24:3 BERKELEY TECHNOLOGY LAW JOURNAL

Symposium: Security Breach Notification Six Years Later

2009

Pages
1009
to
1255

Berkeley Technology Law Journal
Volume 24, Number 3

Production: Produced by members of the *Berkeley Technology Law Journal*. All editing and layout done using Microsoft Word.

Printer: Joe Christensen, Inc., Lincoln, Nebraska.
Printed in the U.S.A.
The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences—Permanence of Paper for Library Materials, ANSI Z39.48—1984.

Berkeley Technology Law Journal
U.C. Berkeley School of Law
Student Center, Ste. 3
Berkeley, California 94720-7200
btlj@law.berkeley.edu
www.btlj.org

BERKELEY TECHNOLOGY LAW JOURNAL

VOLUME 24 NUMBER 3 SUMMER 2009

TABLE OF CONTENTS

SYMPOSIUM: SECURITY BREACH NOTIFICATION SIX YEARS LATER

SUBSCRIBER INFORMATION

The *Berkeley Technology Law Journal* (ISSN 1086-3818), a continuation of the *High Technology Law Journal* effective Volume 11, is edited by the students of the University of California School of Law, Berkeley (Boalt Hall), and published four times each year (March, June, September, January) by the Regents of the University of California, Berkeley, Journal Publications, School of Law, 2850 Telegraph Avenue, Suite 561 #7220 Berkeley, CA 94705-7220. Periodicals Postage Rate Paid at Berkeley, CA 94704-9998, and at additional mailing offices. POSTMASTER: Send address changes to Journal Publications, 311 U.C. Berkeley School of Law, University of California, Berkeley, CA 94720-7200.

Correspondence. Address all correspondence regarding subscriptions, address changes, claims for non-receipt, single copies, advertising, and permission to reprint to Journal Publications, 2850 Telegraph Avenue, Suite 561 #7220 Berkeley, CA 94705-7220; (510) 643-6600; JournalPublications@ law.berkeley.edu. Authors: see section entitled Information for Authors.

Subscriptions. Annual subscriptions are $65.00 for individuals, and $85.00 for organizations. Single issues are $27.00. Please allow two months for receipt of the first issue. Payment may be made by check, international money order, or credit card (MasterCard/Visa). Domestic claims for non-receipt of issues should be made within 90 days of the month of publication; overseas claims should be made within 180 days. Thereafter, the regular back issue rate ($27.00) will be charged for replacement. Overseas delivery is not guaranteed.

Form. The text and citations in the *Journal* conform generally to the UNITED STATES GOVERNMENT PRINTING OFFICE STYLE MANUAL (29th ed. 2000) and to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 18th ed. 2005). Please cite this issue of the *Berkeley Technology Law Journal* as 24 BERKELEY TECH. L.J. ___ (2009).

BTLJ ONLINE

The full text and abstracts of many previously published *Berkeley Technology Law Journal* articles can be found at http://www.btlj.org. Our site also contains a cumulative index, general information about the *Journal*, selected materials related to technology law, and links to other related pages.

INFORMATION FOR AUTHORS

The Editorial Board of the *Berkeley Technology Law Journal* invites the submission of unsolicited manuscripts. Submissions may include previously unpublished articles, essays, book reviews, case notes, or comments concerning any aspect of the relationship between technology and the law. If any portion of a manuscript has been previously published, the author should so indicate.

Format. Submissions are accepted in electronic format through the Express*O* online submission system. Authors should include a curriculum vitae and resume when submitting articles. The Express*O* submission website can be found at http://law.bepress.com/expresso.

Citations. All citations should conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 18th ed. 2005). In addition, the author should include his or her credentials, including full name, degrees earned, academic or professional affiliations, and citations to all previously published legal articles.

Copyrighted Material. If a manuscript contains any copyrighted table, chart, graph, illustration, photograph, or more than eight lines of text, the author must obtain written permission from the copyright holder for use of the material.

DONORS

The *Berkeley Technology Law Journal* and the Berkeley Center for Law & Technology acknowledge the following generous donors to Berkeley Law's Law and Technology Program:

Benefactors

CHADBOURNE & PARK LLP

COOLEY GODWARD KRONISH LLP

COVINGTON & BURLING LLP

FENWICK & WEST LLP

KIRKLAND & ELLIS LLP

LATHAM & WATKINS LLP

MORRISON & FOERSTER LLP

ORRICK, HERRINGTON & SUTCLIFFE LLP

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP AND AFFILIATES

WEIL, GOTSHAL & MANGES LLP

WILSON, SONSINI, GOODRICH & ROSATI

WINSTON & STRAWN LLP

Members

ALSTON + BIRD LLP

BAKER BOTTS LLP

BINGHAM MCCUTCHEN LLP

DLA PIPER RUDNICK GRAY CARY

DECHERT LLP

FINNEGAN HENDERSON FARABOW GARRETT & DUNNER LLP

FISH & RICHARDSON P.C.

GOODWIN PROCTER LLP

GUNDERSON DETTMER STOUGH VILLENEUVE FRANKLIN & HACHIGIAN, LLP

HAYNES & BOONE LLP

HICKMAN, PALERMO, TRUONG & BECKER, LLP

KEKER & VAN NEST LLP

KNOBBE MARTENS OLSON & BEAR LLP

MCDERMOTT WILL & EMERY

MORGAN, LEWIS & BOCKIUS LLP

PERKINS COIE LLP AND AFFILIATES

ROPES & GRAY LLP

SIDLEY AUSTIN LLP

SONNENSCHEIN NATH & ROSENTHAL LLP

TOWNSEND AND TOWNSEND AND CREW LLP

VAN PELT, YI & JAMES LLP

WHITE & CASE LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

Patrons

BAKER & MCKENZIE LLP

GREENBERG TRAURIG, LLP

DURIE TANGRI LLP

The *Berkeley Technology Law Journal* is a nonprofit organization and welcomes donations. Donors are recognized appropriately for their contributions. For more information, contact the *Berkeley Center for Law and Technology*, University of California, Berkeley, School of Law, 376 Boalt Hall Berkeley, California 94720-7200. Telephone: 510-642-8073. E-mail: bclt@law.berkeley.edu.

ADVISORY BOARD

BOARD OF EDITORS 2009-2010

BERKELEY CENTER FOR LAW & TECHNOLOGY

UCB SECURITY BREACH NOTIFICATION SYMPOSIUM

MARCH 6, 2009

HOW A BILL BECOMES A LAW, REALLY

California State Senator Joseph Simitian

At some point in your life you probably opened up a high school civics book to review a flow chart labeled "How a Bill Becomes a Law."

Though complex, the process that chart describes seems relatively thoughtful, deliberate, and in its own way, quite orderly. It is a substantially accurate description of the process in theory, which is to say it bears only a passing resemblance to the process in practice.

In truth, the legislative process is far more random, dramatic, and idiosyncratic than any flow chart could ever describe.

Indeed, Assembly Bill 700, the security breach notification legislation, which is the subject of my remarks this afternoon, is the law today only because of a spelling error, an afterthought, an unrelated concern with digital signatures, a page three news story, the rule of germaneness, the intellectual quirks of a lame-duck Senator, the personal experiences of 120 State legislators, and another bill altogether, Assembly Bill 2297.

That being the case, I've entitled my talk this afternoon "How a Bill Becomes a Law, Really."

In early 2001, I was newly-arrived in Sacramento, a just-elected member of the California State Assembly; and at my request, the then Speaker of the State Assembly created a six-member Select Committee on Privacy, and named me as its Chair.

In that capacity I began to explore the issue of on-line privacy, and met with industry representatives from Silicon Valley, the area I represent. I followed up with academicians and attorneys, as well as consumer advocates and privacy buffs. And I read as much on the subject as my schedule permitted, so that by February of 2002, I was ready to meet with industry representatives again, this time in Sacramento.

Somewhat naïvely, perhaps, I was determined to employ a "different" kind of process in exploring these issues—a conversation and a collaboration, rather than a debate or an adversarial argument. Into a room with perhaps 25 or 30 industry lobbyists and advocates I marched with a "Discussion Document" containing a list of nine issues related to online privacy.

Notwithstanding my repeated assurances that none of these nine items was in fact a formal proposal, the advocates who assembled assumed that none of these items would have been on my agenda absent some interest on my part in pursuing the items legislatively. The result was a meeting, which perhaps inevitably, focused more on defensive posturing than creative collaboration.

In truth, what I was looking for at the time was a relatively narrow issue to pursue; one that was well defined, with high prospects of passage. I thought then, and still do, that on-line visitors needed additional protection, and I held to the view that incremental progress was better than no progress at all.

As the February 22nd legislative deadline for bill introduction drew near, I had narrowed my list of possible proposals to a handful, and was inclined to introduce a bill that would focus on just two very limited but important functions: a requirement that anyone collecting personal identifying information online from Californians be obliged to post a privacy policy, and that they be obliged to comply with that policy (however limited or expansive it might be).

That was it. As I envisioned it at the time, that was the whole bill.

Before I formally introduced the bill, however, I thought it might be helpful if my staff and I checked one last time with a pair of behind-the-scenes advisors—two privacy savvy lawyers who had made themselves available to help on an occasional, and ad hoc, basis.

One was a fellow named Chris Kelly, formerly the Chief Privacy Officer at Excite@Home, and today the Chief Privacy Officer at Facebook. The other ad hoc advisor was a woman named Deirdre Mulligan, who just the year before had joined the Samuelson Clinic here at U.C. Berkeley.

Less than 48 hours before our legislative deadline, we put together an after-hours conference call. I quickly explained the bill, and asked for comment. Both Deirdre and Chris thought it was a good first effort. The bill was narrowly tailored, and modest in scope, but it was a significant privacy "plus" for folks who were doing business online. Yes, it was modest; but it was meaningful progress in a developing area of the law.

And then, almost as a throwaway, I asked "anything else?" "Well," suggested Deirdre, "If you wanted, you could add something else to provide notice in the event of a security breach—unauthorized access to confidential data. I know it's a long shot, but it might be worth a try. And if you actually got it passed, it would be a very big deal."

I hesitated for a moment. Notice of a breach had in fact been among the issues on my original nine item discussion agenda, but I'd passed it by as

overly ambitious. "What do you think?" I asked Chris, who answered, "Sure. Why not give it a try? The push-back will be huge; but if nothing else, it's a bargaining chip—a give-away as you move your bill through the process."

"O.K.," I said. "Let's do it." And in a split second, the decision was made. An eleventh hour afterthought became a part of the bill. One day before the deadline, I introduced Assembly Bill 2297, "The Online Privacy and Disclosure Act of 2002."

And that's when things got interesting because, as it turns out, the bill was a very hard sell—moving off the Assembly floor with just 41 votes (the bare minimum in an 80-member house).

But unbeknownst to me, I was about to catch a break.

According to subsequent press reports, "on April 5, 2002 computer hackers were able to illegally access sensitive financial and personal information, including the Social Security Numbers, of approximately 265,000 State workers, from a State database maintained at the Teale Data Center. According to the California State Controller's office, the information on these computers also contained employees' names and (payroll) deduction information . . . ."

The April 5th breach was apparently not discovered, however, until May 7th, and State employees were not notified until May 21st, nearly a month and a half after the incident. According to testimony heard in the State Senate it was during this time that "unauthorized persons in Germany attempted to access one state worker's bank accounts and another employee had an unauthorized change of address attempt made on her credit card account."

Significantly, among the 265,000 State employees whose data was compromised, there was a 120 member subset of employees critical to our story: eighty members of the California State Assembly and forty members of the State Senate—all of whom received the same form letter, almost two months after the incident, informing them of the breach.

Now, one of those State Senators was Mr. Steve Peace, a twenty-year veteran legislator in the final months of his final term, and not unimportantly, also the Chairman of the Senate Committee on Privacy.

In early June, still 2002, as my A.B. 2297 worked its way through the process, Senator Peace called an informational hearing to explore the ramifications of the incident at the Teale Data Center. Disturbed by what he found, Mr. Peace decided to propose legislation to address the need for notice; but quickly discovered that an existing bill, my own A.B. 2297, was coming his way, which created a bit of a turf problem.

On the Senate side of the Capitol, Mr. Peace had a genuine interest in the issue and by virtue of his position and seniority, he certainly had some standing. On the Assembly side, however, I'd been working on my bill with some success, and notwithstanding my status as a first term member in the Assembly, by the unwritten rules of the Legislature, I legitimately "owned" the issue.

The proposal I received from Mr. Peace, which was relayed by his staff to my staff to me, was that I should drop the "security breach" provision in my bill, that he would 'gut and amend' one of his bills to address the issue, and that I could be named principal co-author of Mr. Peace's bill in the Senate.

I was, to put it succinctly, unenthusiastic about the offer. While I respected Mr. Peace's standing and expertise, not to mention his clout, it seemed to me that I was being asked to be second banana on my own bill; and I suggested an alternative.

"How about I strip the 'security breach' language out of my A.B. 2297, but we both do a gut and amend to create a pair of security breach bills with identical language in the Assembly and the Senate?" On Senator Peace's bill I could be named as his principal co-author, and on my identical bill Senator Peace could be listed as my principal co-author.

In this way we would double our chances of successfully moving a bill through the process, we would both be genuine collaborators as to the content of the bills, and our respective contributions to the field would each be duly recognized. Mr. Peace considered, agreed, and we were on our way.

For my part, since I was still intent on moving A.B. 2297 with its original privacy policy and compliance provisions, I needed another vehicle—a bill that is—that could accommodate a "gut and amend" and become a security breach bill.

Happily, I had A.B. 700, a bill I wasn't using—an altogether unrelated piece of legislation dealing with digital signatures. I had introduced the digital signature bill a year and a half earlier at the behest of the California Association of Realtors, got it passed in the Assembly and then, when the bill proved unnecessary, let it languish in the Senate, where it sat quietly at this point in our story.

Now, in order to amend a bill, the proposed amendments must be "germane." And while "security breach" and "digital signature" issues may strike many of you as more or less unrelated—this was a case of "close enough for government work." Both bills did in fact deal with the conduct of business online; and perhaps more importantly, even as a first term Assembly member, I had already learned that "germaneness" is in the eye of the beholder. It

is essentially whatever forty-one members of the Assembly and twenty-one members of the Senate are willing to let it be. And so it was that A.B. 700, a digital signature bill, which had long been in hibernation, became an active effort at making new law on the issue of breach and notice.

Though the timeline was tight, our twin bills moved swiftly through the system.

The fact that every member of the Legislature had just been a tardily noticed victim was of immeasurable help. The issue was no longer hypothetical; it was now real, and it was personal.

Moreover, the fact that the bill regulated the behavior of State government as well as the private sector put many Republicans more at ease than a business directed bill might have done. For a number of my Republican colleagues, this was a chance to wag a finger at an unresponsive State bureaucracy, and they were happy to take it.

Mr. Peace's standing, staff, and expertise were helpful as well, and it didn't hurt that he was not only Chair of the Senate Committee on Privacy, but also the Chair of the Senate Budget Committee and our bicameral Budget Conference Committee. His bill moved, and so did mine.

As amendments were taken, token opposition become almost nonexistent. On August 31, 2002, the final day of the two-year session, the Assembly concurred in Senate Amendments by a unanimous vote on a special consent calendar, and, without any debate whatsoever, A.B. 700 was on its way to the Governor.

But still, the saga continues. As a pair of identical bills makes their way to the Governor, the obvious question is which one, if either, is about to become law. As it happens, if the Governor signs both bills, the second bill signed either "chapters out," or replaces, the first bill signed; or, at a minimum, supersedes an earlier identical provision.

The author of the second signed bill therefore gets to say that his bill has become State law. The author of the first signed bill, who of course is looking for bragging rights of his own, gets to say that his bill broke new ground and changed state law, if only for a moment.

In such a circumstance, of course, you can't help but wonder, when these two bills hit the Governor's office, in a crush of 1,379 end-of-session bills, will anybody notice, or care, which bills gets signed first. In fact, they do.

It turns out that the Peace bill had a typo, a spelling mistake. The error is noted and reported, so the Peace Bill is signed first, and my bill, A.B. 700, the Simitian bill, is signed second. The expectation then is that my bill will supersede and/or chapter out the Peace bill. Except, as it turns out, the legislation

Mr. Peace and I have authored does not simply amend existing law—it creates a wholly new statute: Sections 1798.29 and 1798.82 of the Civil Code.

That being the case, the duplicate statutes, all but identical except for the typo, both become law, and follow one after another in the Civil Code—almost indistinguishable, except that Mr. Peace's version may be identified by the missing "c" in "acquisition," roughly halfway through the code section.

At least that was the case until January 1, 2008. On that date, the redundant language in the code was corrected by yet another bill—Assembly Bill 1298 by Assembly Member Dave Jones—that made changes to existing law relating to the disclosure of personal information, including medical information maintained by a business or state agency or contained in a credit report. In addition to those substantive changes in law, A.B. 1298 repealed the duplicate sections of law placed into the code by Mr. Peace's bill back in 2002, leaving only the language of A.B. 700.

All of which is neither here nor there. The credit (or the blame, depending on your point of view) is properly shared by each of the two authors—each of whom brought something essential to what was ultimately a successful effort.

That being the case, it's probably time to look more closely at the substance, rather than the saga, of A.B. 700.

The underlying rationale for A.B. 700 is simplicity itself. Before a consumer can protect himself from the unauthorized acquisition and use of confidential information, the consumer has to know that an unauthorized acquisition has occurred.

Without that knowledge, the consumer isn't even aware of the need to protect himself—never mind thinking about the ways in which he might want to protect himself.

Simply put: to be unaware is to be vulnerable. And at its core, that's what A.B. 700 is all about.

By its terms, the bill provides that "any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system . . . to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

The same basic requirement applies to someone who maintains such data for an information owner or licensee; and, as mentioned earlier, the provisions of A.B. 700 apply to State agencies, in addition to private entities and individuals who "conduct business" in California.

As the bill worked its way through the system, a number of amendments were incorporated which were designed to respond to the concerns expressed by business and industry.

Among the accommodations to industry:

The notice requirement generally does not require notice of unauthorized acquisition of encrypted data.

The definition of personal information is more limited and narrowly tailored than originally proposed.

A legitimate delay in providing notice is authorized when necessary to accommodate legitimate law enforcement efforts.

The language of the bill was modified to help protect industry from unreasonable consequences where information may have been accessed, but not actually acquired, or where a good faith acquisition or inadvertent disclosure is involved.

The bill specifically provides for state preemption of the issue to ensure that cities, counties, or other public agencies in the State will not be able to impose additional or contradictory requirements.

And perhaps more critical to industry representatives, alternative notice provisions were incorporated, so that if the cost or number of notices required proves unduly burdensome, a range of notice options is authorized.

Finally, the operative date of the measure was delayed six months, from January 1st to July 1st of 2003, in order to provide adequate time for informing and educating the State agencies and the business community as to the obligation to comply and the essential elements of compliance; and in order to provide adequate time for public and private entities to adopt the appropriate practices and policies, and further secure their systems.

In its final form, I think A.B. 700 mostly does what it set out to do: it provides some assurance that when consumers are at risk because of an unauthorized acquisition of personal information, the consumer will know that he is vulnerable, and will thus be equipped to make an informed judgment about what steps, if any, are appropriate to protect himself physically and/or financially.

That, as I've said, was and is the core purpose of A.B. 700. There were other goals as well, however.

Certainly when A.B. 700 was written and passed, I hoped to provide an incentive to those responsible for public and private databases to improve their security (and thus reduce the risk for all of us). I believed then and believe now that "shame and cost" are powerful motivators for improved security.

We also hoped, but were not sure, that non-Californians, consumers around the country, would also be protected to some degree, since as a practical public-relations matter it's difficult to inform only the customers in California when a national database is hacked. As it's turned out, this goal has been more fully realized than we might have hoped.

And, finally, we hoped to prod other states or the federal government into taking meaningful action. As you all know, it is the states and not the federal government that have responded to the challenge.

I think I should say at this point that among my principal interests in pursuing A.B. 700, and related legislation, is a firm belief that the future of e-commerce is directly linked to the public's confidence in online privacy protection and data security.

I am a Silicon Valley legislator. In 2001, the American Electronics Association named me their High-Tech Legislator of the Year. And I am firmly convinced that the growth of e-commerce will be stifled until and unless the public and private sectors, together, address the concerns of the buying public.

It is my strongly held view that enlightened self-interest should have made High Tech an advocate, rather than an adversary, for A.B. 700, and the subsequent legislation it spawned. That is perhaps a discussion for another time.

Having said all that, it's time to talk about the next steps.

The passage of time, and action by more than forty other states, makes it appropriate to ask and answer some obvious questions:

How well has the California statute performed during the past six years?

Can it be improved upon, and, if so, how?

And, of course, what have other states been doing; and, what can we learn from them?

My own view after a half dozen years is that there are least two explicit improvements to the California statute that are called for.

First, greater clarity and specificity as to the content of security breach notices is long past due. Our experience tells us that while many of the breach notices sent out may be clear and comprehensive, a substantial number are not—leaving consumers more confused than informed.

Moreover, greater clarity and specificity about the required content of a security breach notification will also benefit businesses and public agencies who presently wonder just what information they need to supply in order to comply with the law.

Fortunately, nearly a dozen other states have already legislated such content standards, and their work can inform our efforts.

The other relatively modest but significant improvement that can and should be made is a requirement that when notice is sent, a duplicate notice should be sent to the state. This simple additional requirement would give law enforcement, state legislatures, and security professionals a better understanding of the nature and scope of the problem and, I would hope, improve law enforcement, legislative action, and security efforts in this arena.

These two improvements are in fact contained in the currently pending California Senate Bill 20, of which I am the author. My hope is that by year's end S.B. 20 will have been passed by the Legislature and signed by the Governor. In my view, that would make a good law, a groundbreaking law, even better.

In closing, I must tell you that my work in this area has been both challenging and gratifying. One of the most satisfying aspects of my work is the opportunity it affords me to explore whole new areas of thought, commerce, or society—or, to put is less grandiosely, to stick my nose into other people's business.

I entered the Legislature in the year 2000 with no background whatsoever in privacy issues, and no real plan or expectation that privacy issues would ever be a part of my legislative agenda.

In 2003, when Senator Peace and I were recognized by *Scientific American* magazine as one of Scientific American's 50 Leaders in Technology, I recalled that my high school science teacher said he always thought I'd be lucky if I could get a paid subscription to *Scientific American*, never mind get myself inside the magazine.

And while I was flattered to be the 2007 recipient of the RSA Conference Award for Excellence in Public Policy, presented in front of several thousand computer security specialists, I must tell you the staff in my office who help me manage my email were more than a little amused.

But I have learned a lot since my earliest forays into the challenging world of online privacy, and if sharing some portion of what I've learned with you today has been either helpful or enjoyable then I'll be very pleased.

But please know how much I appreciate the opportunity to learn from you and how valuable it is for me as a policymaker to be able to tap into your experience and expertise as I go about my business.

I appreciate it. I appreciate your time and attention. And I appreciate the opportunity to share my thoughts with you this afternoon.

Many, many thanks.

GOVERNMENT DATA BREACHES

By A. Michael Froomkin†

TABLE OF CONTENTS

I. INTRODUCTION

Private data held by the government is not the same as private data held by others. Much of the government's data is obtained through legally required disclosures or participation in licensing or benefit schemes where the government is, as a practical matter, the only game in town. These coercive

---

† University of Miami School of Law. Thanks are due to Caroline Bradley, Reid Cushman, and Patrick Gudridge for helpful conversations, as well as to Barbara Brandon, Kaema Akpan, Adam Schlosser and Victoria Wilson for research help.

or unbargained-for disclosures impute a heightened moral duty on the part of the government to exercise careful stewardship over private data. But the moral duty to safeguard the data and to deal fully and honestly with the consequences of failing to safeguard them is, at best, only partly reflected in state and federal laws and regulations.

Activists, academics, and state legislatures have identified and, in some cases, taken significant preliminary steps to address the problem of data breaches—the unintentional release of personally identifiable information by lawful holders of the data—in the United States.[1] To date, however, the primary focus of these efforts in the U.S. has been private data breaches.[2] This paper addresses a related problem that, while by no means ignored, has not received the attention it deserves: data breaches in the U.S. public sector.[3]

The problem of public data breaches is similar to that of private data breaches, but there are also major differences relating to the nature of the information, the means by which the information is collected, and especially the legal and institutional regime under which the information is held. For example, much government-held data is acquired via legal compulsion or the result of processes where there is neither competition nor bargained-for exchange. These and other differences make the public problem more heterogeneous and arguably less tractable than its private cousin. As a result, while both the prophylactic and corrective justice solutions to the public data breach problem have important resemblances to the solutions aimed at the private sector, the differences are also substantial.

I begin this paper with an illustrative survey of the ways in which government data and government data breaches resemble and differ from private data breaches. I also briefly survey the extent to which the government's moral duty to safeguard data is currently instantiated in statutes and, increasingly, in regulations. Because governments determine what defines an ac-

1. *E.g.*, Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 380 (2006).

2. *E.g.*, ADAM SHOSTACK & ANDREW STEWART, THE NEW SCHOOL OF INFORMATION SECURITY (2008) (advising firms and analysts to apply economic principles to breach problems); Stephen Schauder, *Developments in Banking and Financial Law: 2005*, 25 ANN. REV. BANKING & FIN. L. 109, 111-18 (2006) (discussing the difficulty in balancing the needs of consumer privacy, security, and costs in developing privacy regulation); Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 915-28 (2007) (discussing laws that require private companies to notify individuals of data security incidents involving their personal information).

3. Previous treatments of the government data breach problem include Flora J. Garcia, *Data Protection, Breach Notification, and the Interplay Between State and Federal Law: The Experiments Need More Time*, 17 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 693, 725-26 (2007) (arguing against new regulation at present) and Solove & Hoofnagle, *supra* note 1, at 379-80 (noting gaps in the Federal Privacy Act).

tionable data breach and what remedies are available for damages caused by these breaches, it is not surprising that the remedies available to victims of a government data breach are often less than those available to victims of private sector data breaches.

Part III of this paper discusses the extent to which the government's duty to safeguard private data has a constitutional foundation. I argue that there is a constitutional right, either free-standing or based in Due Process, against government disclosure of personal data lawfully acquired under legal compulsion, at least in cases where the government failed to take reasonable precautions to safeguard the data. This right is separate from any informational privacy rights that constrain the government's ability to acquire personal or corporate information.

The argument requires at most a small, logical extension of existing law; arguably, existing law already encompasses it. The key, oddly enough, is Chief Justice Rhenquist's opinion in *DeShaney v. Winnebago County Department of Social Services*.[4] In the course of explaining why recovery was not appropriate in a child-abuse case where the government, although on notice, did nothing, the Chief Justice distinguished a class of cases in which the government would be liable: those cases where the government took such full control of the situation that it displaced, and disempowered, the relevant private parties. Although the Chief Justice's opinion contemplates people in totalizing institutional settings such as government-run prisons or asylums, it is, at most, a tiny stretch to apply his logic to data held by a government. In the case of government data breaches, the government has full control over the data before releasing it; there is nothing that the subject of the data can do to influence the conditions under which the data is secured.

When the government releases private information without a legal right to do so it harms the subject of the data. The harm is equally large, and should be equally compensable, whether the breach was intentional or negligent. Under the *DeShaney* logic, victims of many governmental privacy breaches should have a claim against states under 42 U.S.C. § 1983 (2006). Similar constitutional claims against the federal government would require a *Bivens* action[5]; I examine, but ultimately reject, a theory of government liability based directly on a *Bivens*-style constitutional privacy tort in light of the Supreme Court's current hostility to expansion of *Bivens*.[6] As a result, persons injured by federal data breaches will have substantially inferior remedies available to them than will victims of state breaches. Further, in both state

4. 489 U.S. 189 (1989).
5. *See* Bivens v. Six Unknown Fed. Narcotics Agents, 403 U.S. 388 (1971).
6. *See infra* Section III.B.2.

and federal cases, victims will find that claims for effective remedies may be hampered by governmental immunity and the problem of valuing the harms caused by a breach.

