vendors.[256] Even individuals knowledgeable about information security will find it difficult to assess how well a database system is designed and implemented.[257] And it is unclear what such individuals could do if informed about a database operator's vulnerabilities, particularly where they have no knowledge that an operator has amassed their data.[258] Thus, the database operator sits in the best position to make decisions about the costs and benefits of its information-gathering.

Individuals constitute actual loss bearers in a Calabresian calculus because they typically shoulder the losses due to identity theft, rather than passing them on through insurance. In 2005, identity-theft victims incurred significant financial expenses, most of which are not covered by basic homeowners' insurance.[259] Experts report that identity-theft insurance is not "worth the money"[260] because it does not cover direct monetary losses incurred as a result of such theft.[261] On the other hand, database operators can most efficiently spread the costs of data leaks by obtaining a single cyber-risk insurance policy as opposed to the countless identity-theft insurance policies obtained by individuals.[262]

Imagine an information broker storing the SSNs of millions of individuals. The broker has exclusive knowledge about, and control over, its information system.[263] Only the broker discovering a flaw in its information security system can assess the costs of fixing it. Individuals might be the cheapest cost-avoiders if they knew to, and could, remove their SSNs from a broker's database. But individuals have no information

256. *See id. See also* SCHNEIER, *supra* note 23, at 29 (explaining that information technology is so advanced that individuals cannot evaluate risks in giving a credit card number to a website). In other words, information asymmetry exists between database operators and individuals. Database operators either know or can ascertain flaws in their security systems—individuals can do neither.

257. Swire, *supra* note 10, at 286.

258. *See* SOLOVE, *supra* note 7, at 81, 84–85.

259. *See* Herb Weisbaum, *Why ID Theft Insurance Might Not Be Worth It*, MSNBC.COM, May 8, 2006, http://www.msnbc.msn.com/id/12692565/. Identity-theft coverage typically costs $20–$100 per year as a rider to a basic homeowner's policy or as a stand-alone purchase with deductibles ranging from $100 to $1000. *Id.* Many policies do not cover legal fees or lost wages due to time away from work. *Id.*

260. *Stop Thieves from Stealing You*, CONSUMERREPORTS.ORG., Oct. 2003, http://www.consumerreports.org/cro/consumer-protection/identity-theft-1003/overview/index.htm.

261. *Id.* (explaining that identity-theft policies seldom cover a victim's out-of-pocket losses, which typically amount to $800); Weisbaum, *supra* note 259 (noting that many identity-theft policies do not cover legal fees or lost wages due to time away from work).

262. *See supra* notes 139–42 (discussing the efficiency of cost-spreading by database operators versus individuals).

263. Swire, *supra* note 10, at 286–87.

about, and have no practical means to find out, where their personal data resides. Even if individuals could determine the location of their personal data, they could not determine the degree of security afforded their information. Individuals also usually cannot ask an information broker to remove their data to avoid a leakage problem.[264] As such, the database operator is best situated to make the optimal choice of either taking additional security precautions or insuring against security-breach losses. To that end, the law-and-economics theory of Calabresi provides strong support for a strict-liability solution for leaking cyber-reservoirs.[265]

Some may argue that market negotiations would provide the optimal solution to the leaking database problem. Ronald Coase explains that in a case where there are no transaction costs, it makes no difference with respect to the efficient use of resources whether the law initially imposes liability on the injurer or lets the loss lie with the victim.[266] Whichever side receives the initial grant of legal rights can negotiate with the other party to receive a payment in exchange for those rights. Under the Coase theorem, parties will bargain to an efficient result if transaction costs are low.[267]

An optimal market solution to today's hazardous reservoirs is not feasible. Coordinating the wishes of thousands, or millions, of individuals whose personal data is collected by an organization would be costly and challenging. For example, it would be exorbitantly expensive to bring together the two million customers of Pay By Touch to bargain with the biometric provider over the way it stores their fingerprint data. Large consumer blocks also encounter difficulty "express[ing] collectively their relative preferences . . . ."[268] Coase's theorem teaches that when transaction costs are high, then imposing liability on the party best able reduce costs

264. *See supra* notes 29–31 and accompanying text (discussing data brokers). Employees and students might be the cheapest cost-avoiders if they could refuse to provide their SSNs to colleges and employers. But both employees and students lack information to warrant such refusals because they cannot determine the degree of security afforded their information, much less how well their information is protected in future years. *See, e.g.*, Privacy Rights, *Chronology*, *supra* note 9 (explaining that a data-security breach at Ohio University released SSNs of alumni as well as current students). Moreover, employees and students may not be in a position to bargain with employers and colleges about the disclosure of their SSNs. *See* SOLOVE, *supra* note 7, at 82–83.