II. THE NATURE OF GOVERNMENT DATA BREACHES

In this Part, I survey the factual and legal background relating to government data breaches in the U.S. It begins with an introduction to the great quantity and variety of data held by federal and state governments, then looks at the limited statistics available regarding the types, frequency, and size of government data breaches. The final three sections consider three types of prophylactic responses: the legal regime governing breaches; the incentive structure in which the breaches occur; and the federal government's recent improvements in the federal regulatory data-holding regime—improvements that are notably silent as to the issue of compensation for breaches.

A. NATURE OF THE DATA

Governments hold a wide variety of data on natural and legal persons, great both in scope and in scale. Numerical comparisons with the private sector are difficult given the inherent difficulties of quantification and the lack of detailed information as to how much data both groups actually hold.[7] In addition, data held by the public and private sectors overlap due to data sharing and data transactions.[8] There is no doubt, however, that federal and state governments hold a wide variety of data about persons and firms (See Tables 1 & 2).

7. For example: does one count bytes, records, or persons in the system? The extent to which disparate decentralized record systems permit cross-referencing is also difficult to quantify. Governments have the greatest breadth of information, e.g. census records. Yet, businesses may in some cases have more fine-grained data if they capture, for example, the details of economic transactions and internet clicktrails. Choicepoint alone is said to have over nineteen billion "records" in its databases. *See* John T. Fakler, *ChoicePoint Settles with FTC*, S. FLA. BUS. J., Jan. 30, 2006, http://southflorida.biz-journals.com/southflorida/stories/2006/01/30/daily13.html. But without more information as to the nature of those records, gross comparisons to state and federal databases are unlikely to be very meaningful.

8. *See, e.g.*, Fred. H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 439 (2008).

Table 1: Illustrative Types of Federal Government Data

Census data[9]	Personal tax data[10]
Corporate tax data[11]	Military records[12]
National security intercepts (e.g. telephone/e-mail intercepts by NSA)	Law enforcement data (e.g. FBI investigative data)
Prison records[13]	Passport applications[14]
Health records (e.g. VA, Medical benefits programs)	Transfer program records (e.g. Social Security, Food Stamps, Veterans)
Federal employee records[15]	Regulatory disclosures (e.g. trade secrets, required disclosures, results of inspections)
Contracting, purchasing[16]	Sealed court records[17]
Immigration records	

9. *See, e.g.*, 13 U.S.C. § 8 (2006).

10. *See, e.g.*, 26 U.S.C. § 6107(b) (2006).

11. *See, e.g.*, INTERNAL REVENUE SERVICE, STATISTICS OF INCOME - 2006: CORPORATION INCOME TAX RETURNS (2006), *available at* http://www.irs.gov/pub/irs-soi/06coccr.pdf.

12. *See, e.g.*, 32 C.F.R. § 70.8(b)(9)(i) (2009).

13. *See, e.g.*, 28 C.F.R. § 512.15 (2009).

14. *See* U.S. Department of State, Obtain Copies of Passport Records, http://www.travel.state.gov/passport/services/copies/copies_872.html (last visited Oct. 12, 2009).

15. *See, e.g.*, 41 C.F.R. § 105-56.015(c) (2009).

16. *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, INTERNATIONAL TRADE: CURRENT GOVERNMENT DATA PROVIDE LIMITED INSIGHT INTO OFFSHORING OF SERVICES, GAO 04-932, at 28-29 (2004), *available at* http://www.gao.gov/new.items/d04932.pdf

17. *See, e.g.*, 6 C.F.R. § 27.400(i)(4) (2009).

Table 2: Illustrative Types of State/Local Government Data[18]

State tax data[19]	State law enforcement data (e.g. police records)
K-12 & university educational records[20]	Records relating to foster children and other reported to child welfare agencies[21]
State transfer programs records	State court records (including, in particular, family court)
State prison records[22]	State regulatory data[23]
State contracting, purchasing	Personal, occupational, and corporate license data (e.g. Driver's Licenses, Bar membership, Contractor licensing)[24]
Records deposited in connection with Driver's License applications subject to the REAL ID Act[25]	

Most privately acquired data is generated incident to, or accompanied by, an economic transaction. Even private medical records originate in a transaction with an important economic component, such as the purchase of medical services or medicine. One characteristic shared by almost all private non-medical transactions is that the data subject could have chosen to forgo the exchange, or could have instead chosen to transact with another entity. Of course, alternatives may be less convenient or more expensive, but the choice nonetheless exists.

The most important exception to this general rule of data collection incident to economic exchange may be that private sector data holders can acquire information about people from the government,[26] or as agents for the government. And there are undoubtedly a number of exceptions to the vo-

18. *See generally* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 15 (2004) (noting that U.S. federal agencies and departments maintain nearly 2000 databases with records relating to immigration, financial history, welfare, licensing, etc); STAFF OF H. COMM.ON GOV'T REFORM, 109TH CONG., AGENCY DATA BREACHES SINCE JANUARY 1, 2003 (2006), *available at* http://oversight.house.gov/documents/20061013145352-82231.pdf.

19. *See, e.g.*, CONN. GEN. STAT. ANN. § 12-120a (West 2008).

20. *See, e.g.*, FLA. STAT. ANN. § 1002.22 (West 2009); W. VA. CODE § 48-9-601 (2001).

21. *See, e.g.*, CAL. WELF. & INST. CODE § 16011 (West 2002).

22. *See, e.g.*, 730 ILL. COMP. STAT. ANN. 5/3-5-1 (West 2009).

23. *See, e.g.*, N.C. GEN. STAT. ANN. § 58-2-69 (West 2009).

24. *See, e.g.*, ALASKA STAT. § 28.05.061 (2009).

25. REAL ID Act of 2005, Pub. L. No. 109-13, div. B, 119 Stat. 231, 302 (2005).

26. *Cf.* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 595-98 (2004) (describing ways in which the government can acquire information from private sector data holders).

luntary character of the transactions, such as emergency medical assistance and the provision of monopoly utility services (such as electricity or natural gas), for which there is only one provider and the option to do without is not realistic.[27] But these cases, while significant in their salience and in the sensitivity of the personal data they give rise to, are nonetheless a very small fraction of the sources of private data in private hands.

Government-held data differs from privately held data in one critical respect: Most of the data listed in Tables 1 and 2 are either disclosures that are required by law (e.g. tax returns, the census, law enforcement) or created in connection with an activity for which there is no realistic alternative source or supplier (e.g. licensing or benefits). Other than government-as-employer, most of the major listed categories of government activity that generate data are not meaningfully optional.

B. TYPES, CAUSES, AND FREQUENCY OF BREACHES

"A data breach occurs when there is a loss or theft of, or other unauthorized access to, data containing sensitive personal information that results in the potential compromise of the confidentiality or integrity of data."[28] Personal data generally includes information that can be used to locate or identify an individual: name, address, telephone number, Social Security Number, driver's license number, account number, or credit or debit card number. It also includes more sensitive information, such as income, personal health records, military records, law enforcement investigatory records, and multifarious disclosures made in connection with the application for government licenses or benefits.

In addition to personal data, the government also maintains extensive records regarding corporations, partnerships, unions and other legal persons. These data include tax records, information submitted in connection with bids for government contracts, and often-voluminous submissions in connection with license applications. Firms in certain highly regulated industries, such as financial service providers, must also make regular detailed submissions in order to comply with their legal obligations.

1. Types and Causes of Breaches

While the data held by state and federal governments may be broader in scope than that held in the private sector, the types of data breaches to which

27. It may be notable that in many of these cases, the lack of choice arises out of or in connection with a government-granted monopoly.

28. Gina Stevens, *Federal Information Security and Data Breach Notification Laws*, CONG. RESEARCH SERV. REPORT RL34120 1 (2009), *available at* http://assets.opencrs.com/rpts/RL34120_20090129.pdf.

the data are vulnerable are in many cases similar. But while the public sector is vulnerable to all the risks that bedevil the private sector, there are some additional dangers that are either peculiar to the public sector or so different in scale as to amount to a difference in kind.

Government data breaches include both scenarios common to the private sector and some that are rarely found there (see Table 3).

Table 3: Major Types of Government Data Breaches

Data released intentionally, but in violation of law or regulations	Data released accidentally due to human error or misconfigured software
Data on physical media that is lost or stolen or otherwise not secured	Insider access in excess of defined permissions or for private purposes, or both
Malfunctioning or wrongly designed software[29]	Outside hackers,[30] viruses, trojan horses
Purportedly anonymized data releases that can be reverse engineered to create personally identifiable data (not unknown in the private sector, but of particular concern relating to census data)[31]	Foreign spying (contrast to industrial espionage in the private sector)

The Privacy Rights Clearinghouse attributed government data breaches in 2006 to five causes: "human/software incompetence" was the largest single cause, responsible for 44% of the cases found; laptop theft was second, accounting for 21%, with other thefts close behind at 17%; outside hackers caused 13% of the known cases; and insider malfeasance was blamed only 5% of the time.[32]

2. Frequency and Size of Breaches

At present, there is no unified and mandatory reporting system for state or federal data breaches. Thus estimates of the size and frequency of gov-

29. *See, e.g.*, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, THE INTERNAL REVENUE SERVICE DEPLOYED TWO OF ITS MOST IMPORTANT MODERNIZED SYSTEMS WITH KNOWN SECURITY VULNERABILITIES, 2008-20-163, at 2 (Sept. 24, 2008), *available at* http://www.treas.gov/tigta/auditreports/2008reports/200820163fr.pdf.

30. Hacking/breaking into a non-public government computer can result in fines or prison sentences ranging from one to twenty years depending on the severity of the breach. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006).

31. *See, e.g.*, LaTanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality,* 25 J.L. MED. & ETHICS 98, 100 (1997) ("In deidentified data, all explicit identifiers . . . are removed, generalized or replaced with a made-up alternative. Deidentifying data does not guarantee that the result is anonymous."); Michael Arrington, *AOL Proudly Releases Massive Amounts of Private Data*, TECH CRUNCH, Aug. 6, 2006, http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/.

32. PRIVACY RIGHTS CLEARING HOUSE, CHRONOLOGY OF DATA BREACHES 2006: ANALYSIS (2007), http://www.privacyrights.org/ar/DataBreaches2006-Analysis.htm.

ernment data breaches rely to some extent on anecdote and guesswork. Nevertheless, even without comprehensive data there is no doubt that breaches of government data are frequent and significant. One recent commentator estimates that from 2000 to 2008, about 530 million records containing personal data were exposed or mishandled.[33] Of those incidents, 23% are estimated to be due to non-education government sources, with an additional 23% shared between public and private educational institutions.[34] Thus, the public sector accounted for somewhere between a quarter and half of all *reported* U.S. data breaches. When one considers that governments frequently are not covered by the increasing number of state data breach reporting statutes that reach private actors, it is possible that the true fraction is higher still.[35]

The Identity Theft Resource Center (ITRC), a private, non-profit group funded in part by data-brokers,[36] identified 110 breaches of state (excluding educational and health sectors), federal, and military databases in 2008, exposing 2,954,373 records.[37] In comparison, the ITRC documented 110 breaches of state and federal databases in 2007, exposing 8,156,682 records.[38] Since 2003, nineteen federal bodies have reported at least one loss of personal data that could potentially expose individuals to identity theft.[39] In one recent incident, the Department of Veteran's Affairs (VA) exposed the records of 26.5 million veterans and active-duty military personnel when computer

33. Jay Cline, *530M Records Exposed, and Counting*, COMPUTER WORLD, Sept. 9, 2008, *available at* http://www.computerworld.com/s/article/9114176/530M_records_exposed_and_counting.

34. *Id.*

35. On the other hand, according to IDENTITY THEFT RESOURCE CENTER, SECURITY BREACHES 2008 (2009), *available at* http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2008.shtml, "[t]he Government/Military category has dropped nearly fifty percent since 2006, moving from the highest number of breaches to the third highest." To what extent this is due to improved practices, and to what extent this is an artifact of reporting rates is not clear.

36. IDENTITY THEFT RESOURCE CENTER, CORPORATE OVERVIEW 3 (2009), *available at* http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Corp._Overview_200906 25.pdf.

37. IDENTITY THEFT RESOURCE CENTER, 2008 DATA BREACH STATS 19 (2009), *available at* http://www.idtheftcenter.org/BreachPDF/ITRC_Breach_Stats_Report_2008_final.pdf.

38. IDENTITY THEFT RESOURCE CENTER, 2007 DATA BREACH STATS 13 (2008), *available at* http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Stats_Report_20071231_1.pdf.

39. *See* COMM. ON GOV'T REFORM, *supra* note 18, at 3-14 (listing the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, and Veterans Affairs, as well as the Office of Personnel Management and the Social Security Administration).

equipment was stolen from a VA employee's home.[40] Likewise, state breaches also occur. In 2008, for example, the Des Moines Register discovered that, since January 2005, the Iowa County land recorders had been posting documents containing the Social Security Numbers of thousands of Iowa residents, including the Governor, on a publicly available web site.[41]

C. UNIQUE LEGAL REGIME

Governments operate in a unique legal regime because they can define the legal definition of a data breach. Governments consider hacking—breaking into a non-public government computer—a serious crime that can result in fines or prison sentences ranging from one to twenty years depending on the severity of the breach.[42] Equally important, in the civil context, governments get to set the legal definition of what is a data breach and what is business as usual. Only some of the forty-four states with data breach statutes subject themselves to notice obligations similar to those that they impose on the private sector. In other words, subject only to federalism constraints and constitutional limitations, governments define which of their acts in releasing data constitutes an action for which the subject of the data can sue the government, just as they define the legal penalties for private data breaches.

State and federal governments also enjoy sovereign immunity. This immunity, however, is far from absolute because it does not protect state or federal governments from some constitutional claims.[43] Furthermore, both the federal and state governments have voluntarily abrogated their sovereign immunity for large classes of cases,[44] but even here there are limits. In addi-

---

40. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, INFORMATION SECURITY: AGENCIES REPORT PROGRESS, BUT SENSITIVE DATA REMAIN AT RISK, GAO 07-935T, at 6 (June 7, 2007), *available at* http://www.gao.gov/cgi-bin/getrpt?-GAO-07-935T.

41. *See* Jaikumar Vijayan, *Social Security Numbers Exposed on Iowa Land-Records Web Site*, COMPUTER WORLD, Sept. 5, 2008, *available at* http://www.computerworld.com/s/article/9114172/Social_Security_numbers_exposed_on_Iowa_land_records_Web_site.

42. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(3) (2006).

43. *See* James E. Pfander, *Sovereign Immunity and the Right to Petition: Toward a First Amendment Right to Pursue Judicial Claims Against the Government*, 91 NW. U. L. REV. 899, 972 (1997) ("[W]here the Constitution requires the government . . . to make victims . . . of constitutional violations whole, remedial obligations apply whether or not the government has adopted an effective waiver of sovereign immunity."); *see generally* Richard H. Seamon, *The Asymmetry of State Sovereign Immunity*, 76 WASH. L. REV. 1067, 1072-1102 (2001) (discussing current doctrines of state sovereign immunity); Gregory C. Sisk, *The Continuing Drift of Federal Sovereign Immunity Jurisprudence*, 50 WM. & MARY L. REV. 517, 574-87 (2008) (examining recent federal sovereign immunity jurisprudence). However, the Constitution imposes some limits on the power of the federal government to subject state governments to suit. U.S. CONST. amend. XI.

44. *See, e.g.*, Clark v. Barnard, 108 U.S. 436, 447 (1883) ("The immunity from suit be-

tion, through section 1983, the federal government has created a mechanism for citizens to sue states if their rights are violated.[45]

The leading example is *Collier v. Dickinson*, a rare, perhaps unique, data-privacy-related section 1983 claim decided in the Eleventh Circuit.[46] Executive-level officers of the Florida Department of Highway Safety and Motor Vehicles (DHSMV) were sued for selling personal information of plaintiffs to mass marketers in violation of the Driver Privacy Protection Act (DPPA).[47] The District Court originally dismissed the claim, holding that qualified immunity shielded the executives' actions.[48] The District Court also held that there is no constitutional right to privacy of the information provided to the DHSMV.[49] The Eleventh Circuit, however, held that the DPPA establishes a statutory right to privacy and that the plaintiff's allegation that the executives acted intentionally and willfully in violation of the DPPA survived summary judgment.[50] Rather than lose the suit, the government agreed to settle with the class of Florida drivers for $10.4 million, meaning that individual members of the class got $1—yes, a whole dollar—each.[51]

The fact that they have lawmaking power means that federal and state governments retain a unique ability to use their legislative, regulatory, and judicial power to define what constitutes a legal data dissemination and what liability they will bear for data breaches. Of those states that have breach laws covering the private sector, several impose duties on themselves similar to

---

longing to a State, which is respected and protected by the Constitution within the limits of the judicial power of the United States, is a personal privilege which it may waive at pleasure."). *But see* Seminole Tribe v. Florida, 517 U.S. 44, 59 (1996) (finding Congress does not have the power to abrogate state sovereign immunity unless it invokes Section 5 of the Fourteenth Amendment or the Interstate Commerce Clause).

45. Section 1983 creates a federal cause of action:

> Every person who, under color of any statute, ordinance, regulation, custom or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress.

42 U.S.C. § 1983 (2006).

46. 477 F.3d 1306 (11th Cir. 2007).

47. *Id.* at 1307.

48. *Id.*

49. Collier v. Dickinson, No. 04-21351-CIV, 2006 WL 4998653, at *10 (S.D. Fla. Mar. 30, 2006) (citing Pryor v. Reno, 171 F.3d 1281, 1288 n. 10 (11th Cir. 1999)), *rev'd* 477 F.3d 1306 (11th Cir. 2007).

50. *Dickinson*, 477 F.3d at 1309-10.

51. Posting of Steve Bousquet to The Buzz: Florida Politics, *For Motorists, a Long Overdue $1 Credit*, http://blogs.tampabay.com/buzz/2009/01/for-motorists-a.html (Jan. 15, 2009, 14:53 EST).

those that they impose on the private sector,[52] but others do not.[53] A few states do provide for fines if the government fails to notify the victim and damages occur as a result of that failure.[54] Uniquely, Oklahoma has a breach law for the public sector, but none for the private sector.[55]

There is no logical reason why various types of unplanned data releases should trigger duties and sanctions when performed by private entities, but trigger no legal consequences when performed by governments. The arguments regarding planned, or permitted, data releases are more complicated. There are public policy reasons why some government disclosures should be encouraged, even if analogous disclosures by private parties might not be permitted. Yet the argument is not equally persuasive in all cases. On the one hand, some government disclosures clearly serve values of transparency,

52. *See* ALASKA STAT. § 45.48.010 et seq. (2009); ARIZ. REV. STAT. ANN. § 44-7501 (2008); ARK. CODE ANN. § 4-110-103 (West 2008); CAL. CIV. CODE §§ 1798.29, 1798.82 (West 2009); DEL. CODE ANN. tit. 6, § 12B-102 (2008); HAW. REV. STAT. ANN. § 487N-2 (LexisNexis 2008); IDAHO CODE ANN. § 28-51-105 (2008); 815 ILL. COMP. STATE. ANN. 530/12 (LexisNexis 2009); IOWA CODE ANN. §§ 715C.1-715C.2 (West 2008); KAN. STAT. ANN. § 50-7a02 (2008); LA. REV. STAT. ANN. § 51:3074 (2008); MASS. GEN. LAWS ANN. ch. 93H, § 3 (West 2007); MICH. COMP. LAWS ANN. § 445.72 (West 2008); NEB. REV. STAT. ANN. § 87-802 (LexisNexis 2009); NEV. REV. STAT. ANN. § 603A.220 (LexisNexis 2009); N.H. REV. STAT. ANN. § 359-C:19 et seq. (2009); N.J. STAT. ANN. § 56:8-163 (West 2009); N.Y. GEN. BUS. § 899-aa, N.Y. STATE TECH. § 208 (2009); OHIO REV. CODE ANN. §§ 1349.19, 1347.12 (West 2009); S.B. 583, 74th LEGIS. ASSEMB., REG. SESS. (Or. 2007); 73 PA. STAT. ANN. § 2303 (West 2008); R.I. GEN. LAWS § 11-49.2-3 (2009); S.C. CODE ANN. §§ 39-1-90, 1-11-490 (2008); TENN. CODE ANN. § 47-18-2107 (2008); VT. STAT. ANN. tit. 9, § 2430 (2008) (excluding law enforcement agencies and the department of public safety); VA. CODE ANN. § 18.2-186.6 (West 2008); WASH. REV. CODE ANN. §§ 19.255.010, 42.56.590 (West 2009); W. Va. CODE ANN. § 46A-2A-101 (West 2009); WIS. STAT. ANN. § 134.98 (West 2009).

53. *See* COLO. REV. STAT. § 6-1-716 (2008); CONN. GEN. STAT. ANN. § 36a-701b (West 2009); D.C. CODE 28-3852 (2009); FLA. STAT. ANN. § 817.5681 (West 2008) (imposing duty on government only when data storage function was contracted out to private firm); GA. CODE ANN. § 10-1-911 (West 2008) (excluding government agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes); IND. CODE ANN. § 24-4.9-1-1 et seq. (West 2009); ME. REV. STAT. ANN. tit. 10, § 1348 (2008) (imposing duties only on information brokers and other persons); MD. CODE ANN., COM. LAW § 14-3504 (West 2008); MONT. CODE ANN. § 30-14-1704 (2007); N.C. GEN. STAT. ANN. § 75-66 (2009) (imposing a duty on the government only when a person knowingly publicizes the personal information of another with actual knowledge that the person whose personal information is disclosed has previously objected to any such disclosure); N.D. CENT. CODE, § 51-30-02 (2008); TEX. BUS. & COM. CODE ANN. § 521.053 (Vernon 2009); UTAH CODE ANN. § 13-44-202 (2008); WYO. STAT. ANN. § 40-12-502 (2009).

54. For example, Louisiana and New Hampshire award actual damages that result from failure to notify. LA. REV. STAT. ANN. § 51:3075 (2009); N.H. REV. STAT. ANN. § 359-C:21 (2007). On the other hand, Utah explicitly excludes these claims. UTAH CODE ANN. § 13-44-301(2)(a) (2008) ("Nothing in this chapter creates a private right of action.").

55. OKLA. STAT. ANN. tit. 74, § 3113.1 (West 2009).

which justifies rules such as the Freedom of Information Act (FOIA).[56] On the other hand, too much transparency may amount to little more than state-mandated data breaches when private information is posted online,[57] or if businesses' trade secrets, submitted in confidence as part of a regulatory proceeding, are released to the public.[58]

Governments, like firms, have a need for revenue, but only governments can legalize their own data breaches. Even here, however, federalism imposes limits, as demonstrated by Congress's reaction to the decision by some states to sell personal data collected incident to the issuance of driver's licenses. Congress enacted the Driver's Privacy Protection Act of 1994 (DPPA),[59] in order to regulate the disclosure of such information.[60] The DPPA's regulatory scheme restricts the State's ability to disclose a driver's personal data without the driver's consent,[61] and to reuse covered information acquired by private parties.[62]

The Supreme Court upheld the constitutionality of the DPPA in *Reno v. Condon*, rejecting a federalism challenge brought by South Carolina.[63] The lynchpin of Chief Justice Rhenquist's opinion is that the DPPA is similar to the statute upheld in *South Carolina v. Baker*, which was found to be constitu-

---

56. 5 U.S.C. § 552 (2006).

57. *See, e.g*, Vijayan, *supra* note 41.

58. Consider the facts of *Chrysler Corp. v. Brown*, sometimes called a "reverse FOIA case," in which Chrysler attempted to block the Defense Logistics Agency's release of its trade secret. 441 U.S. 281, 285, 291 (1979). The Supreme Court assumed that FOIA Exemption 4, 5 U.S.C. § 552(b)(4), would allow the agency to block release if it chose to do so. 441 U.S. at 285, 291. But the agency chose not to invoke Exception 4 and informed Chrysler of their intention to release the information. *Id.* at 287-88. The Supreme Court held that FOIA did not give Chrysler reason to object to the release, but remanded for consideration of the protections that might be available under the Trade Secrets Act, 18 U.S.C. § 1905. *Id.* at 318-19. The discretionary nature of the information release is illustrated by agency practices after *Chrysler*: in order to assure firms that agencies will not use their discretion to release information that the firms prefer to keep private, a category that extends well beyond trade secrets, agencies and firms enter into enforceable confidentiality agreements. *See, e.g.*, JEROME G. SNIDER, CORPORATE PRIVILEGES AND CONFIDENTIAL INFORMATION 2-77 (1999).

59. 18 U.S.C. §§ 2721-2725 (2006).

60. 138 Cong. Rec. H1785-01 (1992).

61. Note especially § 2721, which, with some exceptions, makes it an offense for a state department of motor vehicles officer, employee, or contractor to release personal data gathered in connection with a motor vehicle record, defined as a "motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." 18 U.S.C. §§ 2721, 2725 (2006). Permitted uses include safety recalls, law enforcement, civil and criminal proceedings and "use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license" required by law. 18 U.S.C. § 2721(b) (2006).

62. *See* 18 U.S.C. § 2721(c) (2006).

63. 528 U.S. 141, 143 (2000).

tional because it "'regulate[d] state activities,' rather than 'seek[ing] to control or influence the manner in which States regulate private parties.'"[64] Instead, "[t]he DPPA regulates the States as the owners of data bases,"[65] suggesting that the data are just another form of property subject to ordinary regulation.

Indeed, there are a few significant federal statutory and regulatory limitations on the ability of both state and federal governments to release private data at will. One of the most broad-reaching rules is the 1996 Health Insurance Portability and Accountability Act (HIPAA).[66] HIPAA applies to federal, state, and local government hospitals, as these meet the definition of a covered "health care provider."[67] HIPAA also applies to government health plans including the federal health care program for active duty military personnel and veterans.[68] Furthermore, HIPAA covers health care "clearinghouses" (processors of data created by another).[69] All entities subject to HIPAA must comply with complex, but somewhat toothless, regulations restricting the dissemination of electronically stored patient medical information.[70]

A recent amendment to HIPAA greatly increases the public consequences of a data breach by requiring that all health information breaches, including those by government health providers, be publicized if they involve more than 500 people.[71] The statute also directs the Secretary of Health and Human Services to maintain a website listing the firms responsible.[72] This represents a substantial change from the original HIPAA regime where covered entities had no duty to notify patients of breaches, but only to mitigate the harm.[73]

---

64. *Id.* at 150 (quoting South Carolina v. Baker, 485 U.S. 505, 514-15 (1988)).

65. *Id.* at 151.

66. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, § 261, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 29 U.S.C. and 42 U.S.C.).

67. *See* 42 U.S.C. § 1320d(3) (2006); 45 C.F.R. § 160.103 (2006).

68. *See* COVERED ENTITY CHARTS, HIPAA GENERAL INFORMATION 10, http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf. *But see* 45 C.F.R. § 164.512(k) (2009) (exemption for information uses or disclosures about members of the armed forces where "deemed necessary by military command authorities").

69. *See* 45 C.F.R. § 160.103 (2006) (defining a covered entity).

70. Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. pts. 160 & 164 (2007).

71. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13402, 123 Stat 115 (2009) (codified as amended at 42 U.S.C. § 17932 (2009)).

72. *Id.* at § 13402(e)(4).

73. *See* 42 U.S.C. §§ 1320d-1320d-8 (2006). *Cf.* Brandon Faulkner, *Hacking Into Data Breach Notification Laws*, 59 FLA. L. REV. 1097, 1116 (2007) (noting that pre-amendment "HIPAA does not require entities to notify individuals after unauthorized or wrongful disclosure of individually identifiable health information"); Nicolas P. Terry & Leslie P. Francis, *Ensur-*

There are also some laws specific to the federal government that do not apply to the states. Chief among the federal laws is the much-maligned Privacy Act of 1974,[74] (Privacy Act), which regulates the collection, maintenance, use, and dissemination of an individual's personal data by federal government agencies.[75] The Privacy Act requires:

> Each agency that maintains a system of records shall . . . establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.[76]

Critically, the Privacy Act creates a private right of action in federal district court whenever an agency "fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual."[77] A successful Privacy Act claim requires (1) that the information be a record contained in a system of records, (2) that it have been disclosed improperly, willfully and intentionally, and (3) that the disclosure has caused actual damages.[78]

---

ing the Privacy and Confidentiality of Electronic Health Records, 2007 U. ILL. L. REV. 681, 729 (2007) (noting that pre-amendment "HIPAA seems too weak; it requires simply that custodians of electronic health information keep records about access that patients can review on request. The difficulty is that patients may not know that their records have been accessed and thus may not request information about access.").

74. 5 U.S.C. § 552a (2006). For critique, see for example, Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1088, 1114 (2002), arguing that federal statutory protections have "fared poorly in cases involving information privacy on the Internet." *See also* Jonathan C. Bond, Note, *Defining Disclosure In A Digital Age: Updating The Privacy Act For The Twenty-First Century*, 76 GEO. WASH. L. REV. 1232, 1258-64 (2008) (proposing some interesting suggestions as to how to modernize the Privacy Act); Dennis J. McMahon, Comment, *The Future Of Privacy In A Unified National Health Information Infrastructure*, 38 SETON HALL L. REV. 787, 797 (2008) ("Perhaps the most glaring loophole in the Privacy Act is the 'Routine Use' exception. This exception allows federal agencies to disclose personal information if they determine that the disclosure is part of the routine use of information and it is compatible with the original purpose for collecting the information.").

75. In addition, the E-Government Act of 2002, 44 U.S.C. § 3501 (2006), requires agencies to prepare privacy impact statements before creating new searchable databases or collecting new types of personally identifiable information. *See also* OFFICE OF MGMT. & BUDGET, PUBL'N NO. M-03-22, GUIDANCE FOR IMPLEMENTING THE PRIVACY PROVISIONS OF THE E-GOVERNMENT ACT OF 2002, (2003), *available at* http://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html.

76. 5 U.S.C. § 552a(e)(10) (2006).

77. *Id.* § 552a(g)(1)(D).

78. *See* Doe v. Chao, 540 U.S. 614, 619-21 (2004) (interpreting 5 U.S.C. § 522a(g)(4)(A) (2006)).

The Privacy Act has some teeth, but not too many, when applied to government data breaches. The leading case is *Doe v. Chao*.[79] Doe sued the Department of Labor (DoL) for illegal disclosure of his Social Security Number (SSN), which he had voluntarily disclosed on a benefits application.[80] The DoL then distributed documents to third parties that identified Doe by his SSN.[81] Doe filed suit under the Privacy Act, relying on the civil remedy section of the statute, which reads:

> In any suit . . . in which the court determines the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual an amount equal to the sum of actual damages sustained by an individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000.[82]

Doe argued this meant he was entitled to at least $1,000 if he proved a Privacy Act violation.[83] The government replied that Doe needed to prove actual damages before recovery, and the Supreme Court, in an opinion by Justice Souter, agreed that a showing of "actual damages" was required for recovery.[84] The opinion left the definition of "actual damages" for another day.[85]

The Privacy Act applies to intentional disclosures by the government. It has yet to be successfully invoked to award damages when records were hacked or forcibly accessed, although the recent decision in *American Federation of Government Employees v. Hawley* shows how this might change.[86] *Hawley* concerned the theft of a laptop hard drive containing personnel data for 100,000 Transportation Security Administration (TSA) employees, including SSNs, birth dates, payroll information, bank account numbers, and routing numbers.[87] The court explicitly addressed the issue of whether the government's actions amounted to intentional and willful conduct.[88] Given that the plaintiffs alleged that the TSA had been repeatedly warned about fundamental deficiencies in its security, the court ruled that there was sufficient evidence to suggest that the TSA knew of the risk of a data breach, but inten-

79. *Id.*
80. *Id.* at 616-17.
81. *Id.* at 617.
82. *Id.* at 619 (citing 5 U.S.C. § 552a(g)(4) (2006)).
83. *Id.* at 620.
84. *See id.* at 627.
85. *See id.* at 627 n.12.
86. 543 F. Supp. 2d 44 (D.D.C. 2008).
87. *Id.* at 45.
88. *Id.* at 51-52.

tionally and willfully ignored it, which sufficed for plaintiffs to survive summary judgment.[89] Thus, the District Court held that TSA employees, alleging that the agency had negligently lost control of their personal data by failing to establish safeguards to prevent the loss of hard drives, could state a claim for "embarrassment, inconvenience, mental distress, concern for identity theft, concern for damage to credit report, concern for damage to financial suitability requirements in employment, and future substantial financial harm, [and] mental distress due to the possibility of security breach at airports."[90] Central to this holding was the District of Columbia Circuit rule that emotional trauma alone suffices to state a claim of an "adverse effect" under section 552a(g)(1)(D) of the Privacy Act.[91] Even so, the trial court in *Hawley* noted that whether such injuries qualified as "actual damages," under the standard set in *Doe v. Chao*, remained uncertain.[92]

This preliminary ruling was enough to motivate the TSA to settle the plaintiffs' claim for twenty million dollars,[93] which means that no ruling on the merits of the Privacy Act claims arising from unintentional record disclosure will be forthcoming. And thus the definition of what amounts to "actual damages" under the Privacy Act remains unsettled.

D. DIFFERENT INCENTIVE STRUCTURE

The legal regime regulating government breaches matters because there is some reason to suspect that economic incentives work less well in the public sector than they do in the private sector. Economic theory suggests that firms should respond to financial carrots and sticks. A regulatory regime that requires costly breach notifications, or imposes actual fines, creates an incentive to act in a manner that minimizes the expected total cost of prevention and cure.[94] Firms are also presumed to be sensitive to secondary effects that might reduce their profits, such as bad publicity. State laws requiring breach notices rely on both of these tendencies for their effectiveness: Firms will find that providing the notices costs money and creates bad publicity. Lawsuits, or measures designed to preempt lawsuits, e.g. by offering discount

89. *Id.*

90. *Id.* at 50-51.

91. *Id.* at 51 n.12 (citing Krieger v. U.S. Dep't of Justice, 529 F. Supp. 2d 29, 53 (D.D.C. 2008) (quoting Albright v. United States, 732 F.2d 181, 186 (D.C. Cir. 1984)).

92. *Id.* at 53 (citing Doe v. Chao, 540 U.S. 614, 624-25 (2004)). *Cf.* Jacobs v. Nat'l Drug Intelligence Ctr., 548 F. 3d 375, 377 (5th Cir. 2008) (noting trend towards allowing emotional injuries to qualify as "actual damage" under Privacy Act).

93. Terry Frieden, *VA Will Pay $20 Million to Settle Lawsuit Over Stolen Laptop's Data,* CNN, Jan. 27, 2009, http://www.cnn.com/2009/POLITICS/01/27/va.data.theft/?iref=mpstoryview.

94. For an attempt to put this into practice, see SHOSTACK & STEWART, *supra* note 2.

coupons or free credit monitoring, and responding to customer concerns and complaints, costs more still. It is arguable whether the people in firms who make decisions about information technology (IT) practices have a sufficient financial incentive via stock options or bonuses to be directly concerned about a breach's effect on the company's stock price or profitability, but it is possible that their bosses might. And in any case, being responsible for a well-publicized data breach disaster cannot be career-enhancing.

In contrast, governments and government employees are not especially sensitive to the profit motive. Many civil servants enjoy substantial security of tenure. They shelter not just behind the government's sovereign immunity, but also qualified immunity for many job-related tasks.[95] Government employees are rarely eligible for much in the way of bonuses, although their promotion prospects may be affected by their performance.[96] Economic theory suggests that financial incentives applied to the government organization—be they fines or a requirement to spend money on mitigation—are far less likely to be transmitted to the employee level. Remedies that might be more likely to work, such as dismissing persons whose negligence causes a data breach, are somewhat Draconian, and not obviously effective either.[97] On the other hand, given how easy it has become to encrypt sensitive data, leaving sensitive data unencrypted and then losing control of it may amount to the sort of gross negligence that deserves a strong remedy.

Even if graduated economic incentives are not likely to be very potent, there are other incentives that are more likely to be effective: civil servants and the very large majority of their elected political superiors are acutely sensitive to bad publicity. And news of data breaches, especially those resulting

95. Herring v. Keenan, 218 F.3d 1171, 1178-81 (10th Cir. 2000) (holding that qualified immunity barred otherwise valid *Bivens* action against probation officer as constitutionally based information privacy right against disclosure of HIV status to relatives was not clearly established at time disclosure was made); Helen L. Gilbert, Comment, *Minors' Constitutional Right to Informational Privacy*, 74 U. CHI. L. REV. 1375, 1385 (2007) (stating that "[Q]ualified immunity frequently bars damage awards for plaintiffs because of the ambiguous scope of informational privacy protections.").

96. *See* STEWARD LIFF, MANAGING GOVERNMENT EMPLOYEES 100, 124-25 (2007); PAUL C. LIGHT, A GOVERNMENT ILL EXECUTED: THE DECLINE OF THE FEDERAL SERVICE AND HOW TO REVERSE IT 226, 234 (2008) (noting the unusual nature of Departments of Defense and Homeland Security pay-for-performance system).

97. The UK government has a history of firing officials responsible for leaving secret documents on trains and taxis, but this zero-tolerance policy has not proved particularly effective. *See*, *e.g.*, *Intelligence Official Suspended over al-Qaeda File Left on Train*, TIMES (UK), June 12, 2008, http://www.timesonline.co.uk/tol/news/uk/article 4115588.ece; *More Secret Government Documents Left on Train*, DAILY TELEGRAPH, June 14, 2008, http://www.telegraph.co.uk/news/uknews/2131236/More-secret-government-documents-left-on-train.html; *Second Spy Loses Laptop*, THE REGISTER, March 28, 2000, http://www.theregister.co.uk/2000/03/28/second_spy_loses_laptop/.

from some form of negligence, make for extremely bad publicity.

E. FEDERAL BEST PRACTICES (STATE PATCHWORK)

As governments make the rules to which they themselves are subject, it can be difficult to institutionalize regimes that require governments to create bad publicity for themselves. But, as demonstrated by the HIPAA amendments in the recent economic stimulus bill, it is not impossible.[98] Progress is indeed possible, although we are starting from a relatively low baseline.

In June 2007, the U.S. Government Accountability Office (GAO) identified significant weaknesses in all information security controls protecting federal information systems,[99] and charged that most agencies had not implemented controls to sufficiently prevent, limit, or detect access to computer networks.[100] The GAO broke the weaknesses into five major categories: (1) access controls, which ensure that only authorized individuals can read, alter and delete data; (2) configuration management controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which provides for the prevention of significant disruptions of computer dependent operations; and (5) agency wide information security programs, which provide the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.[101] According to the GAO, data losses are preventable through the implementation of adequate access controls, such as passwords, access, privileges, encryption and audit logs.[102] But because most agencies did not routinely implement these techniques, federal information system controls suffered from persistent weaknesses.[103]

Even before the GAO issued its 2007 indictment, however, the federal government had begun to make significant progress, at least on paper, in the prevention of data breaches, although not so much on compensation and cure.[104] The Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide security for the information systems that support the operations and assets of the agency, including those provided or managed by

98. *See supra* text accompanying notes 71-73.
99. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 40, at 10.
100. *Id.* at 2.
101. *Id.* at 10.
102. *Id.* at 11.
103. *Id.* at 11-12, 14.
104. *See infra* text following note 117.

another agency, contractor, or other source.[105] The federal government has begun to take this duty more seriously over the past three years, in large part due to prodding from the Office of Management and Budget (OMB). OMB is responsible for establishing government-wide policies and for providing guidance to agencies on how to implement the provisions of FISMA, the Privacy Act, and other federal information security and privacy laws.[106] Under FISMA, and even more so under the OMB's guidance, agencies are required to do cost-benefit analyses, and to provide security "commensurate with the risk and magnitude of the harm" resulting from possible data breaches and other security risks.[107]

Much remains to be done. According to the 2008 ITRC report, "only 2.4% of all breaches had encryption or other strong protection methods in use. Only 8.5% of reported breaches had password protection. It is obvious that the bulk of breached data was unprotected by either encryption or even passwords."[108] This was so despite a 2006 OMB directive requiring agencies to encrypt and otherwise protect personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter:

> 1. Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing;
>
> 2. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
>
> 3. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
>
> 4. Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive da-

105. Federal Information Security Management Act, 44 U.S.C. § 3544(b) (2006).

106. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, INFORMATION SECURITY: PROTECTING PERSONALLY IDENTIFIABLE INFORMATION, GAO 08-343, at 13 (Jan. 2008), *available at* http://www.gao.gov/new.items/d08343.pdf.

107. 44 U.S.C. § 3544(a)(1)-(2) (2006).

108. Identity Theft Resource Center, 2008 *Breach Total Soars* (Jan. 6, 2009), http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml. The ITRC aggregated breaches from the public and private sectors, so it is conceivable that the government-only statistics would be somewhat better, but because the public sector (government and much of what ITRC calls "education") represented about half of the sample set the numbers in the text are likely to be representative of the government's performance.

ta has been erased within 90 days or its use is still required.[109]

These appear to be sensible requirements, but it has taken time to get the federal bureaucracy to adhere to them.[110]

As of 2007, every federal agency has been required to create a "breach notification policy."[111] For example, the U.S. Equal Employment Opportunity Commission's (EEOC) policy includes a number of useful prophylactic measures, such as the removal of SSNs from the electronic records of people who file employment discrimination charges.[112] It also requires an annual internal review of "the current holdings of all personally identifiable information and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely and complete and reduce them to the minimum necessary for the proper performance of the agency function."[113] And the agency pledges to include these reviews in its annual FISMA report.[114]

Regarding breaches, the EEOC policy reiterates the OMB rule that any breach must be reported to the U.S. Computer Emergency Readiness Team (US-CERT) within an hour of discovery. Public notification moves less quickly. The OMB requires only that the victims be notified "without unreasonable delay" and "consistent with the needs of law enforcement and national security and any measures necessary for your agency to determine the scope of the breach."[115] The OMB rule gives agency heads, or their designates in writing, the authority to delay notification but cautions that "delay should not exacerbate risk or harm to any affected individual(s)."[116]

Even worse, and echoing the OMB's general silence on the subject, the EEOC's compensation menu is rather meager: the agency will decide if credit monitoring will be offered for affected individuals.[117] There are no provisions

---

109. Memorandum from Clay Johnson III, Deputy Dir. for Mgmt., OFFICE OF MGMT. & BUDGET, ON PROTECTION OF SENSITIVE AGENCY INFORMATION, M-06-16, at 1 (Jun. 23, 2006), *available at* http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf.

110. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 106, at 1-4.

111. Memorandum from Clay Johnson III, Deputy Dir. For Mgmt., OFFICE OF MGMT. & BUDGET, ON SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION, M-07-16, at 1 (May 22, 2007), *available at* http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2007/m07-16.pdf (requiring all agencies to "to develop and implement a breach notification policy **within 120 days**") (bold and underlining in original) [hereinafter Johnson Memorandum].

112. The U.S. Equal Employment Opportunity Commission, Breach Notification Policy, http://www.eeoc.gov/breach/breach_notification_policy.html (last modified Sept. 25, 2007) [hereinafter EEOC Notification Policy].

113. *Id.* § 2.

114. *Id.*

115. Johnson Memorandum, *supra* note 111, at 16.

116. *Id.*

117. EEOC Notification Policy, *supra* note 112, at § III(B) ("If the breach includes social

for additional compensation. The closest thing to a compensation requirement in the federal administrative breach regime is the suggestion, which lacks force of law, in the President's Identity Theft Task Force's Strategic Plan, issued April 2007, that criminal laws be amended to ensure restitution for the value of time spent coping with identity theft.[118]

In a January 2008 report, the GAO testified that while there were improvements in information security, not all agencies had followed the OMB guidance.[119] The GAO also found that this gap in the various agencies' policies and procedures reduced the ability to protect personally identifiable information from improper disclosure.[120] There is still substantial variation in agency policies and procedures on information security. Until best practices become more standardized, data breaches from federal government databases, not to mention the states, will continue. As a result, the question of appropriate remedies will not go away.

III. NEW LEGAL REMEDIES AND OLD STUMBLING BLOCKS

Publicity helps mitigate the harms caused by breaches of personal data by putting victims and potential victims on notice that they are at risk. But notice alone is far from full mitigation, much less compensation, for the harms caused by a data breach. Currently, only the Privacy Act offers victims of a federal data breach any reasonable hope of compensation. State laws vary, but to the extent that states have allowed themselves to be sued, the would-be plaintiff will often need to characterize the harm as a tort, or a violation of state law.

This Part begins with a review of the constitutional basis for a right of information privacy. I argue below that there is a constitutional right, either free-standing or based in Due Process, limiting the government's ability to disclose personal data lawfully acquired under legal compulsion, at least in cases where the government failed to take reasonable precautions. This right is separate from any informational privacy rights that constrain the government's ability to acquire personal or corporate information.

---

security numbers or other highly sensitive information, the Core Management Group will determine whether credit-monitoring services will be offered to the affected parties at government expense.").

118. PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN 50 (2007), *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf.

119. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 106, at 4.

120. *Id.* at 19 ("Agencies' implementation of OMB's guidance on personally identifiable information . . . will be essential in improving the protection of personally identifiable information.").

The key holding is *DeShaney*, which sets out a distinction between cases where the government is not liable because private parties retain freedom of action, and those where the government is liable because the government has, in effect, occupied the field.[121] In the case of government data breaches, the government has taken full control of the data; under the *DeShaney* distinction, the government is responsible when it mis-handles the data. If this is correct, then victims of many privacy breaches have a claim under section 1983 against states. Unfortunately, similar constitutional claims against the federal government would require a *Bivens* action, and the Supreme Court has narrowed *Bivens* to a point that makes the federal version unlikely to succeed.[122] As a result, persons injured by federal data breaches will have substantially inferior remedies available to them. Even where claims are possible, however, plaintiffs will need to surmount a valuation problem caused by a judicial suspicion of probabilistic harms—possible harms that may not occur but nonetheless warrant preventive action.

A. CONSTITUTIONAL THEORIES

1. Constitutional Privacy Rights Against Government Disclosure of Private Facts

The Supreme Court's major modern discussion of an informational privacy right remains *Whalen v. Roe*.[123] In *Whalen*, the Court accepted that the right to privacy includes a general "right to be let alone,"[124] which includes "the individual interest in avoiding disclosure of personal matters."[125] Despite finding a theoretical right to avoid disclosure of intimate personal matters in *Whalen*, the Court upheld a New York State statute which required that doctors provide the state with a copy of every prescription for certain drugs, and disclose the names of the patients to whom they were prescribed.[126] These data would be entered into a computerized list.[127] The decision claimed to balance the social interest in informational privacy against the state's "vital

121. 489 U.S. 189, 200 (1989).

122. *See infra* Section III.B.2.

123. 429 U.S. 589 (1977). For an interesting critique suggesting that *Whalen's* intellectual influence has largely been maligned, see Jonathon W. Penney, *Privacy and the New Virtualism*, 10 YALE J.L. & TECH. 194, 210-14 (2007-2008).

124. 429 U.S. at 599 (citing Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)).

125. 429 U.S. at 598-99 (acknowledging the existence of the right, but finding that it could be overcome by a narrowly-tailored program designed to serve the state's "vital interest in controlling the distribution of dangerous [prescription] drugs").

126. *Id.* at 603-04.

127. *Id.* at 593, 603-04.

interest in controlling the distribution of dangerous drugs."[128] Finding New York's program to be narrowly tailored, and replete with security provisions designed to reduce the danger of unauthorized disclosure, the Supreme Court held that the statute was constitutional.[129] The Court allowed the mandatory compilation and disclosure of prescription data, but it left the door open to future restrictions in light of technical change, noting that it was "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal data in computerized data banks or other massive government files."[130] In so doing, the Court set the stage for claims that the Constitution embodies a right to informational privacy.[131]

Indeed, lower courts have interpreted *Whalen* this way.[132] Several courts have found a violation of a constitutional privacy right in the public disclosure of private medical information.[133] Ohio recognized a constitutional right

---

128. *Id.* at 598.

129. *Id.* at 601-04.

130. *Id.* at 605.

131. *See, e.g.*, Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133, 155, 158 (1991) (concluding that because most theories of personhood assume personal information is a crucial part of a person's identity, there should be a recognized right to informational privacy based on personhood and that since information is property, it should be protected by the Fifth Amendment); Gary R. Clouse, Note, *The Constitutional Right to Withhold Private Information*, 77 NW. U. L. REV. 536, 541-47 (1982) (tracing the development of the right to informational privacy, and noting the Supreme Court's use of a balancing test in *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425 (1977), to determine whether an individual's constitutional rights have been infringed by a government-mandated disclosure of information); Gilbert, *supra* note 95, at 1381-88 (surveying cases in the courts of appeal that apply *Whalen's* informational privacy right).

132. For example, cases following on from *Whalen* include: *Tucson Woman's Clinic v. Eden*, 379 F.3d 531, 551 (9th Cir. 2004) (holding that a statutory provision enabling the state to access abortion clinic patients' medical records violated patients' right to informational privacy); *Cooksey v. Boyer*, 289 F.3d 513, 515-16 (8th Cir. 2002) (overturning district court grant of summary judgment and noting that disclosure of personal information might violate the right to privacy); *Powell v. Schriver*, 175 F.3d 107, 111-112 (2d Cir. 1999) (holding that a transsexual inmate had a privacy right of confidentiality in medical records); *Flanagan v. Munger*, 890 F.2d 1557, 1570 (10th Cir. 1989) ("The Supreme Court has recognized that the constitutional right to privacy protects an individual's interest in preventing disclosure by the government of personal matters."); *Eastwood v. Department of Corrections of Oklahoma*, 846 F.2d 627, 630-31 (10th Cir. 1988) ("[A variety of provisions in the Bill of Rights] protects two kinds of privacy interests: the individual's interest in avoiding disclosure of personal matters and the interest in being independent when making certain kinds of personal decisions."); *Mangels v. Pena*, 789 F.2d 836, 839 (10th Cir. 1986) ("Due process thus implies an assurance of confidentiality with respect to certain forms of personal information possessed by the state."); *Taylor v. Best*, 746 F.2d 220, 225 (4th Cir. 1984) (recognizing that the right to privacy includes avoiding disclosure of personal facts); *Slayton v. Willingham*, 726 F.2d 631, 635 (10th Cir. 1984) (holding that the Supreme Court explicitly recognized the constitutional right to privacy in *Whalen v. Roe*).

133. *See, e.g.*, *In re* Doe v. City of New York, 15 F.3d 264, 267 (2d Cir. 1994) (HIV status

of privacy in Social Security Numbers.[134] And the Fifth Circuit found a right against disclosure of "the most private details of [a plaintiff's] life" that had been revealed to state investigators who represented that testimony was absolutely privileged under Florida law and that the contents of his testimony would be revealed to no one.[135] On the other hand, the Sixth Circuit refused to include informational privacy among constitutionally protected interests.[136]

Whalen is more significant for what it foreshadowed than for what it held. Yes, the plaintiff lost: his privacy interest was not strong enough to outweigh the state's interest in drug laws. But because *Whalen*'s plaintiff lost on a balancing test rather than for failing to state a claim, the *Whalen* decision established the principle that there could be an actionable constitutional right to information privacy. Presumably, with the right facts, and perhaps relying on the technical change the Court foresaw in *Whalen*, a claim that the Fourteenth Amendment's protection of privacy included a right to the "nondisclosure of private information"[137] might succeed.

The right to information privacy first enunciated in *Whalen* can be characterized as a component of substantive Due Process,[138] but it is perhaps best understood as a free-standing constitutional right. The *Whalen* court itself was somewhat unclear on the issue, but a series of footnotes suggest that it draws on several parts of the Constitution.[139] Starting with *Griswold v. Connecticut*,[140] and running through *Roe v. Wade*[141] and *Planned Parenthood v. Casey,*[142] the Supreme Court has characterized the broader constitutional right to decisional privacy as having multiple sources, one of which is substantive Due Process. The two privacy rights—informational (*Whalen*) and decisional (*Roe* and *Ca-*

---

disclosure); Doe v. Attorney General of the U.S., 941 F.2d 780, 795-96 (9th Cir. 1991) (collecting cases); Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990) (recognizing right to informational privacy for information related to an individual's fundamental rights and "[p]ersonal, private information in which an individual has a reasonable expectation of confidentiality").

134. *See* State *ex rel.* Beacon Journal Publ'g Co. v. City of Akron, 640 N.E.2d 164, 169 (Ohio 1994) (relying in part on section 7 of the Privacy Act).

135. Fadjo v. Coon, 633 F.2d 1172, 1175-76 (5th Cir. 1981).

136. *See* Lambert v. Hartman, 517 F.3d 433, 445 (6th Cir. 2008) (driver whose identity was stolen as result of clerk of court's publication of her Social Security Number on public website did not have a constitutionally protectable fundamental property interest in her personal information that might serve as basis for substantive Due Process claim); J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981) (compilation and dissemination of social histories prepared by state probation authorities in connection with proceedings involving juveniles).

137. Whalen v. Roe, 429 U.S. 589, 600 (1977).

138. *DeSanti*, 653 F.2d at 1088-89 (tying *Whalen* to substantive Due Process).

139. *See Whalen*, 429 U.S. at 600 nn.23-25.

140. 381 U.S. 479 (1965).

141. 410 U.S. 113 (1973).

142. 505 U.S. 833 (1992).

sey)—are not the same, but they are often conflated;[143] to the extent they are further conflated, the informational privacy right may come to be understood as part of Due Process rather than a free-standing right. Indeed, a number of circuits seem to see it that way.[144]

Supreme Court decisions following *Whalen* appear to agree that there is or ought to be a zone of constitutionally protected informational privacy, even if the Court has yet to encounter data that is entitled to remain in that zone. In *Nixon v. Administrator of General Services*, the Court applied *Whalen*'s balancing test to reject President Nixon's claim that allowing government archivists to review and classify his presidential papers and effects violated his "fundamental rights . . . of . . . privacy."[145] Nixon's privacy interest was found insufficiently strong to outweigh the public interest in preserving his papers.[146] Similarly in both *Cox Broadcasting Corp. v. Cohn*[147] and *Florida Star v. B.J.F.*,[148] the Court struck down state law privacy claims arising from the accurate publication of arguably private facts that had become matters of public record. But in so doing, the Court did suggest that "there is a zone of privacy surrounding every individual,"[149] even if did not say where that zone was or what might occupy it.

---

143. *See, e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 530 (2006) (stating that "[*Whalen*] recognized that the 'right of privacy' [was] based on substantive due process").

144. *E.g.*, Kallstrom v. City of Columbus, 136 F.3d 1055, 1064 (6th Cir. 1998) ("Where state action infringes upon a fundamental right, such action will be upheld under the substantive due process component of the Fourteenth Amendment only where the governmental action furthers a compelling state interest, and is narrowly drawn to further that state interest."); Lyle v. Dedeaux, No. 94-60200, 1994 WL 612506, at *6 (5th Cir. Oct. 24, 1994) (Table case 39 F.3d 320) (holding a disclosure of personal information does not violate a person's right to privacy unless the person's legitimate expectation of privacy outweighs a legitimate state need for the information); Kelly v. City of Sterling Heights, No. 90-1895, 1991 WL 207548, at *2 (6th Cir. Oct. 16, 1991) (Table case 946 F.2d 895) ("A privacy interest is not constitutionally protected unless it relates to sensitive, personal, and private information which warrants confidentiality."); Flanagan v. Munger, 890 F.2d 1557, 1570 (10th Cir. 1989) ("The Supreme Court has recognized that the constitutional right to privacy protects an individual's interest in preventing disclosure by the government of personal matters."); Mangels v. Pena, 789 F.2d 836, 839 (10th Cir. 1986) ("Due process thus implies an assurance of confidentiality with respect to certain forms of personal information possessed by the state. Disclosure of such information must advance a compelling state interest which, in addition, must be accomplished in the least intrusive manner.").

145. 433 U.S. 425, 455-57 (1977).

146. *Id.* at 465.

147. 420 U.S. 469, 495-97 (1975).