265. Posner's theory also supports a strict-liability approach to address the hazardous information reservoirs. *See supra* notes 132–38 and accompanying text (applying Posner's economic analysis to today's leaking cyber-reservoirs).

266. R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 2–8 (1960).

267. *Id.*

268. Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 50 (1997).

results in the most efficient allocation of resources.[269] Consequently, under this law-and-economics approach, strict liability would be the optimal substitute for difficult market negotiations concerning cyber-reservoirs.

b. Enterprise Liability

Enterprise liability theory suggests strict liability to address today's hazardous information reservoirs. This theory imposes the costs of a commercial entity's profitable activities on that entity rather than on the individuals "who happen to be [the] victims."[270] *Rylands v. Fletcher* stands as a model illustration of this approach.[271] Enterprise liability "asserts that actors should bear the costs of those accidents that are 'characteristic' of their activities and then distribute those costs among all those who benefit from the imposition of the risks at issue."[272]

Loss distribution and accident prevention constitute the animating principles of enterprise liability theory.[273] Strict liability effectively distributes the costs of accidents given an enterprise's superior ability to spread accident costs through insurance.[274] The cost-pressures of higher insurance premiums also create incentives for enterprises to take safety precautions for their risky activities.[275] Although enthusiasm for enterprise liability has waned in the past twenty years, it remains "alive and well" in

269. Harold Demsetz, *When Does the Rule of Liability Matter?*, 1 J. LEGAL STUD. 13, 27–28 (1972) (explaining that where transacting costs of negotiation are high under Coase's theorem, the legal system can "improve the allocation of resources by placing liability on that party who in the usual situation could be expected to avoid the costly interaction most cheaply").

270. *See, e.g.*, Gregory C. Keating, *Pressing Precaution Beyond the Point of Cost-justification*, 56 VAND. L. REV. 653, 667 (2003).

271. *See* Fleming James, Jr., *Accident Liability: Some Wartime Developments*, 55 YALE L.J. 365, 366 (1946); Clarence Morris, *Hazardous Enterprises and Risk Bearing Capacity*, 61 YALE L.J. 1172, 1176 (1952); George L. Priest, *The Invention of Enterprise Liability: A Critical History of the Intellectual Foundations of Modern Tort Law*, 14 J. LEGAL STUD. 461, 476 (1985) (explaining that the father of enterprise liability theory, Fleming James, Jr., argued that the modern direction of law was away from a medieval fault-based approach and toward strict liability, with *Rylands v. Fletcher* and workers' compensation plans as its "most prominent models").

272. Gregory C. Keating, *The Theory of Enterprise Liability and Common Law Strict Liability*, 54 VAND. L. REV. 1285, 1334 (2001).

273. *See* 3 HARPER ET AL., *supra* note 119, at 132; Priest, *supra* note 271, at 463.

274. *E.g.*, Robert L. Rabin, *Some Thoughts on the Ideology of Enterprise Liability*, 55 MD. L. REV. 1190, 1193–94 n.22 (1996). *See* Keating, *supra* note 272, at 1324 (describing Judge Friendly's view that enterprises should be held liable for their characteristic risks because they benefit from the imposition of those risks even if liability would not induce precaution). Many enterprise liability theories also contend that the cost-pressures of higher insurance premiums create incentives for enterprises to take safety precautions for their risky activities. *See, e.g.*, *id.* at 1320.

275. Keating, *supra* note 272, at 1320. Justice Traynor's celebrated concurrence in *Escola v. Coca Cola Bottling Co.*, 150 P.2d 436, 440 (Cal. 1944), "afforded prominence both to safety incentives and loss-spreading rationales." Rabin, *supra* note 274, 1194 n.22.

the "rulings and rhetoric of courts across the country and in contemporary legal scholarship."[276]

Under an enterprise liability approach, strict liability would effectively address the characteristic risks of the private sector's cyber-reservoirs. In much the same way that pollution attends the activities of a chemical factory, cyber-security breaches routinely confront database operators. Organizations can spread the losses of data-security breaches with cyber-risk insurance.[277] Under enterprise liability theory, strict liability would stand as an effective means to distribute the costs of leaking cyber-reservoirs and to spur accident–preventing measures.