148. 491 U.S. 524, 540-41 (1989) (concerning name of rape victim erroneously posted by the police, then published by a newspaper in violation of a Florida statute that made it unlawful to report the name of a victim of a sexual offense).

149. *Cohn*, 420 U.S. at 487.

Also relevant is the unanimous decision in *United States Department of Justice v. Reporters Committee for Freedom of the Press*, in which the Supreme Court held that there was a heightened privacy interest sufficient to overcome an FOIA application in an FBI compilation of otherwise public information.[150] Even if the data contained in a "rap sheet" were located in scattered courthouses as public records, the compilation itself, the "computerized summary located in a single clearinghouse," was not available to the public.[151]

> Because events summarized in a rap-sheet have been previously disclosed to the public, respondents contend that Medico's privacy interest in avoiding disclosure of a federal compilation of these events approaches zero. We reject respondents' cramped notion of personal privacy. To begin with, both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person. In an organized society, there are few facts that are not at one time or another divulged to another. Thus, the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private.[152]

Reporters Committee is obviously not a constitutional decision as it merely interpreted a FOIA exception, but it does suggest that, even in 1989, the Court understood that databases can have privacy consequences.

Subsequent Supreme Court cases touching on informational privacy have not changed the basic contours set up by these fundamental cases, although they have filled in some of the details.[153] In the course of upholding a federal

---

150. 489 U.S. 749, 780 (1989).

151. *Id.* at 764.

152. *Id.* at 764-65.

153. In *Bartnicki v. Vopper*, the Court held that privacy claims must give way to the First Amendment "interest in publishing matters of public importance." 532 U.S. 514, 534 (2001). Both *Whalen* and *Bartnicki* are opinions by Justice Stevens, and there is nothing in the 2001 opinion to suggest any retreat from *Whalen*'s 1977 formulation, although *Whalen* is not cited. Justice Stevens did note,

> It seems to us that there are important interests to be considered on *both* sides of the constitutional calculus. In considering that balance, we acknowledge that some intrusions on privacy are more offensive than others, and that the disclosure of the contents of a private conversation can be an even greater intrusion on privacy than the interception itself. As a result, there is a valid independent justification for prohibiting such disclosures by persons who lawfully obtained access to the contents of an illegally intercepted message, even if that prohibition does not play a significant role in preventing such interceptions from occurring in the first place.

statute protecting private information, *Reno v. Condon* treated the regulation of state driver's license databases much like the regulation of ordinary property.[154] *Whalen*'s holding that data privacy is a value of constitutional import endures, albeit in a somewhat latent form as the right is still waiting for its first triumph over countervailing factors in the Supreme Court. As noted above, however, several Circuit Courts have clearly stated that *Whalen* creates a constitutional right to privacy, one that can determine outcomes.[155]

2. The Substantive Due Process Aspect of the Right

A person or firm whose data has been exposed by the government has suffered a compensable deprivation of life, liberty, or property without Due Process of law if the government took on an obligation to keep the data confidential.[156] How to characterize that doctrinally, and in precisely which circumstances current doctrine may permit a remedy, are surprisingly complex questions for what should, morally, be a fairly simple matter. The government may have taken the information by force of law, or because it is the only game in town. The government's promise to safeguard the information may be statutory, regulatory, or in some cases implicit.[157] But if the failure to safeguard the data was negligent or lacked of elementary due care, as opposed to the result of the intervention of a criminal so accomplished that his actions could not reasonably be foreseen, then the government should make restitution.

Begin with a relatively simple case: Suppose that the data in question

---

Id. at 533.

154. Reno v. Condon, 528 U.S. 141, 148 (2000) ("Because drivers' information is, in this context, an article of commerce, its sale or release into the interstate stream of business is sufficient to support congressional regulation.").

155. *See supra* text accompanying notes 132-135.

156. One example is the disclosure of a SSN. The Social Security Act, which requires the use of SSNs for disbursement of benefits, declares that SSNs obtained or maintained by authorized individuals on or after October 1, 1990, are confidential and prohibits their disclosure. 42 U.S.C. § 405(c)(2)(C)(viii)(I) (2006). It is common to speak of a person "owning" their SSN. *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, USE OF THE SOCIAL SECURITY NUMBER IS WIDESPREAD, GAO/T-HEHS-00-111, at 3 (May 9, 2000), *available at* http://www.gao.gov/new.items/he00111t.pdf.

157. A survey of how the government makes binding confidentially promises is beyond the scope of this essay. As a general matter, an oral or even written representation by a government official in many cases will not suffice since it is hornbook law that an official without authority to make a binding representation cannot estop the government. *See* Office of Pers. Mgmt. v. Richmond, 496 U.S. 414, 419-20 (1990). I would argue, however, that a representation by an authorized person would suffice, as would promises made in certain special circumstances such as plea bargaining. *See* Fadjo v. Coon, 633 F.2d 1172, 1175-76 (5th Cir. 1981) (finding right against disclosure of facts being revealed to state investigators after representation that testimony would be revealed to no one).

clearly belonged to the data subject. The subject disclosed it to the government either because it was required or because it was a necessary condition precedent to a government license or benefit.[158] Assume further that a government employee loses a copy of the data by failing to exercise basic care: perhaps a computer was left unsecured, data was accidentally posted to a public web site, or an employee lost control of an unencrypted USB drive. Note that these hypotheticals have a common feature: they don't involve a hacker, much less a movie-quality hacker, or über-criminal.[159] Indeed, they involve great negligence, and perhaps in some cases, gross negligence. As described below, Due Process may not protect the public against theft of data entrusted to the government when the theft is carried out by unusually skilled hackers. The Due Process Clause requires that the government exercise only due care, not perfect care. And even when the government has been only negligent, recovery may be difficult.

The disclosure of private information has a negative impact on the owner or subject of the data. In some cases the data breach threatens to reduce, perhaps to zero, the value of the formerly secret data, destroying much or all of the value of an information asset such as a trade secret. Alternately, the damage could be purely due to secondary effects, such as actual or potential identity theft. In these cases, the data itself is not necessarily reduced in value, but rather the person who acquires it gains the power to cause harm.[160] In either case, there is actual or probabilistic harm.

A harm is probabilistic if it is unknown whether it will occur, or how severe it will be. At the time the government discovers it has lost control over the data, neither it nor the subject may know whether the data has in fact been acquired by anyone else. That a laptop has been lost does not mean it will be found by a malicious third party. That a USB drive is returned by a seemingly good Samaritan does not exclude the possibility that the contents were copied before their return. That data was put on a public website viewed by several dozen people does not tell us whether the people had any

158. The data might, for example, be information attached to a tax return, an EEOC complaint, or personal data disclosed by a probationer or by a government employee, or a trade secret disclosed pursuant to the Federal Insecticide, Fungicide, and Rodenticide Act. The Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) requires manufacturers seeking government registration of pesticides to disclose health, safety, and environmental data to the Environmental Protection Agency. *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1007 (1984) (characterizing disclosures as voluntary).

159. On the dangers of focusing on this unrealistic case, see generally Paul Ohm, *The Myth of the Super-User: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327 (2008).

160. This can be a complex issue. Sometimes the data will have no intrinsic value (e.g. a password) or sometimes its value will be unchanged (e.g. the number of a bank account), but the disclosure will nonetheless be harmful.

interest in it or if they copied the data. Yet, even in cases where the release only creates a *risk* of harm, the subject must expend resources on monitoring and prevention so long as the expected value of the risk is sufficiently great to justify the expense.[161]

The key case in establishing the contours of the Due Process right to compensation for certain government data breaches is Chief Justice Rehnquist's opinion in *DeShaney*.[162] Chief Justice Rehnquist is an unexpected source for a major information privacy right, and *DeShaney* is a particularly unexpected locus for its elucidation. *DeShaney* is notorious as an opinion in which the Supreme Court held that the state of Wisconsin had no duty under the Constitution to protect a boy, the infamous "poor Joshua" of Justice Blackmun's dissent,[163] from a permanently disabling beating by his father.[164] The absence of a duty was controversial because the state social services were on actual notice that Joshua had been repeatedly injured and was at risk.[165] In finding that the Due Process clause imposed no duty of care on state social services regarding children residing with a parent, at least absent a statutory or regulatory undertaking to protect children from their parents, Chief Justice Rehnquist distinguished Joshua's case from one where a duty would have existed. Mere notice was not enough; the state would have had a duty only if it had placed Joshua in circumstances where it "renders him unable to care for himself, and at the same time fails to provide for his basic human needs . . . ."[166] The duty arises "from the limitation which it has imposed on his freedom to act on his own behalf" not "its failure to act to protect his liberty interests against harms inflicted by other means."[167] Chief Justice Rehnquist

161. On the valuation issue, see *infra* Section III.C.

162. 489 U.S. 189 (1989). I am grateful to Patrick Gudridge for pointing out the centrality of *DeShaney* in this context.

163. *Id.* at 213 (Blackmun, J., dissenting).

164. *Id.* at 191.

165. *See id.* at 192-93.

166. *Id.* at 200.

167. *Id.* The full quotation is:

> [W]hen the State by the affirmative exercise of its power so restrains an individual's liberty that it renders him unable to care for himself, and at the same time fails to provide for his basic human needs—*e.g.,* food, clothing, shelter, medical care, and reasonable safety—it transgresses the substantive limits on state action set by the Eighth Amendment and the Due Process Clause. The affirmative duty to protect arises not from the State's knowledge of the individual's predicament or from its expressions of intent to help him, but from the limitation which it has imposed on his freedom to act on his own behalf. In the substantive due process analysis, it is the State's affirmative act of restraining the individual's freedom to act on his own behalf-through incarceration, institutionalization, or other similar restraint of personal liberty-which is the "deprivation of liberty"

immediately added in a footnote that, "[e]ven in this situation, we have recognized that the State 'has considerable discretion in determining the nature and scope of its responsibilities.'"[168]

When the State takes a person's data and holds it in a fashion outside the person's control, the State has done to that data exactly what Chief Justice Rehnquist said was necessary to trigger Due Process Clause protection: it has "by the affirmative exercise of its power" taken the data and "so restrain[ed]" it that the original owner is unable to exert any control whatsoever over how the government stores or secures it.[169] The government's "affirmative duty to protect" the data "arises . . . from the limitation which it has imposed on his freedom to act on his own behalf" to keep the data secure.[170] Again, "it is the State's affirmative act of restraining the individual's freedom to act on his own behalf" which creates a duty on the government to keep the data secure.[171] The State created the danger, and thus the State is responsible for the outcome.[172]

One might object that the *DeShaney* holding stands for the proposition that when the government stands by and lets another do harm to a person, that person has no recourse unless the government has taken on an affirmative duty to protect. In this view, exposing private data on the web or losing an unencrypted database is not the harm. Rather, the harm comes from a third party's use of the data, something for which this reading of *DeShaney* says the government should not be blamed. But this is a misreading of *DeShaney* because the analogy is incorrect. In *DeShaney*, the State had no duty because it had never taken Joshua into care.[173] The harms he suffered at his father's hands were private wrongs, a direct transaction in which the government had no part.[174] The Chief Justice characterized the State as an absent party:

> The most that can be said of the state functionaries in this case is that they stood by and did nothing when suspicious circumstances dictated a more active role for them. In defense of them it must al-

---

> triggering the protections of the Due Process Clause, not its failure to act to protect his liberty interests against harms inflicted by other means.

Id. (citations omitted).

168. *Id.* at 200 n.7.

169. *See id.* at 200.

170. *See id.*

171. *See id.*

172. *Cf.* Michele H. Berger, Comment, *Negligence Or State-Created Danger: Two Avenues For Injured Student Informants Pursuing School Liability*, 30 U. LA VERNE L. REV. 94, 96-104 (2008) (discussing effects of "state-created danger doctrine" in the context of schools).

173. *See DeShaney*, 489 U.S. at 199-200.

174. *See id.* at 201.

> so be said that had they moved too soon to take custody of the son away from the father, they would likely have been met with charges of improperly intruding into the parent-child relationship, charges based on the same Due Process Clause that forms the basis for the present charge of failure to provide adequate protection.[175]

Indeed, it was the claim that the government had a duty to intervene which was the heart of the plaintiff's case, and which the majority rejected.[176]

Contrast this to a hypothetical lost database: there is no question that the government had taken full control of the data before it lost them. Once the government takes that control, the subject of the data is completely disempowered with regards to how the data will be protected. Therefore, it is nonsensical to suggest that when the government negligently allows a third party to access the data, that third party is the only relevant actor for Due Process purposes. The government remains the critical intermediary, the one actually responsible for allowing the loss. In the case of information controlled by the government, it is not a bystander, but rather a direct agent. The government's active role in controlling the data, one that displaces the subject or owner of the data, is what creates the duty of care. Or as the Seventh Circuit stated, "The state must protect those it throws into snake pits, but the state need not guarantee that the volunteer snake charmer will not be bitten."[177]

The relevant law here is substantive, not procedural, Due Process. Interestingly, however, the answer would be about the same under a procedural Due Process standard. Procedural Due Process is not a fixed quantum but a sliding scale, one that alters with the circumstances. The leading case on how much process is due remains *Mathews v. Eldridge*.[178] Although it was originally a property-rights test, a plurality of the Supreme Court recently applied the *Mathews* test to a liberty interest in *Hamdi v. Rumsfeld*.[179] The plurality used *Mathews* to set up a three-part balancing test: weighing "the private interest that will be affected by the official action" against the Government's asserted interest, "including the function involved" and the burdens the Government would face in providing greater process.[180] The *Mathews* calculus then contemplates balancing of these concerns, through an analysis of "the risk of an erroneous deprivation" of the private interest if the process were reduced and the "probable value, if any, of additional or substitute safeguards."[181]

---

175. *Id.* at 203.
176. *See id.*
177. Walker v. Rowe, 791 F.2d 507, 511 (7th Cir. 1986).
178. 424 U.S. 319 (1976).
179. 542 U.S. 507, 529-31 (2004) (plurality opinion).
180. *Id.* at 529 (quoting *Mathews*, 424 U.S. at 335).
181. *Id.*

The *Mathews* test has justly been criticized for requiring courts to balance incommensurable qualities.[182] And it is indeed no bright line. But in the context of data security, it must surely encompass at least an industry-standard level of care. Failing to update software, placing private data in public files online, losing laptops, tapes, or USB drives with unencrypted (or weakly encrypted) data are all so far below the basic standard of care as to be actionable. Indeed, one could reasonably argue that the federal government's evolving, and improving, guidelines for the storage of personal data creates a standard to which state government should also be held.

On the other hand, the *Mathews* test would produce a much less victim-friendly picture when data breaches are caused by a malicious and skilled hacker as opposed to an opportunistic third party taking advantage of government carelessness. If, despite reasonable security precautions, a government database is hacked, especially from the outside the government would be able to argue that the real cause of the breach is external, exceptional, and unpredictable.[183] In many of these "smart hacker" cases, the government would likely be able to convince a court that additional security sufficient to prevent this previously unknown threat would not have been a reasonable expenditure. And that, as we will see, is also, more or less, the substantive Due Process result.

B. MODES OF RECOVERY

If the informational privacy right first alluded to in *Whalen* is indeed actionable in cases where the government failed to exercise due care, then there could be no better place to put it into action than to use it to remedy damages caused by accidental or illegal government data breaches. In *Whalen* the data were kept for lawful purposes. In the data breach scenario, the harm is not keeping the data, which presumably is also held for a lawful purpose, but rather it is an accidental or illegal disclosure. Establishing that the right exists is not enough, however, as the modern Supreme Court has erected doctrines that complicate any attempt at recovery, both under section 1983 against a state, and under *Bivens* against the federal government.

1. Section 1983 Action Against a State

If, as I have argued above, the right to have one's data looked after properly is indeed based in the Constitution, pleading a section 1983 claim for damages due to an actual or feared data breach should in principle be

182. *See, e.g.*, Edward L. Rubin, *Due Process and the Administrative State,* 72 CALIF. L. REV. 1044, 1136-44 (1984).

183. Inside jobs raise questions of due care in supervision and in the deployment of internal controls.

straightforward.[184] But two doctrines create possible obstacles: the Supreme Court's reluctance to allow section 1983 cases involving mere negligence in substantive Due Process claims, and a valuation problem. This section considers the first issue, the availability of relief under section 1983; valuation is discussed below in Section III.C.

A negligent act by a state official leading to a data breach should be actionable under section 1983.[185] That said, the government's duty of care is not unbounded. Yet, since *DeShaney*, the Supreme Court has not decided how much the duty extends to non-custody circumstances in which the state fails to provide or maintain services. Nevertheless, most courts of appeals accept that a duty enforceable under section 1983 applies if the State creates, and even more so if it enhances, a danger, although some courts require a high standard of egregiousness.[186] On the other hand, several courts have held that even where there is a duty, the responsible party may be protected by qualified immunity if the underlying federal right was unclear.[187]

Assuming no qualified immunity, the first critical issue therefore is deciding which data breaches are properly chargeable to the government under *DeShaney*, and which result primarily from the independent actions of a third party not under government control. A second issue, still the subject of debate in the larger context of section 1983, is the extent to which a plaintiff would have to prove more than ordinary negligence, unless the fact of the government-enhanced risk suffices to establish liability.

Failing to update software and leaving known exploits unpatched, placing private data in public files online, losing laptops, tapes, or USB drives with unencrypted (or weakly encrypted) data are all actions that make it easy for a third party to gain access to government-held data. In each of these cases, the but-for cause of the breach is the government's failure to meet minimal professional standards for handling sensitive data.[188] Under the *DeShaney* stan-

184. *See supra* note 45 (quoting 42 U.S.C. § 1983 (2006)). There are two elements of any section 1983 claim: the plaintiff must allege (1) a deprivation of a federal right and (2) that the person who deprived him of that right acted under color of state law. Gomez v. Toledo, 446 U.S. 635, 640 (1980).

185. Note, however, that several circuit court cases hold that the Ninth Amendment alone does not support a section 1983 claim. *See* MARTIN A. SCHWARTZ, 1 SECTION 1983 LITIGATION: CLAIMS AND DEFENSES § 3.03[B] at 3-25 n.80 (4th ed. 2003 & Supp. II 2008) (collecting cases). The Ninth Amendment is a part of the constitutional basis for a right to privacy. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

186. *See* SCHWARTZ, *supra* note 185, § 3.09[E] at 3-252.

187. *Id.* § 3.09[D] at 3-252.

188. Indeed, one could reasonably argue that the federal government's evolving and improving guidelines for the storage of personal data creates a standard to which state government should also be held. *See supra* Section II.C.

dard, these sorts of breaches should be blamed on the responsible party—the government—not the opportunistic third party who takes advantage of the responsible party's carelessness. What is more, many of these breaches will be the result of a policy, or pattern and practice, of failing to secure and patch systems, or failing to encrypt databases.

But where there is a sound policy in place requiring security, and it is routinely followed but was uncharacteristically ignored, a section 1983 claim may yet founder on the rule that mere negligence cases do not qualify for recovery. That is, unless the state-created danger rule is understood to mean that where the government steps in and forecloses self-help, mere negligence might be enough.[189] On the other hand, if the data has been kept in a reasonably secure fashion, and a skilled hacker nonetheless gets access, the breach is something external, exceptional, and unpredictable.[190] If additional security sufficient to prevent this previously unknown threat would not have been a reasonable expenditure ex ante, it is hard to see how the government can fairly be blamed.

Furthermore, a section 1983 claim requires that the person committing the deprivation have "acted under color of state law."[191] The Supreme Court has held in several contexts, however, that mere negligence by a state or local official does not give rise to a substantive Due Process claim against a state or municipality. Rather, to recover against a state government entity under section 1983 there must be an intentional or deliberate deprivation of life, liberty, or property,[192] or at least "deliberate indifference."[193]

The deliberate indifference requirement need not be fatal. As noted

---

189. *See e.g.*, Butera v. District of Columbia, 235 F.3d 637, 653 (D.C. Cir. 2001) (collecting cases).

190. Inside jobs raise questions of due care in supervision and in the deployment of internal controls.

191. 42 U.S.C. § 1983 (2006).

192. *See* Daniels v. Williams, 474 U.S. 327, 328-330 (1986); *see also* Davidson v. Cannon, 474 U.S. 344, 347-48 (1986) (explaining *Daniels*). The Court subsequently limited the reach of this doctrine when state actors infringe rights other than the Due Process Clause. *See e.g.*, Graham v. Connor, 490 U.S. 386, 395, 397 (1989) ("Today we make explicit . . . that *all* claims that law enforcement officers have used excessive force . . . in the course of an arrest, investigatory stop, or other 'seizure' of a free citizen should be analyzed under the Fourth Amendment and its 'reasonableness' standard, rather than under a 'substantive Due Process' approach," and "the 'reasonableness' inquiry in an excessive force case is an objective one . . . without regard to their underlying intent or motivation.").

193. City of Canton v. Harris, 489 U.S. 378, 388 (1989) (pre-*Collins v. City of Harker Heights*, 503 U.S. 115 (1992), decision finding municipal liability for poor training where failure to train amounted to deliberate indifference to the rights of persons whom the police come into contact); Estelle v. Gamble, 429 U.S. 97, 106 (1976) (deliberate indifference "to a serious medical need").

above, in the case of a data breach, the State's total control of the data, and its enhancement of the risk that the data may be disclosed, imposes an additional burden that it would not have in ordinary circumstances.[194] Alternately, the State's action in taking and holding the data can fairly be characterized as having subjected it to a heightened risk of improper disclosure, invoking the 'enhancement of risk doctrine' adopted by some courts of appeals.[195] In addition, a significant fraction of state breach cases to date are more systematic than the low-level, one-off negligence situations that the Supreme Court seemed concerned about in *Daniels v. Williams*.[196] A failure to have an adequate policy reasonably calculated to prevent data breaches, or a failure to require encryption of stored (and especially transported) data could transform a lost laptop or an improperly accessed server case into a section 1983 pattern-and-practice or deliberate indifference issue.

As this article went to press, the Supreme Court added a potentially more severe difficulty by holding in *Ashcroft v. Iqbal* that all section 1983 (and *Bivens*) plaintiffs must plead that each Government defendant, through his own individual actions, violated the Constitution.[197] The Court rejected the argument that a government official could be liable under a theory of "supervisory liability."[198] How this will play out in the context of government data breaches remains to be seen. Claims traceable to an individual's action—say, a lost laptop—certainly will be simpler to plead than those involving a more systemic failure, such as a department's failure to maintain its software or to properly train staff in its use. As noted above, however, even that simpler case may require a showing of deliberate indifference or its equivalent.

2. Bivens

In *Bivens v. Six Unknown Federal Narcotics Agents*, the Supreme Court found (or created) a federal cause of action for damages resulting from federal agents' violations of the Fourth Amendment.[199] In the almost fifty years since *Bivens*, the Supreme Court has extended it only twice: once to find an implied damages remedy under the Due Process Clause of the Fifth Amendment in

194. *See* SCHWARTZ, *supra* note 185, § 3.09[E] at 3-255 (surveying appellate cases and establishing that "[m]ost of the circuit courts have adopted some version of the state-created danger doctrine").

195. *See supra* notes 186, 194.

196. *See* 35 DAVID B. BROOKS, TEXAS PRACTICE SERIES, COUNTY AND SPECIAL DISTRICT LAW § 2.31 (2d ed. 2008) ("The issue which is the essence of most § 1983 litigation against local government today is whether the conduct of public officials or employees constitutes governmental policy or custom.").

197. 129 S. Ct. 1937, 1948 (2009).

198. *Id.* at 1949.

199. 403 U.S. 388, 391, 396-97 (1971).

Davis v. Passman,[200] and once to find a remedy under the Cruel and Unusual Punishment Clause of the Eighth Amendment in *Carlson v. Green*.[201] Both cases, however, were decided decades ago, and the more modern Court has evinced more than a slight hostility to new *Bivens* arguments.[202] Thus, for example, the Court has firmly resisted efforts to extend *Bivens* to suits requesting remedies from an entire federal agency, stating that *Bivens*' only purpose is to deter individual federal officers.[203] Justice Scalia, in particular, has made no secret of his disdain for *Bivens*, writing (with Justice Thomas):

> I do not mean to imply that, *if* the narrowest rationale of *Bivens did* apply to a new context, I *would* extend its holding. I would not. *Bivens* is a relic of the heady days in which this Court assumed common-law powers to create causes of action—decreeing them to be "implied" by the mere existence of a statutory or constitutional prohibition. As the Court points out . . . we have abandoned that power to invent "implications" in the statutory field. There is even greater reason to abandon it in the constitutional field, since an "implication" imagined in the Constitution can presumably not even be repudiated by Congress.[204]

While *Bivens* remains good law in regard to remedies for egregious rights violations by federal law enforcement officers, there is little reason to believe that the Supreme Court would allow *Bivens* to expand outside its current narrow confines, and particularly little reason to expect expansion in the information privacy context.

Even if the Court were less hostile to *Bivens* claims, it is unclear that the rationale of the *Davis* and *Carlson* cases would apply to the information privacy context. In both those cases, the Supreme Court stressed the absence of any alternate equally effective form of relief.[205] That may doom *Whalen*-based

---

200. Davis v. Passman, 442 U.S. 228, 231, 234 (1979) (recognizing Due Process clause claim alleging right to be free from gender discrimination as cause of action under the Fifth Amendment). *Contra* Schweiker v. Chilicky, 487 U.S. 412, 421-24 (1988) (declining to extend *Bivens* to alleged Fifth Amendment violations stemming from Social Security claims).

201. 446 U.S. 14, 18-20 (1980). *Carlson* represents perhaps the greatest, and also last clear expansion of *Bivens*. *But c.f.*, Bush v. Lucas, 462 U.S. 367, 377-79 (1983) (declining to extend *Bivens* to alleged First Amendment violation of federal employees' rights by their supervisor at a federal agency).

202. *See, e.g.*, Corr. Servs. Corp. v. Malesko, 534 U.S. 61, 71-72 (2001) (rejecting attempt to find implied private right of action, pursuant to *Bivens*, for damages against private operator of halfway house acting under color of federal law).

203. FDIC v. Meyer, 510 U.S. 471, 485 (1994).

204. *Malesko*, 534 U.S. at 75 (Scalia, J., concurring) (citations omitted).

205. *Carlson*, 446 U.S. at 20-21 (noting that "*Bivens* remedy is more effective than the Federal Tort Claims Act (FTCA) remedy"); Davis v. Passman, 442 U.S. 228, 231, 245 (1979).

claims because when it comes to information privacy claims against the federal government, the public enjoys the Privacy Act, despite all its flaws. Indeed, the District of Columbia Circuit recently rejected a *Bivens* data privacy claim for just this reason, noting that the Privacy Act constitutes a "comprehensive statutory scheme" that precludes such suits, and that the "plaintiffs could have stated colorable Privacy Act claims based on some of the alleged disclosures."[206] Other circuits have been more willing to hold that *Whalen* creates an enforceable privacy right,[207] but outside the context of law-enforcement, prison, or parole related cases, and perhaps medical privacy (*Whalen*'s facts), the Supreme Court will likely remain unwilling to follow suit.

C. THE VALUATION PROBLEM

Whether plaintiffs rely on *Bivens* or section 1983, valuation issues present a special problem in information breach cases for two reasons. First, the injuries likely will be as diffuse as the number of people or firms whose data was unintentionally exposed.[208] Second, in many breach cases it is not immediately clear how many people accessed the data nor whether they will make use of it. The harms from a data breach are sometimes immediate, but they are often speculative—perhaps no one saw it or an identity thief is just biding his time.

Valuation can become the critical issue when statutory remedies have threshold damages requirements. One of the possible ways to bring a claim under the Computer Fraud and Abuse Act, for example, requires $5,000 or more damage as a prerequisite to suit.[209] The statute defines damages broadly to include reasonable cost to any victim,[210] and the losses can be aggregated

206. Wilson v. Libby, 498 F. Supp. 2d 74, 87-88, 91 (D.D.C. 2007). Other courts have been more creative, at least in the law enforcement context. *See* Herring v. Keenan, 218 F.3d 1171, 1180-81 (10th Cir. 2000) (holding that *Bivens* action against probation officer for violating his probationer's informational privacy by revealing probationer's HIV-positive status to the probationer's sister and employer stated a claim but was barred by qualified immunity as right was not clearly established at time disclosure was made).

207. *See* cases cited *supra* notes 132, 131.

208. The aggregation issue is a familiar problem from the class action context, but so too is the roadblock that even when many plaintiffs suffer from a common cause, the federal courts will not as a rule entertain a case where the damages are likely to be individuated (e.g. theft from bank accounts). A federal court must find that "the questions of law or fact common to class members predominate over any questions affecting only individual members" before certifying a class. FED R. CIV. P. 23(b)(3).

209. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006).

210. *Id.* § 1030(e)(11). *Cf.* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001) (including cost of conducting a damage assessment and hiring a security consultant among the damages); United States v. Middleton, 231 F.3d 1207, 1213-14 (9th Cir. 2000) (including the wages of the employee who repaired the damage among the damages, even if he would have gotten the same wage regardless of whether he repaired the damage or

among victims.[211] At the time many victims learn of a data breach, however, it is uncertain as to whether they will suffer any tangible loss. The uncertainty itself is a form of damage, as a reasonably prudent person will take steps to secure their assets against third parties, such as an identity thief, who might try to use the data. Nevertheless, this idea has proved oddly difficult for some courts to accept in the data breach context, even though courts have had little trouble seeing probabilistic loss as an actionable harm in other contexts.[212] In *Pisciotta v. Old National Bancorp*, for example, the Seventh Circuit stated, "The plaintiffs maintain that the [Indiana breach] statute is evidence that the Indiana legislature believes that an individual has suffered a compensable injury at the moment his personal information is exposed because of a security breach. We cannot accept this view."[213] This is no isolated phenomenon:

> To date [2008] no court has found a plaintiff damaged by the mere release of the plaintiff's information. . . . [C]ourts have required that the information be used fraudulently. If a plaintiff can provide evidence that the plaintiff suffered an actual loss, they must still prove that this loss was caused by the breach.[214]

As noted above, federal regulations offer the possibility of credit monitoring as a practical matter, and this is what most settlements seem to offer class plaintiffs.[215] There is one notable exception to this rule, *Dickinson v. Collier*, in which class members received only one dollar each without a showing of actual damages.[216]

---

not).

211. Thus, for example, 18 U.S.C. § 1030(c)(4)(A)(I) (2006) sets the penalty for "loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value."

212. *See, e.g.*, Nat'l Res. Def. Council v. EPA, 464 F.3d 1, 6 (D.C. Cir. 2006) (holding that probabilistic risk, or substantial probability, of loss conferred standing).

213. 499 F.3d 629, 637 (7th Cir. 2007).

214. Derek A. Bishop, *No Harm No Foul: Limits on Damages Awards for Individuals Subject to a Data Breach*, 4 SHIDLER J. L. COM. & TECH. 12 at ¶ 23 (2008), *available at* http://www.lctjournal.washington.edu/Vol4/a12Bishop.html.

215. *See* GOV'T ACCOUNTABILITY OFFICE, DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN, GAO-07-737, at 35 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf ("Entities experiencing a breach also often provide affected individuals with free credit monitoring services."). For an overview of recent private data breach court decisions, see generally Bishop, *supra* note 214; John Kennedy & Parishi Sanjanwala, *Outside Counsel: Civil Suits Arising From Information Security Breaches*, N.Y.L.J., Feb. 2, 2007, at col. 4.

216. 477 F.3d 1306 (11th Cir. 2007).

Statutory damages should be a way of overcoming valuation difficulties. The Privacy Act offers statutory damages of $1,000 where an agency acted in a manner that was intentional or willful,[217] but as noted above, in *Doe v. Chao* the Supreme Court held that plaintiffs seeking to recover this sum from the government must prove at least some "actual damages," and that a complaint of emotional injury stemming from the disclosure of their SSNs did not suffice.[218] The government admitted that it published the plaintiff's SSNs widely.[219] At the trial court level the plaintiffs did allege that they were concerned about identity theft, but they appear to have framed this as an emotional injury claim, rather than as a probabilistic injury.[220] Thus, *Doe v. Chao*, does not directly address whether a properly pled probabilistic injury would state a claim under the Privacy Act, although the thrust of *Doe v. Chao* would seem to lean against it.

IV. CONCLUSION

Government data breaches have some similarities to private sector data losses, but there are also major differences. Governments have the power to compel data disclosures by law, and by de facto legal regimes that make disclosures a prerequisite for licenses and benefits that are required to live a normal life, or to conduct a normal business.

Data breach legislation fueled by, and fueling, an increased public concern over data breaches represents one of the important success stories over the past decade in the campaign to increase the legal protection for personal data privacy in the United States. Florida's current breach statute, for example, requires corporations to notify victims of a data breach within forty-five days, or face fines of up to $500,000 per breach.[221] While the statute does not apply to government agencies, it does cover government contractors.[222] Often, governments have exempted themselves from data breach laws that cover data held in the private sector.

---

217. 5 U.S.C. § 552a(g)(4) (2006).

218. 540 U.S. 614, 617-18, 622-23 (2004) (rejecting tort-like 'general damages').

219. The government had not contested this allegation at trial before the magistrate judge. Doe v. Herman, No. Civ. A. 297CV00043, 1999 WL 1000212, at *2 (W.D. Va. Oct. 29, 1999) (report and recommendation of magistrate judge), *report and recommendation adopted in part by* Doe v. Herman, No. Civ. A. 2:97CV00043, 2000 WL 34204432 (W.D. Va. Jul 24, 2000), *aff'd in part, rev'd in part by* Doe v. Chao, 306 F.3d 170 (4th Cir. 2002), *aff'd* by Doe v. Chao, 540 U.S. 614 (2004).

220. "The Plaintiffs allege that the distribution of this information to complete strangers has had adverse effects on them. They assert that the Department's conduct raises a serious and grave threat to privacy, security, credit ratings, identity and well-being." *Id.*

221. FLA. STAT. § 817.5681 (West 2009).

222. FLA. STAT. § 817.5681(1)(d) (West 2009); *see* Garcia, *supra* note 3, at 706.

The Federal Information Security Management Act and new federal regulations, however, require federal agencies to make serious efforts to protect private data. Major data breaches trigger a duty to disclose, at least eventually. But the administrative remedies available to parties whose data has been exposed are still paltry, generally limited to credit monitoring. Other statutes, such as the Privacy Act and the Computer Fraud and Abuse Act, create potential remedies, but, so far, only for parties who can show substantial actual (rather than feared or potential) damage.

At present, states generally lag behind the federal government both in their commitment to rigorously and systematically securing data, and in the remedies available under statute. Among the better policies needed are:

- more systematic reporting of government data breaches;
- some consistent definitions of covered data;
- enactment of statutes (state or federal) that provide for Privacy Act-like remedies against states; and
- better legal treatment of the risks of identity theft and other dangers that are triggered by a data breach. This should include those that may not be categorized as "actual injury" as required under current law.

Although there has been significant progress in some states and at the federal level, much remains to be done to improve government responses to data breaches and especially to provide remedies to those harmed by data breaches. I have argued above that a constitutional remedy combining *Whalen*, *DeShaney*, and section 1983 is available against states guilty of data breaches, at least in cases where the state failed to exercise due care when holding the data. This right is separate from any informational privacy rights that constrain the government's ability to acquire personal or corporate information. But even if courts accept this analysis, much remains to be done.

PRIVACY COSTS AND PERSONAL DATA PROTECTION: ECONOMIC AND LEGAL PERSPECTIVES

Sasha Romanosky & Alessandro Acquisti†

TABLE OF CONTENTS

---

† Sasha Romanosky is a PhD student at the Heinz College at Carnegie Mellon University. Alessandro Acquisti is an Associate Professor of Information Systems and Public Policy also at the Heinz College at Carnegie Mellon University. We can be reached at [sromanos, acquisti]@andrew.cmu.edu. We would like to thank the following people for their insightful comments and feedback: John Bagby, Fred Cate, Ben Edelman, Mark Melodia, and Alana Maurushat. We would like to acknowledge CyLab at Carnegie Mellon for their generous support. We would also like to thank Charlotte Chang, Varty Defterderian, Kristin Kemnitzer, and Peter Nagle for their excellent editing.

I. INTRODUCTION

In 1994, the U.S. Congress enacted the Drivers Privacy Protection Act (DPPA)[1] to protect the privacy of personal data collected by states' Departments of Motor Vehicles (DMVs). The Act made parties such as data brokers or DMVs liable to individuals whose personal information had been wrongfully used or released. The DPPA allowed offended individuals to bring a civil action in a United States district court against violators, permitting courts to award "*actual damages*, but not less than liquidated damages in the amount of $2,500."[2] However, obtaining compensation by proving *actual* damage proved elusive: after all, what constitutes an actual damage when an individual's personal information assembled by a state's DMV is simply passed to third parties—such as data aggregators and data brokers? In 2005 the Eleventh Circuit resolved that under the DPPA, individuals did not have to prove actual damages in order to get liquidated damages.[3] But this has not translated to other privacy legislation, particularly in the area of consumer data breaches:[4] obtaining compensation for the loss or theft of personal information held by another entity has not, generally, proved viable.[5]

Economic and legal theories seem to assess differently what constitutes consumer harm resulting from a breach of personal data: economic theory may recognize privacy costs that legal jurisprudence does not.[6] For an economist, the potential damages from the dissemination of consumer informa-

1. 18 U.S.C. §§ 2721-2725 (2006).
2. 18 U.S.C. § 2724(b)(1) (2006) (emphasis added).
3. Kehoe v. Fid. Fed. Bank & Trust, 421 F.3d 1209, 1210 (11th Cir. 2005).
4. We generally refer to "breaches" as the loss or theft of personal consumer information. For instance, the California data breach disclosure law defines a breach as an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." *See* CAL. CIV. CODE §§ 1798.29, 1798.82 (2002).
5. For example, in a 2004 case involving the wrongful disclosure of a Social Security Number, the Supreme Court ruled that the Privacy Act of 1974 requires an individual to prove actual harm before he can receive the minimum statutory award. Doe v. Chao, 540 U.S. 614, 617-18 (2004).
6. Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information*, *in* SECURING PRIVACY IN THE INTERNET AGE 111, 115-16 (Anupam Chander et al., eds., 2007).

tion may be various: from the increased probability of receiving spam or being subject to identity theft (which elevates the individual's expected, though not necessarily realized, costs), to the decrease in market value of their personal data, given its wider availability and lower scarcity. For the economist, the difference between an actual and a possible cost is a matter of probabilities and uncertainty; in either case, the breach of a consumer's data has heightened the *expected* costs—be they tangible or intangible—that the consumer will suffer when (and if) his data is abused. However, while other areas of law have accepted the concept of probabilistic damage,[7] such ambiguity is, most of the time, unacceptable to personal data protection legislation: under the law, a person may not be able to sue a data broker for *future* or *potential* identity theft, which *may* have originated from the disclosure of his personal data. Under tort law, compensation for losses requires plaintiffs to demonstrate harm to one's person or property. While additional pecuniary awards can be granted for economic loss, they are predicated on actual or physical harm. As a result, courts (and juries) have often rejected attempts to award damages for breaches of personal information,[8] challenging the very effectiveness of policy initiatives aimed at protecting consumer data.[9] The goal of this Article, therefore, is to examine U.S. personal data protection laws using the lens of economic theory. We focus on consumer data breaches resulting from the loss or theft of personal information held by another entity.

Personal information flows are necessary for the functioning of modern economies and are often beneficial to consumers (data subjects), first parties (data holders), and third party companies (data brokers). Consumers benefit from transactions involving their personal data due to easier access to credit and insurance,[10] customization,[11] and personalization.[12] However, they may

---

7. *See generally* Glen O. Robinson, *Probabilistic Causation and Compensation for Tortuous Risk*, 14 J. LEGAL STUD. 779 (1985); Richard W. Wright, *Actual Causation vs. Probabilistic Linkage: The Bane of Economic Analysis*, 14 J. LEGAL STUD. 435 (1985). *See also* Jennifer A. Chandler, *Negligence Liability for Breaches of Data Security*, 23 BANKING & FIN. L. REV. (2008), 223-47 *available at* http://ssrn.com/abstract=998305, discussed *infra* in the Article, on the comparison between harm following data breaches and medical cases that allow for damages for monitoring one's health after being exposed to toxic chemicals.

8. *See infra* Section III.B.

9. P. H. RUBIN & T. M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION 16 (2002).

10. *See generally* NICOLA JENTZSCH, THE REGULATION OF FINANCIAL PRIVACY: THE UNITED STATES VS. EUROPE (ECRI, Research Report, No. 5) (2003); Nicola Jentzsch & San José Riestra, *Consumer Credit Markets in the United States and Europe*, *in* THE ECONOMICS OF CONSUMER CREDIT 27 (Giuseppe Bertola et al., eds., 2006).

11. *See* Robert C. Blattberg, & John Deighton, *Interactive Marketing: Exploiting the Age of Addressability*, 33 SLOAN MGMT. REV. 5, 5 (1991).

also be harmed by abusive treatment of their data; they may suffer from identity theft, discrimination, or social stigma;[13] they may witness degraded value of their personal data publicly disclosed, or suffer other psychological, intangible costs. Companies also bear costs when they misuse—or, specifically, lose because of negligence or criminal attacks—consumers' personal data: they may sustain negative publicity, embarrassment, lost sales, or suffer fines or other sanctions.[14] Technological solutions such as data security and privacy enhancing technologies[15] can help balance the interests and needs of data subjects and data holders.[16] However, they are not always spontaneously adopted by individuals or companies,[17] which drives the motivation for policy intervention: in the U.S. there exists a patchwork of state and federal legislative initiatives that attempt, in coordination with self-regulatory approaches, to reduce data breaches, protect personal information, and mitigate the harm to disparate parties due to these breaches.

In this Article, we undertake an economic analysis and comparison of such legal mechanisms for consumer data protection. Our goal is not to establish the value of privacy legislation using economic theory: the vast and complex array of U.S. legislative initiatives meant to protect personal information is clear proof of an interest in protecting consumer data while maintaining beneficial flows of personal information. Rather, we investigate the effectiveness of those initiatives. We focus on data breaches and the resulting

---

12. *See* Alessandro Acquisti & Hal R. Varian, *Conditioning Prices on Purchase History*, 24 MARKETING SCI. 367, 374 (2005).

13. *See* Alessandro Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification*, *in* PROCEEDINGS OF THE 5TH ACM CONFERENCE ON ELECTRONIC COMMERCE 21 (2004).

14. *See* David Streifield, *On The Web, Price Tags Blur*; *What You Pay Could Depend On Who You Are*, WASH. POST, Sept. 27, 2000, at A1. *See also* Alessandro Acquisti et al., *Is There a Cost to Privacy Breaches? An Event Study*, ICIS 2006 PROCEEDINGS 1563 (2006). For further discussion regarding sanctions imposed by the FTC on firms that violate privacy policies and engage in deceptive practices using consumer data, see *infra* Section III.A.

15. *See generally* Ian Goldberg, *Privacy-Enhancing Technologies for the Internet III: Ten Years Later*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES (Alessandro Acquisti et al. eds., Auerbach, 2008).

16. Data subjects (consumers) may want stronger protection of their personal information, while data holders (ecommerce, marketing, data brokers, etc.) benefit from less stringent regulations.

17. *See generally* Benjamin D. Brunk, *Understanding the Privacy Space*, 7 FIRST MONDAY 10 (Oct. 2002), http://131.193.153.231/www/issues/issue7_10/brunk/index.html (discussing investments in privacy enhancing technologies). Naturally, companies have incentives to invest in information security to protect their information systems and assets. *See generally* Lawrence Gordon & Martin Loeb, *The economics of information security investment*, 5 ACM TRANSACTIONS ON INFO. & SYS. SECURITY, 438 (2002). However, it is an unresolved issue how much the consideration of consumer data privacy affects those incentives.

consumer costs of such violations.[18] Specifically, we present an economic analysis of three legislative approaches used to reduce the potential privacy harm from a firm's activity: ex ante safety regulation, ex post liability, and information disclosure. In addition, we discuss the means by which legal and economic frameworks calculate and compensate for consumer loss. Ex post liability, ex ante regulation, and information disclosure laws have had only mixed success in preventing consumer data breaches. Some of the causes for such lukewarm results relate to challenges that each of these mechanisms face in the marketplace—challenges that economic theory (in particular, behavioral economics and transaction costs economics) help explain.

The rest of the Article is structured as follows: first, we introduce the general mechanisms of regulation, liability, and information disclosure. We next present examples of these approaches in the area of personal information protection and analyze their impact, showing a gap between the legislature's intentions and marketplace reaction. Finally, we provide a formal economic analysis of regulation, liability, and information disclosure, and contrast conditions under which they may be socially efficient or inefficient.[19]

II. CONSUMER DATA PROTECTION LAWS

Despite, or perhaps because of, the adoption of more U.S. state laws requiring firms to notify consumers of data breaches, breaches appear to be occurring more frequently. For example, the identity theft resource center (ITRC)—which maintains a detailed catalog of reported data breaches—recently announced a surge in breaches in 2008 to 656, up 47% from the previous year.[20] Such breaches can have a tremendous range of impacts for the individuals whose data are affected. In cases where the breach is caused by simple loss of a backup tape, or theft of a device with intention to wipe the contents and sell the hardware, the financial impact to consumers may be negligible—in fact, there may be none. However, breaches can also result in various types of identity theft (ranging from fraudulent unemployment

18. In this article, we focus on data breaches in which the data of individuals (such as consumers, employers, or third parties) held by a company was exposed because of poor security practices, obtained by unauthorized parties (such as cyber-criminals), lost (in computers or data storages went missing), sold, or otherwise traded in manners that generate suspicion of illegality in the victims.

19. We refer to whether these methods succeed or fail to minimize total firm and consumer costs. A level of care that minimizes the sum of these costs is known by familiar economic terms as the socially optimal level.

20. Identity Theft Resource Center, *2008 Data Breach Totals Soar*, http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml (last visited July 18, 2009).

claims[21] to fraudulent tax returns,[22] fraudulent loans,[23] home equity fraud,[24] and payment card fraud[25]) which can impose financial, psychological, and other costs on the victims.[26] Consumer costs can be indirect, too. For instance, in response to a breach notification, consumers must process the information and decide a course of action. This imposes cognitive costs and can represent a significant burden.

In addition to losses inflicted to others, the breached institutions can also incur significant costs as a result of incident investigations—whether they are schools, retail stores, hospitals, or government agencies. Such costs include fines paid to federal agencies, legal fees, and consumer redress. For example, the Department of Veterans Affairs paid $20 million to veterans and current military personnel after the theft of a laptop that contained personal information of 26 million veterans, even though officials maintain that no information was accessed.[27] Choicepoint incurred at least $26 million in fines and fees from a breach in 2005,[28] and as of fall 2007 the retailer TJX reported losses of $256 million from its massive data breach in 2005.[29] Heartland Payment Systems, one of the largest credit card processing companies in the United States, incurred $12.6 million in fines and fees from a breach in 2008

21. *See* Dan Goodin, *IT Contractor Caught Stealing Shell Oil Employee Info*, THE REGISTER, Oct. 7, 2008.

22. *See* Robert McMillan, *United Healthcare Data Breach Leads to ID Theft*, NETWORK WORLD, June 3, 2008.

23. *See* Mary Hogan, *Arrests Made in ID Theft Case*, SEALY NEWS, Aug. 9, 2008.

24. *See* Brian Krebs, *Thieves Stole Identities to Tap Home Equity*, WASH. POST, Nov. 28, 2008, at E10.

25. *See* Mark Jewell, *TJX Breach Could Top 94 Million Accounts*, MSNBC, Oct. 24, 2007, http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml (reporting that payment fraud from the TJX breach reached $83 million); Ross Kerber, *Grocer Hannaford Hit by Computer Breach*, BOSTON GLOBE, Mar. 18, 2008, http://www.boston.com/business/articles/2008/03/18/grocer_hannaford_hit_by_computer_breach/ (reporting 1,800 cases of fraudulent payment card use); *Data-Breach Lawsuit Follows $9 Million Heist*, SECURITY FOCUS, Feb. 6, 2009 (reporting fraudulent losses of $9 million from RBS Worldpay breach).

26. A particularly nefarious example of the consequences of the theft of personal information occurred in *Remsburg v. Docusearch*: the defendant sold personal information about the plaintiff's daughter to Liam Youens, who stalked and killed her. Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003).

27. Terry Frieden, *VA Will Pay $20 Million to Settle Lawsuit Over Stolen Laptop's Data*, CNN, Jan 27, 2009, http://www.cnn.com/2009/POLITICS/01/27/va.data.theft/index.html.

28. Jaikumar Vijayan, *ChoicePoint To Pay $10M To Settle Last Breach-Related Lawsuit*, COMPUTER WORLD, Jan. 28, 2008, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9059659.

29. Ross Kerber, *Cost of Data Breach at TJX Soars to $256m; Suits – Computer Fix Add to Expenses*, BOSTON GLOBE, Aug. 15, 2007, at A1.

that has affected, as of this writing, more than 665 financial institutions.[30] In fact, a recent study revealed an increase in costs to companies because of data breaches every year since 2005.[31]

As a result of data breaches and their costs, U.S. policymakers have produced a patchwork of legislation that creates incentives for companies to protect personal information, and decrease the harm to disparate parties as a result of breaches of this information. This Part presents an overview of the legal approaches adopted to protect personal information, borrowing a classification of legislative initiatives found in the economic theory of law.

A long tradition of scholarship has investigated the relationship between economics and the law, and has applied economic modeling to the analysis of various legislative approaches designed to reduce accident costs.[32] Some literature directly compares ex ante safety regulation with ex post liability,[33] whereas other literature separately discusses the economics of information disclosure.[34]

Ex ante safety regulation is a common way to control or limit an externality caused by a firm's harmful activity. This is an ex ante mechanism, in the sense that it is meant to prevent harm from occurring through the enforcement of minimum standards or operating (compliance) restrictions. It is considered "public" in nature because enforcement is promulgated by sta-

---

30. Linda McGlasson, *Heartland Data Breach Update: Now More Than 665 Institutions Impacted*, BANK INFO SECURITY, Feb 12, 2009, http://www.bankinfosecurity.com/articles.php?art_id=1200.

31. PONEMON INSTITUTE, LLC, 2008 ANNUAL STUDY: COST OF A DATA BREACH 10 (2009).

32. *See generally* STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW (2004); WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF TORT LAW (1987); John Prather Brown, *Toward an Economic Theory of Liability*, 2 J. LEGAL STUD. 323 (1973); A. Mitchell Polinsky & Steven Shavell, *Economic Analysis of Law* (Stanford Law Sch., John M. Olin Program in Law & Econ., Olin Working Paper No. 316, 2005), *available at* http://ssrn.com/abstract=859406; Cento Veljanovski, *The Economics of Law* 151 (Inst. of Econ. Affairs, Hobart Paper No. 157, 2006), *available at* http://ssrn.com/abstract=935952.

33. *See generally* Steven Shavell, *Liability for Harm Versus Regulation of Safety* (Nat'l Bureau of Econ. Research, Working Paper Series No. 1218, 1983), *available at* http://ssrn.com/abstract=227549; Steven Shavell, *A Model of the Optimal Use of Liability and Safety Regulation*, 15 RAND J. ECON. 271, 271-80 (1984) [hereinafter *Model*]; Charles D. Kolstad et al., *Ex Post Liability for Harm vs. Ex Ante Safety Regulation: Substitutes or Complements?*, 80 AM. ECON. REV. 888 (1990); Patrick W. Schmitz, *On the Joint Use of Liability and Safety Regulation*, 20 INT'L REV. L. & ECON. 371 (2000).

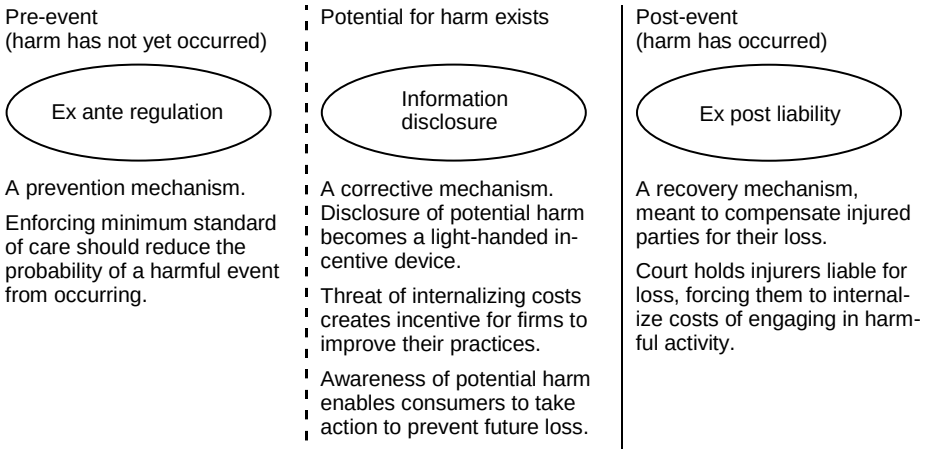
34. *See generally* Steven Shavell, *A Note on the Incentive to Reveal Information*, 14 GENEVA PAPERS ON RISK & INS. 66 (1989); Boyan Jovanovic, *Truthful Disclosure of Information*, 13 BELL J. ECON. 36 (1982); A. Mitchell Polinsky & Steven Shavell, *Mandatory Versus Voluntary Disclosure of Product Risks* (Stanford Law & Econ., Olin Working Paper No. 327, 2006), *available at* http://ssrn.com/abstract=939546.

tutes and government agencies,[35] though safety standards can also be created through self-regulation by firms. An important characteristic is that sanctions can be imposed simply as soon as standards have been violated, even though no harm has yet occurred.

Ex post liability, instead, is exercised after harm has occurred. It is a legal device that enables victims to sue for damages, forcing firms to internalize part of the harm they cause. It is "private" in nature because suits are initiated by private entities such as consumers and corporations.

Finally, information disclosure forces firms to reveal information about the risks of their products or services. The intent is to allow consumers to take action to mitigate potential loss, and create a strong incentive for firms to improve their practices—in order to avoid negative publicity and customer backlash. This approach is a lighter form of intervention in that it does not mandate specific technologies or precautions, and therefore allows market forces to respond freely. Figure 1 illustrates these three mechanisms.

Figure 1: Three Policy Approaches



The dashed vertical line represents an event that could lead to harm, such as a data breach, while the solid vertical line represents the actual harmful consequence, such as identity theft. Below, we discuss how these three legislative approaches have been implemented in the area of consumer data protection as mechanisms to help prevent data breaches. Indeed, the scope of laws and regulations relating to consumer privacy is broad and it is not the purpose of this paper to summarize them all. Instead, we focus our attention on personal consumer data that are the subject of many data breaches, and

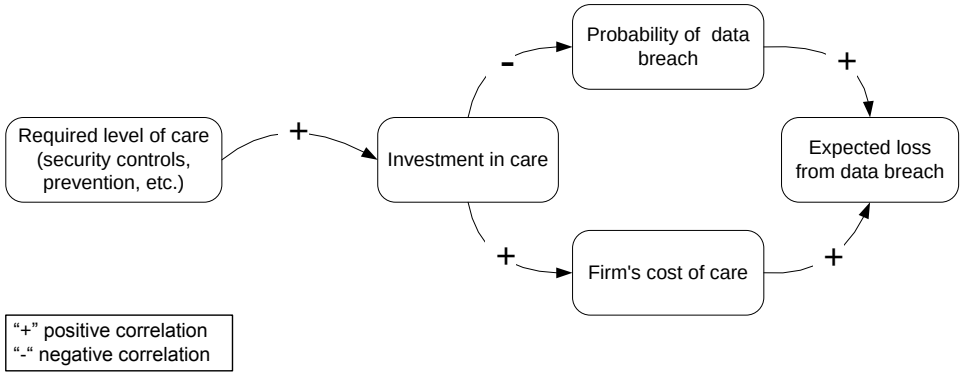
35. Susan Rose-Ackerman, *Regulation and the Law of Torts*, 81 AM. ECON. REV. 54, 54 (1991).

note that the three approaches can (and certainly have been) used in combination.