2. Justice Approach

Justice theories connect tort law to the "doing of justice between the parties to the litigation."[278] Some share the nineteenth-century economic moralist's commitment to *laissez-faire* but within a framework informed by a libertarian conception of justice.[279] Other justice theories reject a *laissez-faire* philosophy and the economic moralist's intuition that injurers stood on equal footing as the injured.[280] For instance, fairness theory finds that risks are not fairly allocated between enterprises and individuals. Justice requires that those who benefit from an activity bear its costs and risks.[281] A fairness approach would defend strict liability as a just price for a database operator's freedom to collect ultrasensitive personal information.[282] Corrective justice and civil recourse theories, on the other

276. Keating, *supra* note 272, at 1333. *See also* 3 HARPER ET AL., *supra* note 119, at 196 n.19 (explaining that "loss distribution, based in effect on enterprise liability," as preferable to negligence "has been widely recognized for years" and is not limited "to activities to which strict liability has heretofore applied"); NOLAN & URSIN, *supra* note 245, at 150–51 (suggesting enterprise liability's continuing prominence); Murphy, *supra* note 175, at 666 (highlighting the vitality of *Rylands* in the twenty-first century to ensure that polluting enterprises pay their way). For examples of contemporary scholarship advocating the retention of enterprise liability, see Steven P. Croley & Jon D. Hanson, *Rescuing the Revolution: The Revived Case for Enterprise Liability*, 91 MICH. L. REV. 683, 692 (1993) (offering "new arguments on behalf of old justifications for the expansion of manufacturer liability"); William K. Jones, *Strict Liability for Hazardous Enterprise*, 92 COLUM. L. REV. 1705 (1992) (discussing same).

277. *See supra* note 239 (discussing the increasing availability and use of cyber-risk insurance).

278. John C.P. Goldberg, *Twentieth-century Tort Theory*, 91 GEO. L.J. 513, 564 (2003).

279. *See, e.g.*, Richard A. Epstein, *A Theory of Strict Liability*, 2 J. LEGAL STUD. 151, 203–04 (1973).

280. *See supra* notes 197–200 and accompanying text (describing the philosophy of the nineteenth century's economic moralists).

281. *See, e.g.*, Gregory C. Keating, *Rawlsian Fairness and Regime Choice in the Law of Accidents*, 72 FORDHAM L. REV. 1857, 1886–87 (2004).

282. *See id.* at 1887–90.

hand, would reject strict liability unless the database operator's wrongful behavior could be presumed in the wake of a data leak.[283] This subsection addresses each of these theories in turn.

a. Libertarians

Libertarian tort theory would uphold strict liability for data leaks as a means to provide just compensation for an individual's property losses caused by the release of sensitive personal data. Libertarian theory endeavors to offer a "complete theory of *laissez-faire*" that acknowledges the need for rules governing both "common property and forced exchanges."[284]

Under this theory, a person exercises absolute dominion over his person, reputation, and things acquired through his actions.[285] If someone acts in a manner that injures another's physical self, possessions, or reputation, the injurer owns the loss.[286] Because defendants would pay for damage inflicted on their own property, justice requires defendants to bear the costs if they damage another's property.[287] Thus, an injurer who infringes, or impairs the value of, a victim's property must compensate the property owner for the loss as if the loss were the injurer's own loss.

The hazards of the release of a person's SSN or biometric data constitute the loss of property under libertarian tort theory. People "own" their good credit rating, the personal freedom from an erroneous arrest intended for an identity thief, and the right to be free of financial expenses to repair their credit.[288] Because a database operator would incur losses upon the leakage of its own data, it must compensate individuals harmed by the release of their personal information. From the libertarian perspective, strict liability might ensure that an individual's property rights are not unjustly impaired by database operators.

283. *See* Zipursky, *supra* note 143, at 699–700.

284. *See* RICHARD A. EPSTEIN, PRINCIPLES FOR A FREE SOCIETY: RECONCILING INDIVIDUAL LIBERTY WITH THE COMMON GOOD 3, 320 (1998) (calling for a reinvigoration of *laissez-faire* philosophy); Goldberg, *supra* note 278, at 564–65.

285. Goldberg, *supra* note 278, at 564–65. *See generally* ROBERT NOZICK, ANARCHY, STATE, AND UTOPIA 79–84 (1974) (articulating a libertarian theory of a minimal state that upholds one's freedom to engage in risky activities whose benefits outweigh their costs, such as polluting or driving, so long as the individuals who benefit from the activities compensate those who bear the costs).