A. EX ANTE REGULATION

Consumer data protection and compliance regulations require firms to invest in a minimum level of security controls in the hopes of reducing the probability of a data breach and resulting harm. Figure 2 illustrates this mechanism: as the required level of care increases, the investment in security protections also increases, reducing the probability of a breach, which in turn is expected to decrease the loss caused by the firm's activity (such as those cause by a data breach).[36] However, increased investment in care also increases a firm's total expected cost.[37]

Figure 2: Ex Ante Safety Regulation



While a number of U.S. federal and state laws currently mandate only "reasonable" security controls, some states have recently adopted more specific and proscriptive standards.[38] For example, Connecticut law (HB5658),

36. The signs on the arrows in the diagram reflect the correlation between two adjacent stages. E.g., an increase in the probability of a breach increases the expected loss from a data breach. Similarly, because the correlation is positive ("+"), a decrease in the probability of a breach decreases the expected loss.

37. This causality diagram foreshadows an interesting policy problem: while spending more on security lowers the probability of a breach (and resulting harm), it also increases the firm's costs. And so, it is no longer obvious whether the net effect is higher or lower overall costs.

38. *See* Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (2006) (requiring financial institutions to provide "adequate" security controls for consumer information); Sarbanes-Oxley Act 15 U.S.C. § 7262 (2002) (requiring firms to implement reasonable security controls for material computing systems); Health Insurance Portability and Accountability Act Pub L. No. 104–191, § 110 Stat. 1936 (1996) (requiring covered entities to establish reasonable controls protecting personal health information).

An Act Concerning the Confidentiality of Social Security Numbers, requires any person or business that collects or possesses Social Security Numbers to create and publicly display a privacy policy.[39] It also requires, more generally, anyone who possesses personal information to protect it while in use, and destroy it before disposal.[40] Michigan, Rhode Island, and Texas also require similar kinds of data protection and disposal measures.[41]

Both Massachusetts[42] and Nevada,[43] on the other hand, enforce stricter standards through data encryption. For example, in Massachusetts, businesses must encrypt all personal information sent across public (wired or wireless) networks or stored on portable devices (laptops, USB drives, etc). The law "establish[es] minimum standards . . . to safeguard personal information" which apply to every person or business that owns, licenses, or stores personal information of Massachusetts residents.[44] Similarly, the encryption provision of Nevada's data security law prohibits businesses from transferring unencrypted personal information beyond the "secure system of the business."[45]

Federal administrative agencies have also tried to enforce similar standards on entities under their jurisdiction. For example, the SEC proposed an amendment to Regulation S–P as Regulation S–P: Privacy of Consumer Financial Information and Safeguarding Personal Information where they propose "more specific requirements for safeguarding information and responding to information security breaches, and broaden the scope of the information covered by Regulation S–P's safeguarding and disposal provisions."[46] Specifically, the proposal would require stricter "administrative, technical and physical information safeguards" for the protection of personal customer data, an increase in the scope of information covered, proper guidelines for

39. H.B. No. 5658 (Conn. 2008), *available at* http://www.cga.ct.gov/2008/ACT/PA/2008PA-00167-R00HB-05658-PA.htm (requiring that policies must "protect the confidentiality of, prohibit unlawful disclosure of, and limit access to SSN").

40. *Id.*

41. *See* MICH. COMP. LAWS ANN. § 445.84 (West 2005); R.I. GEN. LAWS § 11-49.2-2 (2005); TEX. BUS. & COM. CODE ANN. § 48.102(a) (2005).

42. 201 MASS. CODE REGS. 17.01 (2009). Most components become effective May 1, 2009 while the requirement to encrypt data stored on portable devices has been extended to Jan. 1, 2010. *See generally* Kris D. Meade & Robin B. Campbell, *Massachusetts Sets the New Standard, But Delays Implementation*, PRIVACY LAW ALERT (2008), *available at* http://www.crowell.com/NewsEvents/Newsletter.aspx?id=1096.

43. NEV. REV. STAT. § 597.970 (2008).

44. 201 MASS. CODE REGS. 17.01 (2009).

45. NEV. REV. STAT. § 597.970 (2008).

46. Regulation S–P: Privacy of Consumer Financial Information and Safeguarding Personal Information; Proposed Rule, 73 Fed. Reg. 13,692 (Mar. 13, 2008) (to be codified at 17 C.F.R. pt. 248), *available at* http://www.sec.gov/rules/proposed/2008/34-57427fr.pdf.

the disposal of personal information, and require that these security policies be formalized in writing.[47]

The FTC employs Section 5 of the FTC Act[48] to impose sanctions on firms that exhibit unfair or deceptive practices—practices that they feel would likely result in the disclosure of personal information or a privacy invasion. The FTC has also created the *Red Flag Rules* which define specialized guidelines for financial institutions and creditors to implement controls that would detect potentially fraudulent activity leading to identity theft.[49]

The enforcement of minimum protection standards can also be achieved through self-regulation. For instance, VISA, MasterCard, and other credit card companies have created a set of guidelines for the protection of payment (debit and credit) card data. Formally know as the Payment Card Industry Data Security Standard (PCI DSS),[50] these rules are mandated by the credit card companies and are ostensibly a prerequisite for any merchant that wants to process payment card transactions. VISA also imposes a requirement that strong encryption be enabled on U.S. gas pumps in order to prevent unauthorized disclosure of personal financial information.[51]

B. EX POST LIABILITY

Negligence liability claims in the context of breaches of personal information generally allow compensation to victims who successfully demonstrate four conditions: (1) that a firm had a duty of care to protect the plaintiff's information, (2) that the firm breached this duty, (3) that actual harm was suffered, and (4) that this harm was a direct result of the firm's breach of duty.[52]

---

47. *Id.*

48. 15 U.S.C. §§ 41-58 (2000). The FTC also imposed sanctions on firms that already incurred breaches, though had not necessarily demonstrated actual harm.

49. *See generally* FEDERAL TRADE COMMISSION, *Fighting Fraud with the Red Flags Rule*, http://www.ftc.gov/redflagsrule (a website developed by the FTC to assist organizations in developing the proper procedures).

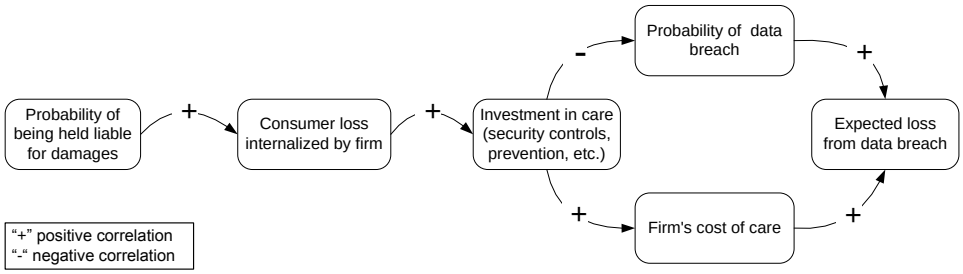
50. PCI SECURITY STANDARDS COUNCIL, *About the PCI Data Security Standard (PCI DSS)*, https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (last visited May 1, 2009).

51. Jaikumar Vijayan, *Clock Ticking for Gas Stations to Pump Up Data Security*, COMPUTERWORLD, Jan. 7, 2009, *available at* http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9125261.

52. *See* Guin v. Brazos Higher Educ. Serv. Corp., No. 05-668, 2006 U.S. Dist. LEXIS 4846, at 6 (D. Minn. Feb. 7, 2006); Kahle vs. Litton Loan Serv., 486 F. Supp. 2d 705, 708 (S.D. Ohio 2007); Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018, 1020 (D. Minn. 2006); Pisciotta v. Old Nat'l. Bancorp, 499 F.3d 629, 634 (7th Cir. 2007); *see also* Chandler, *supra* note 6, at 223; John Hutchins, A New Frontier in Privacy Litigation: The Advent of Private

Ex post liability serves as a deterrent for firms by raising their expected costs of engaging in some harmful activity and compensating injured parties for their loss. In the context of consumer losses due to breaches, this causality is illustrated in Figure 3: as the probability of being held liable for damages due to breaches increases, so does the amount of consumer loss internalized by the firm. This, in turn, increases the firm's incentive to further invest in security controls, reducing the probability of a data breach, and finally, reducing the expected harm. Just as with ex ante regulation, higher investment in care also increases the firm's cost of care, increasing the total expected cost of a data breach.

Figure 3: Ex Post Liability



The strongest push towards assigning liability for data breaches has emerged from state legislation that shifts liability for breaches of a specific type of personal information—credit card numbers—from the financial institution to the merchant.[53] While consumers are responsible for a maximum of fifty dollars from a fraudulent charge on their credit card,[54] there are still tangible costs associated with providing the consumer with a new credit card, which represents a social loss.[55] Specifically, such legislative efforts are created to make retailers liable to card-issuing banks for the costs of reissuing payment cards.[56]

For example, while only contractually binding, under the PCI DSS, merchants may be held liable to card-issuing banks if they (or their service providers or business partners) fail to maintain minimum security controls on

Lawsuits Over Data Security Breaches at the ABA Annual Meeting, Section of Litigation, Remarks at the ABA Annual Meeting (Aug. 8, 2008).

53. Tracy B. Gray et al., *Privacy & Data Security Briefing: Issue 2*, HOGAN AND HARTSON LLP, at 8 (2008), *available at* http://www.hhlaw.com/pressroom/newspubs/PubDetail.aspx?publication=3628.

54. 15 U.S.C. § 1693(g) (2006).

55. The concept and implication of social loss will be discussed further in this Article.

56. Gray, *supra* note 53, at 9.

computing systems that store, process or transmit payment card information.[57] In addition to minimum standards of care, the PCI DSS effort holds a merchant's acquiring bank liable for breaches suffered by the merchant.

Moreover, in some instances PCI DSS has evolved into a legal standard through the adoption of certain components as state law. For example, Minnesota's Plastic Card Security Act (HF1758) allows financial institutions to bring action against merchants who suffer a breach of a payment card's magnetic stripe information.[58] The act "essentially imposes strict liability on merchants" by requiring them to reimburse financial institutions for issuing new payment cards.[59] Nevada also legalizes PCI DSS by requiring data collectors who accept payment card information from a sale to comply with the PCI DSS standards.[60] Moreover, Nevada law creates a standard of care by absolving any data collector of liability for damages from a data breach if the data collector is in compliance with PCI DSS and if the breach was not caused by gross negligence.[61]

In addition, Connecticut amended its data breach disclosure law (SB1089) to include provisions for liability to the merchant.[62] Specifically, a merchant that suffers a data breach "shall be liable to a bank . . . for the costs of any reasonable action undertaken by the bank . . . on behalf of its customers as a direct result of the breach."[63] The related costs include cancellation or reissuance of cards, and costs associated with stop payments and refunds.[64]

---

57. The relationships involved in PCI DSS compliance are unusual. While it is the merchant that must demonstrate compliance with the PCI DSS standard, it is the merchant's acquiring bank (the entity that settles credit card transactions on behalf of the merchant) that is subject to a fine by a credit card company. This is because only the acquiring bank has a direct relationship with the credit card company, not the merchant. *See* Benjamin Wright, *New Merchant Liability for Losing Credit Card Data,* SANS TECHNOLOGY INSTITUTE, June 14, 2007, http://www.sans.edu/resources/leadershiplab/cc_data_mn_law_bw1.php; David Navetta, *The Legal Implications, Risks and Problems of the PCI Data Security Standard*, THE SCI-TECH LAWYER, Volume 5, Number 1, Summer, 2008, http://www.abanet.org/scitech/scitechlawyer/pdfs/data.pdf.

58. H.F. 1758, 85th (Minn. 2007-2008).

59. Michael P. Carlson & Laura E. Meyer, *Minnesota's New 'Plastic Card Security Act': A Harbinger of Things to Come?*, TRENDS, March/April 2008, at 7, *available at* http://www.faegre.com/files/12645_Trends%20March%20and%20April%202008.pdf.

60. *See* S.B. No. 227 (Nev. 2009), https://www.leg.state.nv.us/75th2009/Bills/SB/SB227_EN.pdf (repealing NRS 597,970).

61. *Id.*

62. S.B. 1089, Gen Assem., Reg. Sess. (Conn. 2007).

63. *Id.*

64. *Id.*

Other states have tried to pass similar liability bills, including Texas, Illinois, Iowa, Washington, Wisconsin, Alabama, Michigan, and New Jersey. A Massachusetts bill (HB 213)[65] was defeated despite the fact that Massachusetts hosts the head office of TJX Cos., the company that suffered a breach of some 45 million credit card records in 2005.[66] Governor Schwarzenegger vetoed the California bill (AB 779), citing that it would unfairly harm small businesses.[67] The Governor claimed that "the marketplace has already assigned responsibilities and liabilities that provide for the protection of consumers" and that "the Payment Card Industry has already established minimum data security standards."[68] The New Jersey law was more robust in that it "could potentially impose liability on any business or government agency that experienced a data security breach involving personal information."[69]

Finally, some data breach disclosure laws allow for a private right of action against an institution in the event of a data breach, as we discuss further below.

C. INFORMATION DISCLOSURE

Information disclosure policies, specifically data breach disclosure laws, work in indirect ways. The force of public notification, a form of light-handed paternalism, enables both consumers and firms to change their behavior and reduce losses. However, information disclosure competes with the stricter, more direct forms of legislation such as ex ante regulation and ex post liability.

Information disclosure as it relates to consumer privacy and data breaches is mainly achieved with the body of state data breach disclosure (or, security breach notification) laws. Currently, at least forty-five states require firms to disclose to consumers when their personal information has been lost or stolen.[70] These laws leverage two important principles, *sunlight as a disinfectant*[71]

---

65. *See* H.B. 213, 185th Gen. Court, Reg. Sess. (Mass. 2007).

66. Grant Gross, *U.S. Authorities Settle with TJX*, TECHWORLD, Mar. 31, 2008, http://www.techworld.com/security/news/index.cfm?newsid=11844. Other reports, however, identify the number of compromised accounts at over 100 million. Privacy Rights Clearing House, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Feb. 13, 2009).

67. Letter from California governor, Arnold Schwarzenegger, to the members of the California State Assembly, *available at* http://gov.ca.gov/pdf/press/2007bills/AB%20779%20Veto%20Message.pdf.

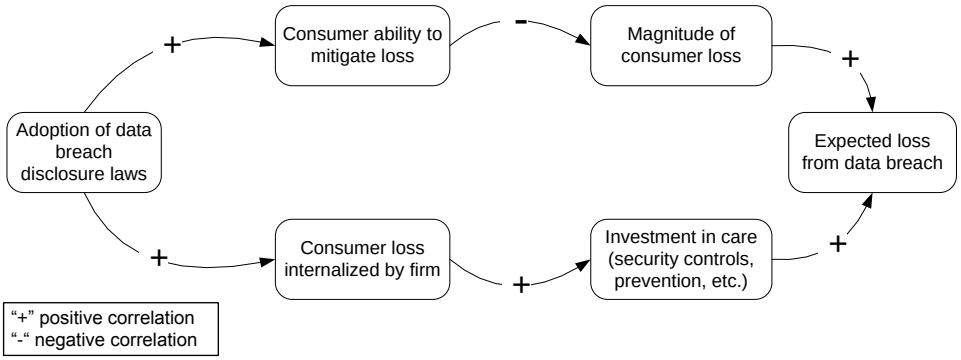
68. *Id.*

69. Gray, *supra* note 53, at 9.

70. *See* Posting to Perkins Coie Internet Case Digest, Missouri Becomes the 45th State to Enact Data Breach Notification Legislation, http://www.digestiblelaw.com/data security/blogQ.aspx?entry=6064&id=34 (July 20, 2009).

and *right to know*.[72] Consider Figure 4. First (upper path), as more states adopt disclosure laws, more consumers are notified, allowing them to take action to mitigate potential harm, such as identity theft. This system is entitled the "right to know." Next (lower path), as more states adopt the laws, more organizations are forced into the "sunlight," increasing the amount of consumer loss internalized by the organization, thus increasing their incentives to improve their security controls. Together, these effects should result in fewer breaches, reducing harm and leading to lower losses overall. The effect of public shame and embarrassment from breaches also contributes to the internalization of the loss.

Figure 4: Information Disclosure



Other statutes also provide for consumer notification in the event of a data breach, and a number of federal bills along similar lines have been written, though they have not passed.[73] For example, the Health Information

71. This phrase is originally attributed to Justice Louis Brandeis from his book. LOUIS BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 92 (1914).

72. DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 134 (2004), *available at* http://docs.law.gwu.edu/facweb/dsolove/Digital-Person (discussing "right to know" in the context of information privacy); WESLEY A. MAGAT & W. KIP VISCUSI, INFORMATIONAL APPROACHES TO REGULATION 1 (1992) (discussing "right to know" in the context of environmental regulation).

73. *See* Anne Shelby, *Pending Privacy and Data Security Legislation in the 110th Congress*, PRIVACY & SECURITY LAW BLOG, Mar. 30, 2007, http://www.privsecblog.com/2007/03/articles/federal-legislation/pending-privacy-and-data-security-legislation-in-the-110th-congress; Data Breach Notification Act, S. 239, 110th Cong. (2007), S. 139, 111th Cong. (2009); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007); Identity Theft Prevention Act, S. 1178, 110th Cong. (2007); Data Security Act of 2007, S. 1260, 110th Cong. (2007), H.R. 1685, 110th Cong. (2007); Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007), H.R. 2221, 111th Cong. (April 30 2009); Notification of Risk to Personal Data Act, S. 1350, 108th Cong. (2003), S. 115, 109th Cong. (2005), S. 751, 109th

Technology for Economic and Clinical Health Act (HITECH), part of the American Recovery and Reinvestment Act specifically addresses unauthorized disclosure of personal health information.[74]

III. THE IMPACT OF CONSUMER DATA PROTECTION LAWS

The judgment of the relative costs and benefits of the different legislative approaches we have presented in the previous Section remains nebulous. Since many of the laws described within this Article have only recently been adopted (or will soon be adopted), rigorously estimating their impact is sometimes impossible. Moreover, it is not always clear what metrics should be used to estimate their impact: Even when the stated function of the law may be clear (for instance, forcing firms to disclose breaches they suffered), the ultimate intent may be more ambiguous. Is the purpose of a data breach notification law to afford some level of protection to consumers' data by forcing firms to internalize consumers' losses, or simply to increase the amount of information available to consumer about the handling of their data? Is the legislature trying to fine-tune an "optimal" balance between the costs and benefits of data privacy and commercial flows of information, or trying to achieve a given standard of protection, independently of its economic trade-offs?

Against such background, below we attempt to provide some suggestive evidence for how each of the three legal mechanisms have impacted firms, consumers, data breaches, and the resulting harm from these breaches.

A. EX ANTE REGULATION

We begin by looking at the fines and sanctions that have been levied by regulatory agencies against firms for violating data protection regulations—in particular, the SEC and the FTC. To our knowledge, the SEC has imposed only one sanction against a company for failure to meet minimum standards of care. In July, 2008, the SEC fined LPL Financial $275,000 for shoddy se-

Cong. (2005), S. 1326, 109th Cong. (2005), H.R. 1069, 109th Cong. (2005), H.R. 5582, 109th Cong. (2006), S. 239, 110th Cong. (2007).

74. *See* James B. Wieland, *The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"): Congress Includes Sweeping Expansion of HIPAA and Data Breach Notification Requirements in the Stimulus Bill*, HEALTHCARE INFORMATION PRIVACY, SECURITY AND TECHNOLOGY BULLETIN, Feb. 19, 2009, http://www.ober.com/shared_resources/news/client_alerts/alert_health/alert_health_021909.html. Specifically, section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act, "HITECH") of the American Recovery and Reinvestment Act of 2009 discusses breach notification requirements. Pub. L. No. 111-5, § 13402, 123 Stat. 115, 227 (2009).

curity controls which led to a breach of consumer data and unauthorized trades.[75] In the settlement, the SEC stated, "[d]espite its being aware as early as 2006 that it had insufficient security controls to safeguard customer information at its branch offices, LPL failed to implement adequate controls, including some security measures, which left customer information at LPL's branch offices vulnerable to unauthorized access."[76]

As mentioned, the FTC has enforced sanctions, both pecuniary and privacy policy-driven ex ante, and also in response to a data breach, where harm may or may not have been directly attributable. For example, in *In re Eli Lilly*, the FTC alleged that Eli Lilly violated its own privacy policy by identifying subscribers' e-mail addresses in an e-mail related to Prozac.[77] The FTC settlement required that Lilly augment its security controls and practices.[78] In *In re Microsoft*, the FTC alleged that Microsoft violated its stated privacy policy of protecting users' information within their .NET Passport service and required them to develop a "comprehensive information security program" certified by an "independent professional every two years" for twenty years.[79] Overall, these cases provide some evidence that federal agencies such as the SEC and FTC can and do impose fines on firms that fail to meet certain standards of care for protecting consumer data.

Regarding PCI DSS, the total volume and actual fines imposed on firms from breaches of credit card data is unclear.[80] VISA claims that acquiring banks are subject to a $100,000 fine for not reporting a confirmed breach and a $500,000 fine for any of their merchants that suffer a breach while non-compliant.[81] In actuality, VISA reported levying fines against U.S. acquiring banks for $3.5M in 2005, $4.6M in 2006, and $11.5M in 2007.[82] In October of 2007, VISA began fining U.S. acquiring banks $25,000 for each

75. *See* SEC Exchange Act Release No. 58515, 7 (Sept 11, 2008), *available at* http://www.sec.gov/litigation/admin/2008/34-58515.pdf.

76. *Id.* at 4.

77. *In re* Eli Lilly, 133 F.T.C. 763, 767 (2002).

78. *Id.* at 784-85.

79. *In re* Microsoft Corp., 134 F.T.C. 709, 742 (2002). Other examples of FTC action ex ante include *In re* Petco Animal Supplies, Inc, 139 F.T.C. 102 (2005), and *In re* Guess?, 136 F.T.C. 507 (2003).

80. While it is the merchant who must demonstrate compliance with the PCI DSS standard, it is the merchant's acquiring bank that is subject to a fine by a credit card company. This is because only the acquiring bank has a direct relationship with the credit card company, not the merchant.

81. *See* VISA, *If Compromised*, http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html (last visited July 10, 2009).

82. *See* VISA, Keeping Electronic Payments Secure, *available at* http://www.corporate.visa. com/md/fs/security/security.jsp (last visited Feb. 21, 2008) (describing vendor compliance and fines levied by VISA).

Level 1 merchant that was non-compliant,[83] and MasterCard is allegedly fining Level 1 and 2 merchants $375,000 annually, and Level 3 merchants $150,000 annually for non-compliance.[84] In particular, VISA fined TJX's acquiring bank $880,000 for the retailer's non-compliance with the PCI DSS standards.[85] Recently, Heartland admitted that "a majority" of the $12.6 million paid in fees from its massive breach went to MasterCard.[86]

While the FTC and SEC clearly do not levy fines against all institutions that incur data breaches, they do act, if only against visibly egregious breaches of consumer data. Furthermore, there is a shortage of data regarding fines imposed for non-compliance of the PCI DSS standard. In short, it is difficult to draw robust conclusions.[87]

B. EX POST LIABILITY

Measuring the impact of an ex post liability policy is also difficult. Private actions brought by consumers against firms often employ negligence claims as a way to recover losses from data breaches. Some of the data breach disclosure laws do allow for private right of action in the event of a data breach. Often, however, courts dismiss negligence claims because of the plaintiff's inability to show actual damages as required by negligence tort claims. This economic loss rule makes it very difficult for plaintiffs to be compensated for strictly pecuniary losses under tort law.[88] These rulings generally establish that

---

83. *Id.* "Level 1" merchants are defined by VISA to be those that process more than 6 million credit card transactions per year. *See* VISA, Merchants, http://usa.visa.com/merchants/risk_management/cisp_merchants.html (last visited July 19, 2009) (describing the levels and their associated validation requirements).

84. Quarterly fines to level 2 merchants are allegedly $25K, $50K, $100K, $200K while quarterly fines to level 3 merchants are $10K, $20K, $40K, $80K. *See* Branden Williams, *MasterCard to Fine Merchants for Non Compliance*, BRANDEN WILLIAMS' SECURITY CONVERGENCE BLOG, http://blogs.verisign.com/securityconvergence/2009/07/mastercard_to_fine_merchants_f.php (last visited July 30, 2009). Level 2 and 3 merchants are those processing from 1–6 million and 20k–1 million transactions annually, respectively.

85. Ross Kerber, *Visa Fines Bank After Losses in TJX Breach*, BOSTON GLOBE, Oct. 29, 2007, at F1.

86. *See* Heartland Payment Systems, Inc., 6, http://www.sec.gov/Archives/edgar/data/1144354/000119312509107150/d10q.htm; Alex Goldman, *Heartland Hit With $12M Breach Tab*, INTERNET NEWS, May 8, 2009, http://www.internetnews.com/security/article.php/3819596 (citing that $6 million in fines went to MasterCard and $1 million to VISA).

87. Some argue that the actual fines imposed by the credit card companies on merchants are inconsequential compared to increases in transaction fees (called interchange fees).

88. For instance, in *Kahle v. Litton Loan Servicing LP*, the court ruled that, "any injury of Plaintiff is purely speculative" and dismissed the case claiming that the plaintiff "failed to establish an injury." 486 F. Supp. 2d 705, 712 (S.D. Ohio 2007). In *Forbes v. Wells Fargo Bank*, the court ruled that the "the plaintiffs' injuries are solely the result of a perceived risk of future harm." 420 F. Supp. 2d 1018, 1020 (D. Minn. 2006). In *Key v. DSW Inc.*, the court ruled

"unless you have an actual showing of harm as a victim of identity theft, potential harm will not suffice."[89]

Not surprisingly, individuals are also unable to recover costs from efforts to reduce potential identity theft. The Seventh Circuit in *Pisciotta v. Old National Bancorp* did not believe it was reasonable for the company to pay identity theft monitoring services for its consumers because "had the Indiana legislature intended that a cause of action should be available against a database owners for failing to protect adequately personal information, we believe it would have made some more definite statement of that intent."[90] In *Forbes v. Wells Fargo Bank*, the court also explained that costs involved in "expenditure of time and money were not the result of any present injury, but rather the anticipation of future injury that has not materialized."[91] The court ruled similarly in *Kahle v. Litton Loan Services* stating that the case "clearly reject[s] the theory that a plaintiff is entitled to reimbursement for credit monitoring services or for time and money spent monitoring her credit."[92] Yet, consumers continue to try to bring actions for data breaches, for instance, against Starbucks,[93] Heartland,[94] Hannaford Bros,[95] and RBS WorldPay.[96]

---

that the plaintiff's "potential injury is contingent upon her information being obtained and then used by an unauthorized person for an unlawful purpose." 454 F. Supp. 2d 684, 689 (S.D. Ohio 2006). In *Randolph v. ING Life Ins. & Annuity Co.*, the court stated that the plaintiffs failed to demonstrate that any damages were "actual or imminent, not conjectured or hypothetical" and therefore dismissed the claim, charging that "the plaintiff's allegations therefore amount to mere speculation that at some unspecified point in the indefinite future they will be victims of identity theft." No. 06-1228, 10 (D.D.C.Feb. 20, 2007); *see also* Guin v. Brazos Higher Educ. Serv. Corp., No. 05-668, 2006 U.S. Dist. LEXIS 4846, at *10 (D. Minn. Feb. 7, 2006). In *Giordano v. Wachovia Sec., L.L.C.*, the court stated that, "a plaintiff must allege an actual injury or that an injury is so imminent as to be 'certainly impending.' " No. 06-476, 2006 U.S. Dist. LEXIS 52266, 11 (D.N.J. July 31, 2006).

89. Michael Santarcangelo & Patrick Romero, *Do Data-Breach Laws Give You The Power to Hold Corporations Liable?,* SECURITY CATALYST, Nov. 1, 2007, http://www.securitycatalyst.com/do-data-breach-laws-give-you-the-power-to-hold-corporations-liable-2/. Most recently, in *Ruiz v. Gap*, the U.S. District court for the Northern District of California held that an increased risk of identity theft was sufficient for a plaintiff to establish standing but insufficient to maintain a negligence claim. 2009 WL 941162 (N.D. Cal. Mar. 24, 2008); *see* Hogan & Hartson, *Privacy and Data Security Briefing* at 8, June 2009, http://www.hhlaw.com/files/Publication/1f6d3cbc-6ad2-4d0a-a4ca-4fcf4a04b891/Presentation/PublicationAttachment/8dee823c-f6d1-473b-a34f-d2c8407ed313/PrivacyBriefing.pdf.

90. Pisciotta v. Old Nat'l. Bancorp, 499 F.3d 629, 637 (7th Cir. 2007).

91. *Id.* at 55; *see Forbes*, 420 F. Supp. 2d at 1020.

92. *Kahle*, 486 F. Supp. 2d at 711. In *Kahle*, the court ruled that "any injury of Plaintiff is purely speculative" and dismissed the case, claiming that the plaintiff "failed to establish an injury." 486 F. Supp. 2d at 710.

93. Robert McMillan, *Starbucks Sued After Laptop Data Breach*, PC WORLD, Feb. 23, 2009, http://www.pcworld.com/article/160042/starbucks_sued_after_laptop_data_breach.html.

Others take a more creative approach by considering alternative legal arguments, such as medical cases that allow damages for monitoring one's health after being exposed to toxic chemicals.[97] However, it is questionable whether these arguments have legal standing. In *Stollenwerk v. Tri-West Healthcare Alliance*, the district court dismissed a claim that used health analogies (i.e. "toxic torts") because in such cases there is potential for actual (physical) harm.[98] Here, the court stated that "despite findings that identity theft results in more than purely pecuniary damages, including psychological or emotional distress, inconvenience, and harm to his credit rating or reputation, as a matter of law identity theft and credit monitoring must still be differentiated from toxic torts and medical monitoring."[99]

Defending the condition of causality has also been problematic for plaintiffs. Consider a consumer who shops at three competing retail stores using his customer loyalty cards.[100] Quite often, loyalty card applications require the consumer's social security number in order to perform a credit check. Consider then that he receives a breach notification from two of the three companies, and that sometime shortly after, he notices a new loan application (with charges!) on his credit report. He has just become a victim of identity theft. But was it because of these breaches or from something else? Even if he could link the source of the fraudulent application to one of the two companies, from which one exactly did the criminal steal his information? This is precisely what he must prove.

In summary, while consumers do appear to suffer losses as a result of data breaches (whether they be financial, psychological, or expenditures for prevention of future harm), such harms have yet to be fully recognized by

---

94. Elinor Mills, *Heartland Sued over Data Breach*, CNET NEWS, Jan. 28, 2009, http://news.cnet.com/8301-1009_3-10151961-83.html.

95. Trevor Maxwell, *Judge tosses all but one Hannaford data breach claim*, PORTLAND PRESS HERALD, May 13, 2009, http://pressherald.mainetoday.com/story.php?id=256153.

96. Robert Lemos, *Data-breach Lawsuit Follows $9 Million Heist*, SECURITY FOCUS, Feb. 06, 2009, http://www.securityfocus.com/brief/903.

97. Chandler, *supra* note 7.

98. Stollenwerk v. Tri-West Healthcare Alliance, No. 03-0185PHXSRB, 2005 U.S. Dist. LEXIS 41054 (D. Ariz. Sept. 8, 2005), *aff'd*, 254 Fed. Appx. 664 (9th Cir. 2007); *see also* Posting of David Navetta to InfoSec Compliance Blog, Stollenwerk v. Tri-West Health – Rise of the Phoenix?, http://infoseccompliance.com/2008/01/04/stollenwerk-v-tri-west-health-%e2%80%93-rise-of-the-phoenix/ (Jan. 4, 2008) (reviewing the case as well as a recent appellate ruling (9th Cir. Nov. 20, 2008) which upheld the lower court's ruling regarding the "toxic tort" claim).

99. *Id.* at 6.

100. The loyalty card, recall, provides the consumer with discounts and special promotions in exchange for his personal information and acceptance of the firm monitoring his shopping habits.

the court system. However, in situations with tangible losses and clear causation, the breached-against party can recover.[101]

C. INFORMATION DISCLOSURE

Above, we presented anecdotal and suggestive evidence regarding the impact of regulation and liability in terms of consumer data protection. In this Section we present evidence of the impact of information disclosure in regards to firm and consumer behavior. Some have tried to determine how the laws have changed organizations' behavior. The authors of a recent study interviewed corporate executives and found that companies are, indeed, improving their practices.[102] Specifically, the laws "empowered [the Chief Security Officers] to implement new access controls, auditing measures, and encryption," and increased awareness within the companies of the importance of information security.[103] There is also evidence to support the belief that disclosure laws can reduce the costs of identity theft, because the sooner one is notified of potential harm, the more quickly one can take action to prevent losses.[104]

Another potential outcome of the notification laws is that public disclosure (the sunlight effect) of a data breach could have a material effect on consumer behavior. Indeed, two surveys suggest that 21%[105] and 19%[106] of respondents claimed to have ceased relationships with the company that suf-

---

101. For example, TJX recently settled with VISA for $41 million for the cost of replacing credit cards. Linda McGlasson, *TJX, Visa Agree to $40.9 Million Payout for Data Breach*, BANK INFO SECURITY, Dec 4, 2007, http://www.bankinfosecurity.com/articles.php?art_id=648.

102. SAMUELSON LAW, TECHNOLOGY, & PUBLIC POLICY CLINIC, UNIVERSITY OF CALIFORNIA-BERKELEY SCHOOL OF LAW, SECURITY BREACH NOTIFICATION LAWS: VIEWS FROM CHIEF SECURITY OFFICERS (2007).

103. *Id.* at 4.

104. SYNOVATE, FEDERAL TRADE COMMISSION: 2006 IDENTITY THEFT SURVEY REPORT 24 (2007) [hereinafter SYNOVATE] (finding that: (1) 30% of those who discovered that their personal information was being misused 6 months or more after it started had to spend $1,000 or more, compared to 10% of those who found the misuse within 6 months; (2) 69% of those who discovered the misuse within 6 months spent fewer than 10 hours compared to 32% of those who took 6 months or more to discover it; and (3) 31% of those who discovered the misuse of their information 6 months or more after it started reported that the thief obtained $5,000 or more, compared to 10% of those who found out in less than 6 months). Other reports provide similar qualitative findings. *Id. at* 8; JAVELIN STRATEGY & RESEARCH, 2009 IDENTITY FRAUD SURVEY REPORT: CONSUMER VERSION 9 (2009), *available at* http://www.idsafety.net/901.R_IdentityFraudSurveyConsumerReport.pdf.

105. Ellen Messmer, *Data Breaches Hurt Corporate Image but Don't Necessarily Drive Customers Away*, NETWORK WORLD, Aug. 29, 2007, http://www.networkworld.com/news/2007/082907-data-breaches-hurt-corporate-image.html?page=1.

106. PONEMON INSTITUTE, NATIONAL SURVEY ON DATA SECURITY BREACH NOTIFICATION 4 (2005).

fered a data breach. A note of caution, however, is that results obtained through customer surveys can be more reflective of *intended* rather than *actual* behavior.

Some research efforts have also focused on estimating the cost of a data breach to both firms and consumers. For instance, a recent study found that the average cost to a firm from a data breach has been increasing steadily since 2005 ($4.54M in 2005, $6.35M in 2007, $6.65M in 2008).[107] The study calculates totals by aggregating costs of investigation, notification, legal fees, consumer redress (and services such as credit monitoring or reimbursement of credit cards) and customer churn. In fact, the study claims that the majority (69%) of total costs in 2008 was due to lost business, and this percentage increased relative to 2007 and 2006 (65% and 54% of total costs, respectively).[108] If true, this suggests that consumers are indeed punishing firms for data breaches.

However, another recent empirical study attempted to measure the effect of data breach notification laws on identity theft. Using reported identity theft data from the FTC from 2002–2007 and a variation of adoption of data breach disclosure laws across U.S. states, the researchers found that adoption of disclosure laws reduced identity theft by about 2%, though this is only a marginally statistically significant level.[109] Meanwhile, despite increased adoption of data breach disclosure laws, identity theft also appears to be increasing. According to the FTC, reported cases of identity theft have been steadily increasing since 2000 with almost 314,000 consumer complaints in 2008.[110] Another report shows an increase of 8.6% in identity fraud victims in 2008 over the previous year.[111]

In summary, while robust, empirical evidence regarding data breach disclosure laws is minimal, these early studies provide some evidence that the laws may be affecting firm and consumer practices, but only have a marginal effect on identity theft due to breaches.

---

107. PONEMON INSTITUTE, 2008 ANNUAL STUDY: COST OF A DATA BREACH 11 (2009).

108. *Id.* at 12.

109. Sasha Romanosky et al., Do Data Breach Disclosure Laws Reduce Identity Theft? (Sept. 16, 2008) (unpublished article, on file with the Berkeley Technology Law Journal), *available at* http://ssrn.com/abstract=1268926.

110. FTC, CONSUMER SENTINEL NETWORK DATA BOOK 5 (2008). 2006 was the only one year that saw a decline in reported cases (246k down from 256k in 2005, a change of 3.7%). Note that this report reflects total identity theft complaints, only some of which are due to data breaches.

111. *See* JAVELIN, *supra* note 104, at 18. However, the number of 2008 victims (487) is lower than in 2003 (514). This survey also estimates that 11% of identity fraud is due to data breaches while another 11% is due to "online activity." *See* Figure 2 *infra.*

D. DISCUSSION

Though it may be difficult to express a reliable valuation of the impact of these three policy interventions, it is fair to say that their impact has been, at best, mixed.

We can reasonably conclude that the state data protection laws and self-regulations (PCI DSS) are building a foundation for a stronger duty of care for firms to adequately protect consumer information. However, the existence of a relatively small number of sanctions by the FTC, SEC, and the credit card companies, as well as the rising number of reported data breaches,[112] suggest that firms continue to fail in this duty.

Moreover, it appears that these policies have not been subject to rigorous scrutiny, because the legal initiatives are so new, because there is a dearth of reliable quantitative data, or because few attempts have been made to empirically estimate their effects. As mentioned above, it is also not clear what should be the appropriate metric by which to estimate their impacts. Even when the legislature's intention may, at first glance, seem transparent (i.e. defend consumers' privacy), the actual objective may be more ambiguous. For instance, is the objective of data breach notification laws to decrease the instances of identity theft, to decrease the amount of damage they cause on average, to improve firm practices, or all of the above?

Next, we will provide a brief economic analysis of each of these policy approaches in order to offer insight into the conditions under which they become more (or less) effective.

IV. THE ECONOMIC ANALYSIS OF EX ANTE SAFETY REGULATION, EX POST LIABILITY, AND INFORMATION DISCLOSURE

Above, we illustrated the causal mechanisms upon which ex ante safety regulation, ex post liability, and information disclosure rely, and we discussed their limited impacts. Now, we ask the question: given the choice, which policy approach would a social planner (e.g. regulator, government, policy maker, etc.) implement? While companies and consumers will naturally lobby to minimize their own private costs, the social planner's goal is to minimize *the sum* of these costs.

We leverage the economic analysis of accident law and define cost equations for two economic agents: the firm (injurer) and the consumer (victim),

112. See the annual statistics on reported data breaches from DatalossDB. DataLossdb.org, Data Loss Statistics, http://datalossdb.org/statistics (last visited Apr. 30, 2009).

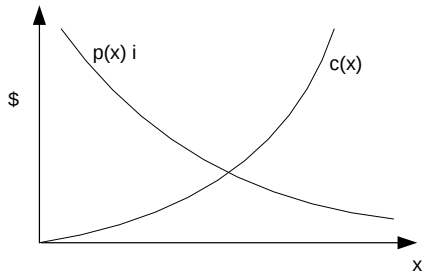
and determine how their costs are affected by each policy approach. The social planner's cost function, therefore, is simply the sum of firm and consumer costs. While they are abstractions from reality (and therefore necessarily inaccurate), these models are useful to understand how incentives and liabilities drive agents' behavior.

First, we will write equations that reflect the simple mechanism of each policy approach, what we will call the "basic equations." This first step will help us understand how these policies operate in an ideal situation. Next, we identify and discuss inefficiencies of each policy—practical conditions under which the policies deviate from theory. Finally, we will update the basic models to reflect these inefficiencies in order to better understand how firms and consumers *actually* behave, what we will call the "extended equations."

A. GENERAL FORMS

Consider a firm that faces the threat of a failure in its product or service (for instance a data breach or environmental pollution) which could harm its consumers. The firm can invest in some level of care, x, to avoid such harm, but the cost of this care, c(x), increases with investment. However the probability of the accident, p(x) and thus the expected harm p(x)i (calculated as the probability multiplied by i, the cost of investigating the cause of the accident) decreases with investment, as shown in Figure 5.[113] The firm's strategic decision is to determine in how much care they should invest in order to minimize their total private costs.

Figure 5: Basic cost functions



Therefore, one might write the firm's loss equation as:

113. The X axis in Figure 5 represents the level of investment in care (security controls) and the Y axis represents cost. As is commonly portrayed, the cost of care, c(x), becomes increasingly steep, implying that it costs more to protect something the more one has already invested. Similarly, the change in probability of an accident occurring, p(x), declines as one invests more in care.

$$\text{Firm loss} = c(x) + p(x)\, i \qquad (1)$$

where, x, c(x) and p(x) and i are as described above. In the event of an accident, consumers may suffer losses and so we can write their loss function as:

$$\text{Consumer loss} = p(x)\, h \qquad (2)$$

where h is the total consumer harm. Finally, the total social loss is composed of both consumer and firm loss:

$$\text{Social loss} = c(x) + p(x)\,[i + h] \qquad (3)$$

Recall that in our model, the decision variable is x, the level of care taken by the firm. Therefore, the objective of the social planner is to achieve a value of x that minimizes equation (3), because social costs are lowest when the firm invests in the socially optimal level. In order to have the firm invest at this level, it must internalize the full amount of its harm.[114] However, since firms are motivated (only) by their own private costs, they invest in a level of care that minimizes (1), not (3), which is always less than socially optimal.[115]

Together, these three equations define our system and the losses to each party, absent any legal intervention. Next, we show how the equations can be modified to reflect ex ante safety regulation, ex post liability, and information disclosure. Note that economic models for regulation and liability have already been explored by a number of scholars, so we present general forms of their results below in an attempt to build upon, not repeat, existing work.[116]

---

114. In familiar economic terms, the social planner wishes to increase the level of care (x) until the marginal cost of the next "unit" of prevention equals the marginal benefit from that unit. That is, until the incremental benefit from one more unit is perfectly offset by the cost of that additional unit. If the firm's cost function is the same as equation (1), then the firm would choose to invest in the same level of care as that desired by the socially planner (i.e. the socially optimal level). An important note, of course, is that the social planner is not choosing to *minimize* accidents, but *optimize* them. This is achieved by minimizing the sum of firm and consumer loss, as seen in equation (3).

115. The concept of an entity not bearing the full cost of their actions (i.e. an externality) is fundamental to microeconomic theory. *See generally* LANDES & POSNER, *supra* note 32 (discussing externalities as applied to tort law).

116. *See id.*; Steven Shavell, *Economics and Liability for Accidents*, (John M. Olin Center for Law, Economics, and Business Discussion Paper No. 535); Kolstad et al., *supra* note 33, at 890.

1. Ex Ante Safety Regulation

Under ex ante safety regulation, the social planner must set a standard of care that is constant for all firms no matter their risk of harm. Hence the total cost to society becomes:

$$\text{Social loss} = c(s) + p(s)\,[i + h] \tag{4}$$

where s is a mandated standard that holds the social cost constant with any change in care, x.[117] Firm and consumer costs are similarly given by:

$$\text{Firm loss} = c(s) + p(s)\,i \tag{5}$$

$$\text{Consumer loss} = p(s)\,h \tag{6}$$

2. Ex Post Liability

Finally, ex post liability allows compensation to victims for harm caused by firms. In effect, this causes a transfer of cost from the injurer to the injured.[118] However, prior analysis reveals a more complicated form that recognizes how a firm's total cost is reduced because of some probability of evading lawsuit:[119]

$$\text{Firm loss} = c(x) + p(x)\,[i + \alpha\, h] \tag{7}$$

$$\text{Consumer loss} = p(x)\,[1 - \alpha]\,h \tag{8}$$

$$\text{Social loss} = c(x) + p(x)\,[i + h] \tag{9}$$

Where α effectively captures the probability of being held liable for damages and the portion of consumer harm internalized by the firm ($0 < \alpha <$

117. Given a distribution of harm across all firms, and absent better information, the regulator must choose a level of care that reflects the average amount of harm. Its objective, then, is to determine the level of care that minimize $c(s) + p(s)\,E(h)$, where $E(h)$ is the expectation operator that represents the average level of harm. *See* Shavell, *Model*, *supra* note 33, at 273.

118. We have generalized the type of liability by not specifying negligence versus strict liability. However, in general, privacy harms are best dealt with using negligence liability for which a firm is held liable if they invest in a level of care lower than the standard of care (due care).

119. *See* Shavell, *Model*, *supra* note 33, at 273 (defining the firm's loss function). The social loss function remains unchanged from Equation 3. The difference is simply in how costs are partitioned between injurer (firm) and injured (consumer). Shavell also considers cases where the firm faces the potential for bankruptcy (judgment proof). However, given the extreme rarity of such cases due to data breaches, we will ignore this complexity.

1),[120] and h is again total consumer harm. The consumer loss is then a function of the probability of harm and the remaining cost not paid by the firm.

3. Information Disclosure

As discussed, information disclosure creates two important incentive devices. First, information about potential harms allows consumers to take action to reduce their loss (e.g., notify banks and credit card companies, close accounts, check credit reports, etc.). Second, consumers are also empowered to force firms to internalize some of their loss by "punishing" them for bad practices.[121] Modifying equations (1) and (2) as shown below represents these changes:

$$\text{Firm loss} = c(x) + p(x)\,[i + \lambda\, h(e)] \qquad (10)$$

$$\text{Consumer loss} = p(x)\,[1 - \lambda]\, h(e) \qquad (11)$$

$$\text{Social Loss} = c(x) + p(x)\,[i + h(e)] \qquad (12)$$

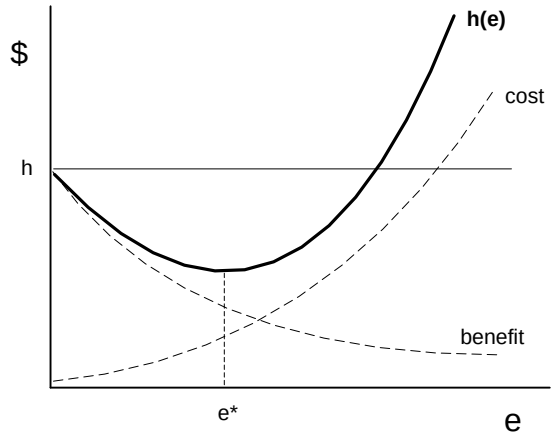
where λ is the amount of consumer loss internalized by the firm ($0 < \lambda < 1$), and the remaining portion, $1 - \lambda$, is that which is born by the consumer.

Further, consumer harm is no longer a constant (h), but becomes a function of consumer action, e. Naturally, we recognize that any action incurs both cost and benefit, and therefore the consumer's strategic decision is to invest in a level of care that minimizes their harm. Total consumer harm, h(e), therefore, is the sum of the dashed cost and benefit curves as shown in Figure 6.

120. As α approaches 1, the company becomes more liable. A value of 1 would imply that the company is always liable (strict liability), whereas a value of 0 would imply that the company always evades lawsuit.

121. For example, they can stop purchasing goods or services from the merchant, sell its stock, or publicly communicate their negative experiences to potential customers. We make the assumption that consumer action affects the *magnitude* of their loss as opposed to the *probability* of the harmful event occurring. These assumptions could easily be relaxed but at the expense of increased complexity and without additional insight. The ability for an individual to contribute in reducing their harm is also known as bilateral care. *See* Shavell, *supra* note 32, at 182 (where both injurers and potential victims are able to affect the probability, not magnitude of harm). And so a characteristic of information disclosure policies is to transform unilateral-care accidents into bilateral-care accidents.

Figure 6: Consumer harm



At small levels of consumer action, the marginal benefit is greater than the marginal cost. Conversely, for very large levels of care, the cost greatly outweighs any benefit. Importantly, there will be a point somewhere in between where the incremental gain from one additional unit of action is perfectly offset by the cost. This point is depicted as e* and represents the optimal level of consumer action.[122]

4. Discussion

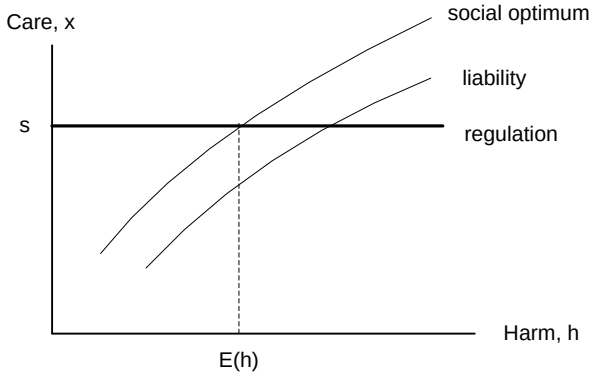
We are now able to provide some initial analysis and comparison between these policy approaches in order to understand whether, at this basic level of analysis, these interventions would incentivize firms and consumers to behave optimally. Two important questions arise: (1) do firms now have incentive to invest in the socially optimal level of care?; and (2) which policy approach ensures the lowest social cost?

First, regulation and liability can be compared against the basic model with regard to care as a function of harm as shown in Figure 7.[123]

122. For the purpose of this model, we assume that h(e=0) = h. That is, the amount of consumer harm from no consumer action is equivalent to h, the level of harm absent disclosure legislation. The distinction between absolute and marginal cost/benefit curves is this: absolute curves depict the total cost or benefit (measured in dollars) of consumer action. Marginal curves, however, depict the incremental change in cost or benefit from one more "unit" of care. Also, note that e* is achieved at the intersection of the *marginal* cost and benefit curves (not shown), not absolute cost and benefit curves as shown in Figure 6.

123. Shavell, *Model*, *supra* note 33, at 275.

Figure 7: Level of care for regulation, liability and social optimum



Given that the level of prevention (x) should reasonably increase with harm,[124] it is clear that the level of care taken by the firm under liability will always be less than is socially optimal for any given amount of harm, h, because of the probability of evading lawsuit. Inefficiencies could also exist in liability because of asymmetric information between legislators, firms, and consumers. For example, in negligence rulings, courts and juries need to compare the level of due care to the injurer's actual level of care. Errors in either establishing the proper standard of care or in the court's estimation of an injurer's level of prevention would result in an inefficient outcome, further reducing α.[125] However, because liability "harnesses the information that victims have about the occurrence of harm," ex post liability may be preferred when consumers, rather than the State, have better information about the impact from harmful activities.[126] Liability may also enjoy lower administrative costs than ex ante safety regulations because the costs are incurred only when harm is demonstrated.[127] Nevertheless, costs arise from each lawsuit and include legal expenses and time for both plaintiffs and defendants. Some even claim that administrative costs can be at least as large as the fines paid from a liability settlement.[128]

As expressed, regulation enforces a constant level of care that becomes socially optimal only at the average level of harm, E(h). The critical assump-

124. That is, the more harm a company is likely to cause, the more prevention measures they should take.

125. Polinsky & Shavell, *supra* note 32.

126. Shavell, *supra* note 116.

127. Though it is not clear whether strict or negligence liability is more efficient. *See id.*

128. *See* Shavell, *supra* note 32, at 281 (describing how administrative costs can be at least equal to the amount awarded to plaintiffs); LANDES & POSNER, *supra* note 32, at 58 (describing how almost 2/3 of every dollar awarded is paid in administrative expenses).

tion is that firms are homogeneous in their likelihood of causing harm. However, this becomes inefficient because it enables high risk firms (those that are more likely to cause harm) to under-invest in care and forces low risk firms (those that are less likely to cause harm) to invest more than they should.[129]

It can be shown that when firms do not suffer the full cost of their harm, they will under-invest in care. That is, the level of care that best satisfies the firm will always be lower than the best social level. These results can be confirmed by observing the firm's loss equations, reproduced in Table 1 for convenience. Notice how the firm's losses are always less than society's.

Table 1: Basic loss equations

Policy Intervention	None	Regulation	Liability	Disclosure
Social loss	$c(x) + p(x)\,[i + h]$	$c(s) + p(s)\,[i + h]$	$c(x) + p(x)\,[i + h]$	$c(x) + p(x)\,[i + h(e)]$
Firm loss	$c(x) + p(x)\,i$	$c(s) + p(s)\,i$	$c(x) + p(x)\,[i + \alpha\, h]$	$c(x) + p(x)\,[i + \lambda\, h(e)]$
Consumer loss	$p(x)\,h$	$p(s)\,h$	$p(x)\,[1 - \alpha]\,h$	$p(x)\,[1 - \lambda]\,h(e)$

By examining the cost functions presented, inefficiencies are not simply a casual outcome of one of these approaches, but are *systematic to all* of them. In short, only in rare and extreme cases will any of these policy approaches be able to achieve the socially optimal outcome. Further, we see that for the same level of care, social loss is equivalent under the basic model (equation 3) and that of ex post liability (equation 9). Social loss for information disclosure (equation 12) will be lower for any e where $h(e) < h$ which would certainly be the case for $h(e^*)$ and implies that disclosure is much less effective if consumers do nothing to prevent possible harm. Finally, it is not immediately clear whether total costs from regulation (equation 6) would be higher or lower than other approaches, only that it is constant for any change in care, x.[130]

129. This raises the question of which characteristics of an organization (government agency, school, private company, etc.) would cause them to be lower or higher risk. A recent data breach study revealed that companies with between 11–100 and 1001–10,000 employees suffered the greatest percent of breaches (26% and 27% respectively) while companies sized between 101–1000 and 10,001–100,000 were breached 17% and 18%, respectively. Also, more than sixty percent of breached firms were from the retail (31%) or financial services (30%) industries. However, financial services firms suffered 93% of all records lost. *See* VERIZON BUSINESS, 2009 DATA BREACH INVESTIGATIONS REPORT 6-7 (2009) (sampling almost 600 breaches over the years 2004–2008).

130. To be clear, however, simply examining social costs across approaches *for the same level of care* is not sufficient. A proper analysis would require comparing social costs for each approach *given the firm's optimal level care*.

This Section presented a general discussion of economic models of ex ante safety regulation, ex post liability, and information disclosure. Regulation is efficient only for a single set of firms causing the average amount of harm; liability is efficient only when suits are always initiated and firms always pay for their harm; and information disclosure is efficient when firms bear all of the consumer harm and will reduce total social loss when consumers take action to reduce their harm. Next, we provide a more practical analysis of these approaches in a more specific context and identify how incentives, and therefore levels of care, would change.

B. INEFFICIENCIES IN CONSUMER DATA PROTECTION APPROACHES

This Section refines the previous economic analysis by discussing practical limitations of each of these legal interventions within the context of data breaches and consumer data protection.

1. Ex Ante Safety Regulation

Some scholars claim that regulation focuses on inputs rather than outputs—on prevention controls, rather than actual damage. That is, it enforces minimum standards of safety rather than penalizing injurers for the harms. The trouble is that there may be little correlation between a mandated standard and a decrease in harmful activity.[131] Thus, regulation raises costs to firms while failing to solve the problem.[132] Robert Smith echoes this conclusion:

> First, standards may bear no relationship to hazards in a particular operation, yet compliance (at whatever cost) is mandatory. Second, by requiring a certain set of safety inputs rather than by penalizing an unwanted outcome, such as injuries, the standards approach does not encourage firms to seek other, perhaps cheaper, ways of reducing injuries. Third, the promulgated standards are so numerous . . . and workplaces so diverse, that one must question how comprehensive or knowledgeable inspections can be.[133]

The implication, in the context of data breaches and personal data protection, is that regulations that require specific technologies such as data encryption may be misguided. One commentator argued that such efforts would create a "security floor" that may meet current needs but would soon

131. Cento Veljanovski, *The Economics of Law* 151 (Inst. of Econ. Affairs, Hobart Paper No. 157, 2006), *available at* http://ssrn.com/abstract=935952.