286. Goldberg, *supra* note 278, at 565.

287. Richard A. Epstein, *Causation—In Context: An Afterword*, 63 CHI.–KENT L. REV. 653, 658 (1987) [hereinafter Epstein, *Afterword*]; Epstein, *supra* note 279, at 158.

288. *Cf.* Epstein, *Afterword*, *supra* note 287, at 818–19 (explaining that because auction aggregators that troll an auction web site, such as eBay, gather information from the site and strain it, they interfere with the auction house's property right to exclude such aggregators; thus, the rules for trespass to real property should be imported into cyberspace).

b. Fairness Theory

Fairness theory also supports a strict-liability solution to the Information Era's leaking cyber-reservoirs. The fairness theory, originated by George Fletcher[289] and developed by Gregory Keating,[290] provides the "moral logic" for treating strict enterprise liability as the modern default rule for tort law.[291] In its prescription of fairness, this theory builds on the political philosophy of John Rawls.[292]

Fairness requires an enterprise to compensate individuals injured by its risky, yet profitable, activities if the victim does not benefit from the activities to the same extent that the enterprise does.[293] Tort law's central task is to reconcile the need for freedom to impose risks on others with the need for security from accidental injury.[294] The tension between liberty and security, Rawls's primary goods, must be reconciled in a manner that a "plurality of persons with distinct lives and diverse ends and preferences" would accept.[295]

289. In 1972, George Fletcher propounded the "reciprocity of risk" theory. George P. Fletcher, *Fairness and Utility in Tort Theory*, 85 HARV. L. REV. 537, 540–42 (1972) [hereinafter Fletcher, *Fairness*]. *See also* George P. Fletcher, *Book Review: Corrective Justice for Moderns*, 106 HARV. L. REV. 1658, 1677 (1993) (affirming reciprocity of risk theory in reviewing JULES L. COLEMAN, RISKS AND WRONGS (1992)). For Fletcher, fairness requires compensation for a victim's injuries if the injurer exposed the victim to an unfair amount of risk—that is, more risk than the victim exposed to the injurer. *See* Fletcher, *Fairness*, *supra*, at 546–48. *Rylands* epitomized the reciprocity theory for Fletcher because John Rylands imposed a risk on his coal-mining neighbor, Thomas Fletcher, who did not impose such risks on him. *See id.* at 546, 550. Thus, fairness required John Rylands to compensate Thomas Fletcher. *See id.*

Fletcher's "reciprocity of risk" paradigm would likely uphold a strict-liability approach to today's insecure cyber-reservoirs. Database operators, in amassing massive collections of sensitive personal data in databases, impose risks upon individuals but such individuals do not impose risks on database operators. Thus, the database operator's imposition of nonreciprocal risks upon individuals would warrant strict-liability treatment for the harm caused by leaking data under the "reciprocity of risk" theory.

290. *See* Gregory C. Keating, *Reasonableness and Rationality in Negligence Theory*, 48 STAN. L. REV. 311, 313–14 (1996) [hereinafter Keating, *Reasonableness*] (building on the "incomplete" reciprocity theory of George Fletcher and Charles Fried). Keating partially rejects Fletcher's "reciprocity of risk" paradigm and offers a different prescription for fairness. *See* Keating, *supra* note 281, at 1887; Gregory C. Keating, *Distributive and Corrective Justice in the Tort Law of Accidents*, 74 S. CAL. L. REV. 193, 200–01 (2000) [hereinafter Keating, *Corrective Justice*]; Goldberg, *supra* note 278, at 568–69 (describing Keating's interpretive project as updating Fletcher's reciprocity theory and providing a normative basis for the reciprocity principle based on a "Rawlsian conception of fair terms of cooperation among equals").

291. *See* Keating, *Corrective Justice*, *supra* note 290, at 202.

292. *See* Keating, *supra* note 281, at 1857–58.

293. *See id.* at 1873.

294. *Id.* at 1862–63.

295. *Id.* at 1864–66.

When an organization engages in reasonable risky behavior—that is, nonwrongful conduct where an injurer's freedom to impose the risk is more valuable than a victim's forgone security such as reservoirs and blasting—fairness requires that the injurer pay for the victim's harm.[296] It is reasonable for an enterprise to impose nonnegligent risks, but unreasonable for it to refuse to pay for the financial costs of its actions.[297] Strict liability exacts a "just price" for an enterprise's freedom to engage in profitable activities where the victim did not similarly enjoy such a liberty but nonetheless suffered injury.[298] This is true even where victims participate in an enterprise and share in its benefits, but not in the same proportion "to the detriment they suffer" when harmed by the enterprise.[299] The theory of fairness thus prescribes proportionality between the benefits and burdens borne by parties.[300]

The hazards of the Information Age's bursting cyber-reservoirs demand recompense under the fairness theory. In amassing personal data, private entities enjoy appreciable profit-making "freedoms," such as enhanced workplace efficiency, gains from the sale of personal information, and a means to solicit potential customers. On balance, the degree of benefit to individuals whose information is collected is not matched by the detriment they suffer upon the release of their information. For example, individuals gain little in having their SSNs collected by an information broker but suffer much when their information escapes into the hands of an identity thief who commits crimes in their names and mars

296. *See id.* at 1871.

297. Gregory C. Keating, *The Idea of Fairness in the Law of Enterprise Liability*, 95 MICH. L. REV. 1266, 1328 (1997). *See also* Robert E. Keeton, *Conditional Fault in the Law of Torts*, 72 HARV. L. REV. 401, 441 (1959) (articulating moral and fairness grounds for strict liability for hazardous activities under the rubric of "unjust enrichment" because "those who benefit by receiving the products of blasting activities ought to bear the losses if they can be distributed at a reasonable cost").

298. Keating, *supra* note 281, at 1891–92. *See also* MARSHALL S. SHAPO, THE DUTY TO ACT: TORT LAW, POWER, & PUBLIC POLICY 8, 11–12 (1977) (arguing that morality and economic considerations compel the notion that entrepreneurs whose activities cause harm have a duty to repair that harm in return for freedom to act as they wish).

299. Keating, *supra* note 281, at 1891. *See also* Jones, *supra* note 276, at 1778 (contending that fairness demands that when the enterprise "controls the instrumentality of harm" and the victim is "essentially passive" and cannot avoid the harm herself, strict liability should follow); Virginia E. Nolan & Edmund Ursin, *The Revitalization of Hazardous Activity Strict Liability*, 65 N.C. L. REV. 257, 290 (1987) (arguing that strict liability for entities whose commercial activities impose hazards on individuals is fair because the victim imposed "no similar risk" on the enterprise and lacked the ability to protect herself).

300. *See* Keating, *supra* note 281, at 1858. *See also* JOHN RAWLS, POLITICAL LIBERALISM 300 (1993) ("Fair terms of cooperation articulate an idea of reciprocity and mutuality: all who cooperate must benefit, or share in common burdens, in some appropriate fashion judged by a suitable benchmark of comparison.").

their credit. To place liability on the database operator would fairly distribute the costs of the release of such ultrasensitive personal data and equalize the burdens and benefits of profitable cyber-reservoirs of data.

Fairness theory, however, draws a hard line as to the harm it redresses, namely physical injury and personal property damage.[301] To a certain extent, bursting cyber-reservoirs infringe Rawls's basic liberties and thus warrant compensation if the release of sensitive cyber-data resulted in an individual's physical injury at the hands of a stalker or in the loss of an individual's personal property.[302] An individual's arrest for an identity thief's crime would also deprive an individual of personal freedom.[303] And the loss of a home due to a defaulted secondary mortgage loan of an identity thief would constitute personal property damage. To that extent, the fairness theory supports strict liability for the bursting cyber-reservoirs of the Information Age.

c. Corrective Justice and Civil Recourse

Corrective justice and civil recourse theories sit uncomfortably with strict liability. Corrective justice theory embraces an Aristotelian concept of justice that requires injurers to make victims whole.[304] Defendants, however, only bear moral responsibility for their faulty actions.[305] Strict liability is consistent with corrective justice's notion of moral agency if an actor's fault can be presumed.[306] To that end, injuries caused by abnormally dangerous activities, such as operating reservoirs, warrant compensation because fault can be imputed from the "very materialization

301. *See* Keating, *Reasonableness*, *supra* note 290, at 343–44.

302. *See supra* note 64 and accompanying text (discussing Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1006 (N.H. 2003)).

303. *See* JOHN RAWLS, A THEORY OF JUSTICE 61 (1971); Keating, *Reasonableness*, *supra* note 290, at 344. It also might impinge on the individual's right to be free from arbitrary arrest under Rawls's basic liberties. RAWLS, *supra*, at 61.

304. *See* COLEMAN, *supra* note 289, at 320 (corrective justice "imposes the duty to repair the wrongs one does" (emphasis omitted)); ERNEST J. WEINRIB, THE IDEA OF PRIVATE LAW 56–57 (1995); Stephen R. Perry, *The Moral Foundations of Tort Law*, 77 IOWA L. REV. 449, 453 (1992) (corrective justice erases the wrongful actor's gain and restores the victim's loss).

305. *See* WEINRIB, *supra* note 304, at 64, 76 (developing Aristotle's notion that corrective justice addresses the disturbances of the equality between two parties such that the "injustice that corrective justice corrects is essentially bipolar"); Perry, *supra* note 304, at 453–54. *See also* Benjamin C. Zipursky, *Philosophy of Tort Law*, *in* THE BLACKWELL GUIDE TO THE PHILOSOPHY OF LAW AND LEGAL THEORY 122 (Martin P. Golding & William A. Edmundson eds., 2005) (describing varying notions of corrective justice theory).

306. *See* WEINRIB, *supra* note 304, at 187–90.

of the risk."[307] In that case, strict liability simply relieves victims from identifying the injurer's faulty acts.[308]

Civil recourse theory similarly requires a fault finding to warrant redress against a database operator.[309] Under civil recourse theory, tort suits empower victims to bring private actions against those who commit legal wrongs against them.[310] Genuine strict liability can be reconciled with recourse theory if the principle for adopting no-fault liability stems from the notion that wrongdoing is presumed, such as in manufacturing defect strict liability where victims face systematic difficulties in proving what went wrong in the manufacturing process.[311]

The hazardous information reservoirs might merit strict-liability treatment under both civil recourse and corrective justice theory if fault could be presumed from the circumstances surrounding the release of the personal information. For example, a case involving a database operator's posting of SSNs on a website for all the public to see may warrant a presumption of faulty behavior by the database operator. Moreover, just as plaintiffs have difficulty identifying a defect in a defendant's manufacturing process, victims of data leaks may face great obstacles in proving the flaw in a data operator's information system given the rapidly accelerating risk environment. This might support a presumption of fault and the concomitant approval of strict liability.

3. Formalism

Contemporary tort scholars rightfully acknowledge the current predominance of negligence over strict liability.[312] A *Rylands* solution for

307. *Id.* at 188. *See also* COLEMAN, *supra* note 289, at 367–68 (arguing that no matter how well one maintains an above-ground reservoir, "simply building a reservoir creates unnecessary, and therefore unreasonable risks").

308. WEINRIB, *supra* note 304, at 189.

309. *See* Goldberg, *supra* note 244, at 601 (conceiving tort law "as a law for the redress of wrongs [that] conditions the imposition of liability on conduct that is wrongful toward, and injurious to, the victim"); John C.P. Goldberg & Benjamin C. Zipursky, *The Moral of* MacPherson, 146 U. PA. L. REV. 1733, 1812–32 (1998); Benjamin C. Zipursky, *Rights, Wrongs, and Recourse in the Law of Torts*, 51 VAND. L. REV. 1, 3, 15–40, 55–70 (1998) (explaining that tort law only contemplates redress where an injurer bears a relational duty to a victim and commits a wrong against the victim).

310. Zipursky, *supra* note 143, at 754 (explaining that although civil recourse theory differs from corrective justice theory in critical ways, civil recourse theory, like corrective justice theory, takes "the offensive—as a superior analysis of the structure of tort doctrine, as a form of justice and political order different from distributive justice, . . . and as a critique of instrumentalism").

311. Goldberg, *supra* note 244, at 598.

312. *E.g.*, RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL HARM (BASIC PRINCIPLES) § 6 cmts. a, c (Tentative Draft No. 1, 2001) (suggesting that the overarching normative principle of tort law is negligence); James A. Henderson, Jr., *Why Negligence Dominates Tort*, 50 UCLA L. REV. 377,

leaking cyber-reservoirs, however, would not undermine this trend, but would instead carve out a strict-liability exception for the release of sensitive personal data from insecure databases.[313] Such an approach would be consistent with the significant pockets of enterprise liability that remain in a variety of tort actions.[314]

Some would object to this proposal on the grounds that accident law typically confines recovery for injuries resulting in physical harm or personal property loss.[315] The economic loss doctrine would preclude the recovery of pecuniary harm not resulting from bodily or property damage.[316] The following section argues that just as the industrial technologies of the nineteenth century altered the nature of injuries, the twenty-first century's technologies inflict new harms that demand recognition, including economic losses to our market identity and emotional harm suffered as a result of identity theft.

378–79 (2002); Robert L. Rabin, *The Renaissance of Accident Law Plans Revisited*, 64 MD. L. REV. 699, 716 (2005); Gary T. Schwartz, *Mixed Theories of Tort Law: Affirming Both Deterrence and Corrective Justice*, 75 TEX. L. REV. 1801 (1997). *See also* G. EDWARD WHITE, TORT LAW IN AMERICA: AN INTELLECTUAL HISTORY 276–77 (rev. ed. 2003) (addressing the emergence of negligence over strict liability as the dominant standard in manufacturing liability cases).

313. Some may argue that in establishing a *Rylands* claim for bursting cyber-reservoirs, plaintiffs would face significant practical problems proving causation. Although this Article does not attempt to resolve this question, a few preliminary notes can be made. Many contemporary theories that might uphold strict liability also would dispense with the individual causation requirement. *See* Guido Calabresi, *Concerning Cause and the Law of Torts: An Essay for Harry Kalven, Jr.*, 43 U. CHI. L. REV. 69, 105 (1975) (suggesting that any requirement for proof of causation should be obviated when public policy demands); Gifford, *supra* note 244, at 881–87 (exploring several tort scholars' rejection of the notion that a particular victim needs to identify a particular injurer to recover). Concerns about causation also may be somewhat alleviated by the adoption of data-breach notification statutes. Such notices would help victims identify the cyber-reservoir that leaked their sensitive personal data. Menn, *supra* note 19 (noting that 800 individuals were victimized by identity thieves as a result of a data-security breach at ChoicePoint in 2005). Plaintiffs also might invoke cases where manufacturers of mass products were held liable without proof of individual causation under "industry-wide" or market-share liability theories. *See* Donald G. Gifford, *The Peculiar Challenges Posed by Latent Diseases Resulting from Mass Products*, 64 MD. L. REV. 613, 654–55 (2005).

314. *See* WHITE, *supra* note 312, at 253 (noting that enterprise liability endures in many areas of tort law, including liability for abnormally dangerous activities).

315. Keating, *Reasonableness*, *supra* note 290, at 433.

316. RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR ECONOMIC LOSS § 8 (Preliminary Draft No. 1, 2005) ("[A]n actor who accidentally causes pecuniary harm to another that does not result from a wrongful injury to the person or property of the other is subject to liability in tort for neglect of a duty of care to the other only as stated in §§ 9–21."); 4 FOWLER V. HARPER, FLEMING JAMES, JR. & OSCAR S. GRAY, THE LAW OF TORTS §§ 25.18A-25.18D (2d ed. 1986).

D. TWENTY-FIRST CENTURY HARM

Our conception of injury must undergo change in the twenty-first century. "Tort law is both premised on and sends messages about the worth of individuals."[317] In the twentieth century, accidents mangled bodies, flooded property, and emitted pollution.[318] An individual's self-worth stemmed, in many respects, from the individual's ability to work. Tort law, in turn, provided protection and compensation for injuries to those whose livelihoods depended on their physical bodies and property.

At the dawn of this Information Age, individuals define themselves by their interactions and integrity in the marketplace.[319] Impaired credit due to the release of ultrasensitive information to an identity thief compromises an individual's personal independence and self-respect in much the same way that a deprivation of personal property does.[320] A people's liberty to hold their good names, credit, and work free of impersonation is crucial to the development of their personalities.[321]

Moreover, an individual's personal independence is deeply compromised when the individual wrestles with the loss of control that identity theft, and the fear of it, engenders.[322] Emotional distress arising from identity theft impairs an individual's ability to pursue their conceptions of the good life.[323] Just as Holmes recognized the shift from

317. Nancy Levit, *Ethereal Torts*, 61 GEO. WASH. L. REV. 136, 174 (1992).

318. *See* WITT, *supra* note 180, at 141–42.

319. *See* Richard S. Markovitz, *Liberalism and Tort Law: On the Content of the Corrective-Justice-Securing Tort Law of a Liberal, Rights-based Society*, 2006 U. ILL. L. REV. 243, 245, 268–69 (explaining that the recognition of libel, slander, defamation, and privacy actions suggests that tort law recognizes harm caused by an injurer's interference with an individual's right to lead a life of moral integrity).

320. *See* RUDOLPH VON JHERING, THE STRUGGLE FOR LAW 59 (John J. Lalor trans., 2d ed. 1915) ("Property is but the periphery of my person extended to things."). *See generally* Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957 (1982) (conceiving personal property as an extension of the self).

321. *Cf.* Radin, *supra* note 320, at 1014–15 (arguing for the recognition of an expanded notion of personal property interest based on personhood theory); John Stick, *Turning Rawls into Nozick and Back Again*, 81 NW. U. L. REV. 363, 374 (1987) (suggesting that Nozick could argue that Rawls's basic liberties include a wider conception of property rights than Rawls acknowledges because the "rights to use and dispose of property yield much more self-respect than limited rights").

322. *See* Heidi Li Feldman, *Harm and Money: Against the Insurance Theory of Tort Compensation*, 75 TEX. L. REV. 1567, 1587 (1997) (arguing that emotional suffering stunts a person's capacity to flourish).

323. *See* Levit, *supra* note 317, at 189–90. I recognize the possibility that ultrasensitive plaintiffs may attempt to recover emotional distress damages for the leakage of their data. *See* Keating, *Reasonableness*, *supra* note 290, at 344 n.114, 347 (contending that although purely emotional harm is central to an individual's personality, its exclusion from tort law's protection is justified because such damages would put society at the mercy of the emotionally hyperactive). The possibility of

the interpersonal wrongs of the eighteenth century to the mass industrial risks of the nineteenth century, the law should adapt to account for injuries to our changed conception of personhood in the twenty-first century.

Although this Article proposes a *Rylands* solution for leaking cyber-reservoirs, other hazards of the Information Age may have Industrial Age analogues. Rather than meeting the challenges of the Information Age with new or inadequate standards, we can learn much about how to address the risks of the new technologies of the Information Age from the lessons of the Industrial Age. The current crisis of escaping sensitive personal data illustrates the compelling need for a strict-liability standard for information security much as it was needed to address the bursting reservoirs of the Industrial Age.

VII. CONCLUSION

The new information technologies challenge our conception of accidents and injuries. Their diverse new risks include the uncontrolled release of sensitive personal information from insecure computer databases into the hands of hackers, dishonest employees, and other criminals. The escape of such personal data brings the threat of identity theft, criminal impersonation, stalking, and corporate espionage. These risks require a solution.

Congress is considering proposals, both modest and wide sweeping, to address the hazards of gathering massive troves of digital personal data. Public choice analysis, however, suggests that meaningful federal legislation is unlikely in the face of strong interest-group opposition to restrictions on the collection of personal data. The insights of public choice theorists may be particularly apt here as members of Congress rely on these very databases in their reelection campaigns.

An appropriate private law response cannot be found in negligence. The contours of a negligence regime are simply too uncertain, and inherent problems with its enforcement undermines optimal deterrence. Instead, a solution can be found in the lessons of the past. The strict-liability approach of the Industrial Age's *Rylands v. Fletcher* provides a potent metaphor to conceptualize the characteristic risks of new technologies at the dawn of a new economic era. America embraced *Rylands* once it became clear that a strict-liability response was critical to addressing the escalating hazards of

ultrasensitive plaintiffs, however, ought not to preclude recovery for emotional harm given the importance of emotional health to human flourishing and a jury's ability to identify a plaintiff's ultrasensitive nature and, in turn, award damages fairly.

bursting reservoirs and that industry could afford such a standard. Now, as then, the maturity of the new technology-driven economic sector, along with many contemporary tort theories, support strict liability for today's insecure cyber-reservoirs of personal data.

This solution finds its place in the trajectory of tort law over the past 150 years. Although tort law has veered between fault and strict liability, the inadequacy of negligence in this circumstance demands a strict-liability solution. The embrace of this solution requires updating our conception of harm to the conditions of the twenty-first century. The prominence of market identity to our conception of personhood in the Information Age demands an effective remedy when that identity is ruined. A return to *Rylands* can facilitate that remedy.

While this Article suggests a private law solution for the twenty-first century's hazardous information reservoirs, it may also have other, more general implications. Unlike in the Industrial Age where the views of instrumentalists clashed with justice-minded theorists, here instrumental and justice theories come together in support of a strict-liability regime. Other twenty-first century accidents may find similar convergence of those theories that deserve exploration.