132. *Id.*

133. Robert S. Smith, *The Feasibility of an "Injury Tax" Approach to Occupational Safety*, 38 LAW & CONTEMP. PROBS. 730, 730 (1974).

be insufficient.[134] Moreover, data encryption, while possibly useful at preventing unauthorized access, would not affect the probability of a successful cyber-attack.[135]

In regards to PCI DSS, some claim that the fines may be driving "fine avoidance"[136] rather than improved security and that firms are "tick[ing] boxes without having any idea what they have answered"[137] in an attempt to avoid imposed fines due to non-compliance.[138] These comments reinforce the point that firms may only be driven to avoid legal or contractual penalties rather than improving the firm's security posture. The PCI DSS standards may also be creating a false sense of security. By abiding by a series of guidelines or commandments, firms cease to be proactive in protecting against future computer attacks, privacy violations and data breaches.[139]

However, ex ante safety regulation may be appropriate in some conditions. For instance, Kolstad et al. note that if the probability of a firm being held liable for damages is low enough (approaching zero), then ex ante safety regulation may provide one of the only remedies.[140] They explain that this might occur when there is a great deal of uncertainty associated with the harm, such as when the harm is "so new that those it affects and the consequences of the harm are unclear but suspected of being catastrophic", or when the level of accident costs borne is "so small that he or she might not even recognize it, even though many individuals are affected."[141] In a sense, this perfectly describes the duality of privacy harms (including identity theft) caused by data breaches. We have seen the great difficulty that consumers face when bringing negligence claims against firms for data breaches, in part

134. Posting of Ben Worthen to The Wall Street Journal: Business Technology, *Congress Moves on Data Security*, http://blogs.wsj.com/digits/2007/10/11/congress-moves-on-data-security (Oct. 11, 2007).

135. Encryption of stored data can be very useful at preventing unauthorized disclosure of confidential data, but does not, in and of itself, prevent the theft or acquisition of such data.

136. Evan Schuman, *PCI Fines: Nuisance Or A Ticket To ROI?,* STOREFRONT BACKTALK, Nov. 30, 2008, http://www.storefrontbacktalk.com/uncategorized/pci-fines-nuisance-or-a-ticket-to-roi/.

137. John Leyden, *Regulatory Compliance "Irrelevant" to Security: PCI DSS Credit Card 12 Commandments Standard Flawed*, THE REGISTER, Apr. 15, 2008, http://www.theregister.co.uk/2008/04/15/pci_dss_compliance/.

138. *Id.*

139. *Id.*

140. Kolstad et al., *supra* note 33, at 900.

141. *Id.*

because of the uncertainty regarding the prevalence and magnitude of harm.[142]

Finally, a very pragmatic justification for safety regulation is that monitoring a firm's security controls ex ante can be much easier than measuring harms ex post.[143] That is, it may be much easier for the social planner to monitor a firm's compliance with a standard than it is to quantify all possible costs from an accident. So while ex ante regulation may be an imperfect measure (predictor) of ex post harm, it can be preferable when determining ex post harm becomes more uncertain—which is often the case with data breaches and resulting identity theft.

2. Ex Post Liability

Legal scholars have argued that common law, and in particular, tort law, is a socially efficient means of reducing loss to injured parties.[144] Bagby argues that common law is "self-correcting" and that efficiency is achieved when bad rulings are appealed and overturned, creating new precedent, while efficiency is strengthened when good rulings that dissuade litigation are made.[145]

However, a challenge faced by the application of tort liability to data breaches and consumer data protection is the dichotomy between the economic and the legal interpretation of privacy costs. While tort law often ignores losses that are not actual or immediately realized, economic considerations of privacy costs are more promiscuous. From an economic perspective, the costs of privacy invasions can be numerous and diverse. The costs and benefits associated with information protection (and disclosure) are both tangible and intangible, as well as direct and indirect.[146] Direct costs are those

142. This is not to say that identity theft is not real or potentially devastating for some individuals. We merely highlight that specific harms *due to breaches* are, for the most part, difficult to quantify.

143. *See* Donald Wittman, *Prior Regulation versus Post Liability: The Choice between Input and Output Monitoring*, 6 J. OF LEGAL STUD. 208 (1977).

144. *See generally* LANDES & POSNER, *supra* note 32; Mark Geistfeld, *Efficiency, Fairness, and the Economic Analysis of Tort Law*, *in* THEORETICAL FOUNDATIONS OF LAW AND ECONOMICS 234 (Mark D. White ed., 2009) (discussing arguments supporting and refuting the justification for an "efficiency" approach to tort law).

145. JOHN W. BAGBY, COMMON LAW DEVELOPMENT OF THE CUSTODIAL DUTY OF INFORMATION SECURITY IN FINANCIAL PRIVACY RIGHTS 6, 8 (2007), *available at* http://faculty.ist.psu.edu/bagby/Pubs/CommonLawEfficiency-CustodyDutyInfoSecurity1.pdf.

146. *See generally* Robert Gellman, *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete* (Mar. 2002), *available at* http://epic.org/reports/dmfprivacy.pdf. However, some observers only focus on the presence, or lack of evidence, of monetary costs. P. H. RUBIN & T. M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION 45-46 (2001).

immediately realized, such as adverse price discrimination following the revelation of a consumer's personal taste and preferences.[147] Indirect costs are the potential harms from identity theft once personal data has been compromised. Both direct and indirect costs can be tangible and intangible: for example, the tangible monetary loss due to price discrimination and the intangible shame associated with having portions of one's life exposed to the public.

Most often, when personal data is compromised, different types of costs are combined together. For instance, the costs associated with identity theft include direct dollar losses as a result of the crime, and indirect losses associated with investigation, recovery and coping with the ramifications. Examples of indirect losses include: lost wages, lawyers' fees, higher interest rates, anxiety and inconvenience of being denied utility service, time expenditures and psychological stress of dealing with debt collectors, and the distraction of being subject to civil lawsuit or criminal investigation.[148]

To complicate things, costs associated with privacy invasions are often speculative and uncertain (they are probabilistic). After a data breach, a consumer's personal information *may* fall into the wrong hands and *may* then be used in manners that harm that consumer. For an economist, the difference between an actual and a possible cost is simply a matter of probability and uncertainty; in both cases, the breach of a consumer's data has heightened the *expected* costs—be they tangible or intangible—that he will suffer when and if his data is abused. Such ambiguity is, most of the time, unacceptable to the law.[149] As previously discussed, a plaintiff bringing a negligence action against a firm for a data breach is unlikely to recover damages for *future* or *potential* identity theft, which *may* have originated from the disclosure of their personal data. Furthermore, for a plaintiff, it is difficult to prove that the harm originated from a *particular* instance of data breach: the victim may not be even aware that his data was in the possession of a certain firm, may not know that his data has been breached, and may not be able to connect the harm born to the actual breach—since his data may have been available at the same time to many other merchants or third parties. Even worse, since the harm may take place long after the breach episode, the victim may have no practical way of recovering losses from the breached firm. These costs

147. Acquisti & Varian, *supra* note 12.

148. Katrina Baum, *Identity Theft, 2004*, *in* BUREAU OF JUSTICE STATISTICS BULLETIN (2006), *available at* http://www.ojp.usdoj.gov/bjs/abstract/it04.htm.

149. *See generally* Robinson, *supra* note 8 (regarding the difficulties of claiming damages for probabilistic harm); Wright, *supra* note 8 (discussing arguments by legal and economic scholars related to causation for probabilistic harm).

create challenges to the application of liability solution in the case of data breaches and data protection.[150]

3. Information Disclosure

As mentioned, information disclosure allows potential victims to take action to prevent harm. Data breach disclosure laws, for example, enable consumers to notify banks and credit agencies to help prevent the risk of identity theft. Moreover, they can provide valuable information to consumers and the marketplace about a firm's security posture. However, such mechanisms rely on the rationality of consumer behavior; specifically, that consumers are able to understand their risks and know exactly what actions to take and when, and that they can execute those actions without cost. The reality, however, is that consumers suffer from a number of behavioral biases and face a number of transaction costs that prevent or hinder their ability to reduce or avoid loss.

First of all, in the presence of a breach notification, a consumer may not recognize the proper course of action since it is not always clear what actions he should take. Magat and Viscusi argue that consumers do not always react rationally to information regarding a change in risk.[151] Thus, information must be properly conveyed so that consumers understand how to evaluate and use it.[152] How is it even possible for a consumer to compute the risk of a data breach notification for example? Even (or especially) if a consumer could compute such risks, consider the case where in response to a data breach, he chooses to punish a financial firm for faulty security controls by changing to a competitor. Ostensibly, he is reducing his risk of identity theft. Instead, however, he has now disclosed his personal information to another firm and actually *increased* his risk of future harm. In this case, a seemingly incentive-compatible action has had the opposite effect.

Second, the cost of acting may be too great. For example, transaction costs economics refers to the many forms of costs that can be incurred during a transaction.[153] A transaction can be the familiar exchange of goods or services,[154] a contract negotiation, an interaction with another person, or part

150. Solove, *supra* note 6, at 5.

151. WESLEY A. MAGAT & W. KIP VISCUSI, INFORMATIONAL APPROACHES TO REGULATION 17 (1992).

152. *Id.*

153. *See generally* Oliver E. Williamson, *Transaction-Cost Economics: The Governance of Contractual Relations*, 22 J.L. & ECON. 233 (1979).

154. The transaction costs involved in the exchange of goods are simply those incurred beyond the cost of the good, such as the time involved in traveling to a store, searching for a good, and waiting to pay.

of cognitive decision making.[155] For example, consider an individual who just received a data breach notification. They may incur transaction costs when calling the breached firm to obtain more information or when notifying banks and merchants to cancel transactions. Such costs may be greater than any perceived benefit—effectively (and unfortunately) hampering the intended impact of the legislation.

Third, disclosure laws rely implicitly on firm and consumer rationality: that consumers care and that firms know consumers care. But what happens when consumers aren't fully rational, or when firms do not care? Firms may not care when any negative consequence of ignoring the law is less damaging than the benefits of engaging in (and not disclosing) abusive data practices. More concerning, firms may not care if they notice that the marketplace does not react in a significant manner to abusive practices. Consider the results mentioned above indicating that companies subject to data breaches suffer stock market losses[156] and that their customers claim that they would cease relationships with a firm that suffered a data breach. The same results indicate that the stock-market losses are short-termed, while customers who claim to sever their relationship may not follow up on their threats. In fact, it is possible that the escalating number of data breaches reported in the media may create an effect of psychological *habituation*,[157] desensitizing both consumers and firms to their effects—and therefore minimizing the desired impact of notifications.

Furthermore, research in behavioral economics and behavioral decision making provides ample evidence that consumers are unable to conceive of all possible outcomes and risks of data disclosures.[158] Additionally, consumers have trouble with innate judgment biases, such as bounded rationality, rational ignorance, or hyperbolic discounting.[159] Expecting consumers to punish firms that violate their data, or expecting consumers to act upon the reception of breach notifications assumes a level of knowledge, expertise, alertness, and self-control that they may simply not have. For instance, Romanosky, Telang, and Acquisti consider that the effect of the data breach disclosure laws is a function of both firm and consumer action and they both

155. Such as the cognitive effort required to process available information, consider practical alternatives, and finally select a course of action.

156. Acquisti et al., *supra* note 14.

157. *See generally* Jonathan L. Freedman & Scott C. Fraser, *Compliance without Pressure: The Foot-in-the-Door Technique*, 4 J. PERSONALITY & SOC. PSYCHOL. 195 (1966).

158. *See generally* Colin F. Camerer & George Lowenstein, *Behavioral Economics: Past, Present, Future*, *in* ADVANCES IN BEHAVIORAL ECONOMICS 3 (2003).

159. Acquisti, *supra* note 13, at 3-5.

need to take responsibility to prevent breaches and resulting identity theft.[160] But consumers already have enough to worry about. A process akin to "rational ignorance"[161] may lead the consumer to willingly ignore the notification, or to avoid learning about—or acting on—it. Fewer than 10% of individuals whose data had been stolen by criminals availed themselves of the credit protection and insurance and monitoring tools in the Choicepoint breach.[162] Similarly, an FTC survey found that 44% of identity theft victims ignored breach notification letters.[163]

No doubt, information disclosure also imposes additional costs on firms too. These can include: (1) the financial cost of having to engage legal counsel, notify customers either by mail, phone, or public media; (2) establishing call centers and responding to customer inquiries; (3) providing customers redress such as credit monitoring or other identity theft prevention services; and (4) regulatory fines or other fees (such as to the FTC, SEC, or VISA/MasterCard for PCI DSS violations). We discuss a potential outcome of this in the next Section.

C. DISCUSSION

The previous Sections presented simple economic models for consumer, firm and social cost under the three policy interventions. We then highlighted practical limitations of each approach as they related to consumer data protection and data breaches.

We can now incorporate these limitations into our basic economic models and observe the outcomes. For instance, by considering these characteristics, would we now find that firms and consumers have more incentive to behave in a socially optimal manner? Would these result in lower social costs?

As discussed above, ex ante safety regulation focuses on inputs (specific security-enhancing technologies such as encryption), rather than outputs (the actual harm from data breaches). This implies that the firm's cost of care would remain unchanged, but now the probability of harm would be higher because care no longer perfectly corresponds to lower probability of harm. Equation (3) would then become:

---

160. Romanosky et al., *supra* note 109, at 16.

161. *See generally* Bryan Caplan, *Rational Ignorance vs. Rational Irrationality*, 54 KYKLOS 3 (2001).

162. Jon Brodkin, *Victims of ChoicePoint Data Breach Didn't Take Advantage of Free Offers*, NETWORK WORLD, Apr. 10, 2007, http://www.networkworld.com/news/2007/041007-choicepoint-victim-offers.html.

163. SYNOVATE, *supra* note 104, at 57.

$$\text{Social loss} = c(s) + \beta\, p(s)\, [i + h] \tag{13}$$

where $\beta\, p(s)$ represents the increase in the probability of harm, $\beta > 1$.

Next, ex post liability demonstrates inefficiencies because: (a) consumers incur direct and indirect costs from privacy invasions; (b) probabilistic harm is generally not compensable under tort law; and (c) plaintiffs filing negligence claims are often unable to demonstrate causality. The probabilistic and causation characteristics of privacy violations have already somewhat been captured in our model by the parameter α from equation (7) so a more accurate loss function would simply attenuate the value of α as α' where $\alpha' < \alpha$ (note that the social loss would remain unchanged):

$$\text{Firm loss} = c(x) + p(x)\, [i + \alpha' h] \tag{14}$$

Finally, information disclosure suffers from inefficiencies because: (a) consumers may not know what action to take in response to information; (b) transaction, direct, and indirect costs impose a barrier to consumer action; and (c) consumers may suffer from cognitive biases which impair their rational judgment of perceived risks. We also observed how disclosure imposes additional costs on firms, as shown below:

$$\text{Consumer loss} = p(x)\, \gamma h(e)\, [1 - \lambda] \tag{15}$$

$$\text{Firm loss} = c(x) + p(x)\, [i + d + \lambda\, \gamma h(e)] \tag{16}$$

$$\text{Social loss} = c(x) + p(x)\, [i + d + \gamma h(e)] \tag{17}$$

Consumer costs and biases could be accounted for by modifying $h(e)$ as $\gamma\, h(e)$, with $\gamma > 1$, while the cost to the firm from notification is reflected in d, with $d > 0$.

We now present the extended loss equations as shown in Table 2.

Table 2: Extended loss equations

Policy Intervention	Regulation	Liability	Disclosure
Social Loss	$c(s) + \beta\, p(s)\, [i + h]$	$c(x) + p(x)\, [i + h]$	$c(x) + p(x)\, [i + d + \gamma\, h(e)]$
Firm Loss	$c(s) + \beta\, p(s)\, i$	$c(x) + p(x)\, [i + \alpha' h]$	$c(x) + p(x)\, [i + d + \lambda\, \gamma\, h(e)]$
Consumer Loss	$\beta\, p(s)\, h$	$p(x)\, [1 - \alpha']\, h$	$p(x)\, [1 - \lambda]\, \gamma\, h(e)$

Could any of these policy interventions achieve a first-best outcome? Posed another way, under which conditions would the firm's loss function approach the social loss? Some scholars have already concluded that ex ante regulation and ex post liability could be used together to achieve better out-

comes than if each were used individually.[164] However, their results apply to very general cases and not to the context of data breaches and consumer harm.

While we have provided examples of ex post liability, evidence suggests that the current state of negligence liability is unable to compensate for consumer harms incurred from data breaches, implying an effective value of α (or α') close to zero. Financial institutions, on the other hand, are able to recover losses stemming from reissuing credit cards. This makes sense because in these situations, the conditions of (at least strict) liability are clear: causality from harm is apparent and the costs are tangible and physical (the payment card). The net result is that total social cost remains constant, but the effect on firm costs is unclear because while the firm is internalizing more costs incurred by financial institutions it is also avoiding more consumer costs.

Regulation, however, suffers from a very different symptom. Firms bear no consumer loss to begin with, and the inefficiency of inputs (investment in security measures) to outputs (reduction in breaches) only exacerbates the problem by requiring a standard of care greater than necessary in order to obtain the same total cost.[165] The net result is that social costs increase with β, the divergence between inputs and outputs. It may become impossible, therefore, for regulation to ever be used on its own to obtain a first-best option, despite its apparent ease of use.

In regard to information disclosure, one might consider the cost of notification to be a kind of tax imposed on the firm due to a breach. Moreover, recall how the socially optimal level of care is achieved when the firm internalizes all consumer loss. Thus, the more consumer loss internalized by the firm, the lower the disclosure "tax" would have to be in order for the firm to behave optimally. Conversely, the lower the consumer loss internalized by the firm, the greater the disclosure tax needs to be.

V. CONCLUSION

This Article analyzes personal data protection efforts in the United States through the lenses of three economic theories: ex ante safety regulation, ex post liability, and information disclosure. We have described evidence of their impacts and analyzed the mechanisms through which they operate using economic modeling. While these models are simplistic by design, they can

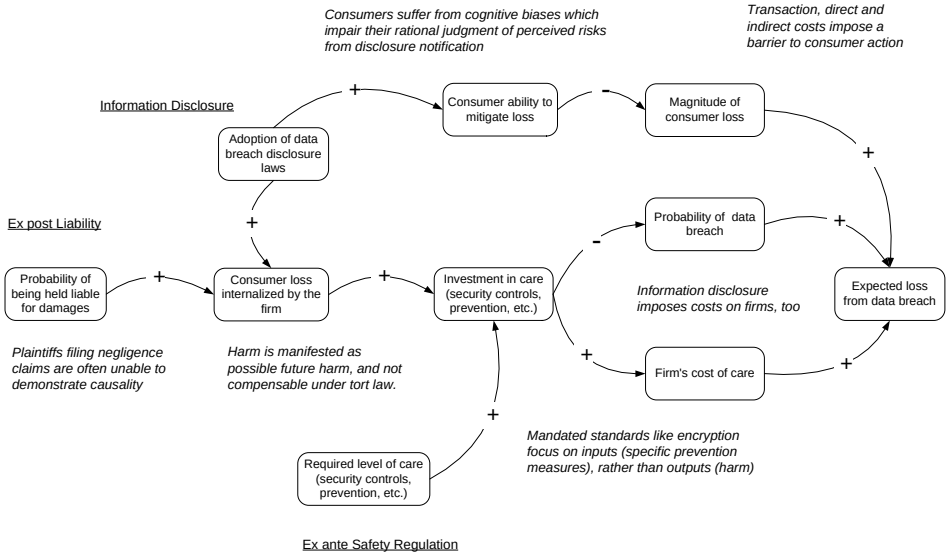
164. *See generally* Shavell, *Model*, *supra* note 33, at 271-80; Kolstad et al., *supra* note 33; Schmitz, *supra* note 33.

165. That is, the standard must be raised such that a probability of a breach offsets the inefficiency.

still be useful to clarify the costs and incentives that drive firm and consumer behaviors. We have also illustrated, both ideally and practically, how these legal mechanisms can suffer from inefficiencies, specifically with respect to data breaches and the protection of consumer data.

The policy mechanisms are illustrated together as we combine Figure 2, Figure 3, and Figure 4, as shown in Figure 8.

Figure 8: Legal mechanisms and their inefficiencies



Each of the policy approaches are underlined, while the inefficiencies are italicized. This figure illustrates the causal relationships between the policy approaches, their intended effects on firm and consumer behavior, and where major assumptions lie.

There are a number of reasons why the policy mechanisms addressed here may not be having a stronger effect. On one hand, they may simply not leverage the proper devices to allow injured parties to avoid or be compensated for loss. On the other hand, they may not be offering the proper incentives for firms and consumers to act either in their own best interests, or that of society. For example, under liability approaches, it becomes difficult for consumers to recover costs. In other cases, it is not clear what the best action is for consumers. What appears to empower them may, in fact, increase their chances of harm.

In conclusion, consider three main categories of costs associated with data breaches discussed in this Article: (1) those incurred by the breached firm itself; (2) those incurred by consumers; and (3) those incurred by financial institutions. Firms will respond naturally to private costs paid as a direct re-

sult of a breach (through investigation, attorney general settlements, and other regulatory sanctions) causing them to increase their care. In regard to costs incurred by banks due to their merchants' breaches, we have shown examples of how self regulation and new state liability laws are holding firms accountable. In this regard, the harm is clear, and so legislative efforts are effective. Alleviating consumer privacy harms, however, is most difficult. The harm is probabilistic and manifested as both direct and indirect, as well as a financial and psychological loss. It can be catastrophic for some, while inconsequential for others. And unfortunately, because reliable information regarding the cause, severity and volume of privacy violations is lacking, contemporary policy approaches appear ill-equipped to adequately prevent or mitigate consumer loss due to data breaches.

FEDERAL SECURITY BREACH NOTIFICATIONS: POLITICS AND APPROACHES

By Priscilla M. Regan[†]

TABLE OF CONTENTS

I. INTRODUCTION

Proposals for a federal security breach notification law have been on the congressional agenda since 2005 when numerous bills on this topic were introduced in the 109th Congress. In subsequent sessions, Senate and House committees have approved bills and sent them to the full chamber. For example, House Bill 4791, which requires federal agencies to notify individuals

† Department of Public and International Affairs, George Mason University.

if their personally identifiable information was compromised or accessed during a security breach,[1] passed the House by a voice vote in June 2008.[2] No stand-alone general security breach notification legislation has yet passed Congress, although some sector specific efforts have met success, including one specific to health records included in the 2009 stimulus bill[3] and one specific to Veterans Administration records.[4]

This Article analyzes a number of factors that hamper easy congressional agreement on the appropriate response to security breaches in the context of notification legislation. In particular, the controversy surrounding federal preemption, the policy goals of security breach notifications, the effectiveness of notification as a policy technique, and the scope of notification have impeded congressional efforts to pass a comprehensive breach notification law. Additionally, the Article discusses features of the relevant congressional policy processes, including partisan viewpoints on the issue and overlapping committee jurisdictions, which have also contributed to the difficulties in achieving congressional passage of security breach notification legislation.

The Article begins in Part II with a brief explanation of the history of security breach notification as an issue of congressional concern. Part III considers the issue of security breach notification in the context of information privacy legislation, identifying ways in which proposed policy approaches are similar to and different from information privacy policies generally adopted in the United States. In Part IV, the Article addresses the factors likely to affect the substance of congressional deliberations as well as the processes of those deliberations. Finally, in Part V, the Article assesses the likelihood for passage of general security breach notification legislation in the near term.

---

1. Federal Agency Data Protection Act, H.R. 4791, 110th Cong. (2007) (requiring the Director of the Office of Management and Budget to develop best practices for agencies to follow in conducting privacy impact assessments).

2. The Library of Congress, http://thomas.loc.gov/cgi-bin/bdquery/z?d110:HR04791:@@@L&summ2=m& (last visited July 11, 2009) (summarizing the legislation and detailing the legislative history). The House of Representatives passed House Bill 4791 on June 3, 2008 by voice vote and then referred to the Senate Committee on Homeland Security and Governmental Affairs. *Id.*

3. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, Div. A., Title XIII, § 13402, 123 Stat. 260 (codified at 42 U.S.C.A. § 17932).

4. Title IX of the Veterans Benefits, Health Care and Information Technology Act of 2006, Pub. L. No. 109-461, 120 Stat. 3403 (codified in scattered sections of 38 U.S.C.) (requiring the Department of Veterans' Affairs to issue regulations requiring notice to veterans when a data breach with a "reasonable risk" of misuse of data occurs).

II. EMERGENCE OF BREACH NOTIFICATION LEGISLATION AS A CONGRESSIONAL CONCERN

The need for a federal security breach notification law was made clear by a sequence of events involving large scale disclosures of personal data. A 2005 data security breach at ChoicePoint, a huge data broker with about 19 billion public and private records, placed the issue of security breach notifications on the congressional agenda.[5] The company disclosed in February, 2005 that it had sold the Social Security Numbers, addresses, and other personal data for approximately 145,000 people to impersonators of business owners.[6] This news was quickly followed by other similar disclosures of security breaches by the LexisNexis Group, Bank of America, and Citibank.[7] By the end of October, 2005, the Privacy Rights Clearinghouse had identified eighty data breaches in the previous eight months, involving the personal information of more than 50 million people.[8]

The scale of the problem and accompanying media attention, coupled with existing public and governmental concern about identity theft,[9] brought the breach issue to the attention of Congress beginning in 2005. When the problem of security breaches initially received congressional attention, there were three aspects of the issue that served to define the policy problem, and subsequently affected the politics of the issue.[10] These include: weaknesses in

---

5. Tom Zeller Jr., *Breach Points Up Flaws in Privacy Laws*, N.Y. TIMES, Feb. 24, 2005, at C1 [hereinafter Zeller, *Breach Points Up Flaws in Privacy Laws*].

6. *Id.*

7. Tom Zeller Jr., *Another Data Broker Reports a Breach*, N.Y. TIMES, Mar. 10, 2005, at C1 [hereinafter Zeller, *Another Data Broker Reports a Breach*]; Tom Zeller Jr., The Scramble to Protect Personal Data, N.Y. TIMES, June 9, 2005, at C1 [hereinafter Zeller, *The Scramble to Protect Personal Data*].

8. Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited June 4, 2009). Privacy Rights Clearinghouse continues to maintain this record of data security breaches with information available at: http://www.privacyrights.org/ar/ChronDataBreaches.htm.
Id.

9. Both the General Accountability Office (GAO) and the Federal Trade Commission (FTC) have a history of active interest in the issue of identity theft. *See*, *e.g.*, U.S. GEN. ACCOUNTING OFFICE, IDENTITY THEFT: PREVALENCE AND COST APPEAR TO BE GROWING, GAO-02-363 (2002); U.S. GEN. ACCOUNTING OFFICE, IDENTITY THEFT: GREATER AWARENESS AND USE OF EXISTING DATA ARE NEEDED, GAO-02-766 (2002); U.S. GEN. ACCOUNTING OFFICE, IDENTITY THEFT: SOME OUTREACH EFFORTS TO PROMOTE AWARENESS OF NEW CONSUMER RIGHTS ARE UNDERWAY, GAO-05-710 (2005); FTC Identity Theft website, http://www.ftc.gov/bcp/edu/microsites/idtheft/ (last visited June 1, 2009).

10. Public policy scholars have demonstrated that there are often a number of ways in which a policy problem can be defined and that the choice of a particular definition will then determine the interests that believe themselves to be affected by the policy, which then influences the politics surrounding that policy. *See*, *e.g.*, JOHN KINGDON, AGENDAS, ALTER-

the ways existing federal laws protected personally identifiable information; the diversity of data management practices contributing to data security breaches; and a state law in California that appeared effective in dealing with data security breaches.

First, the revelations about security breaches made clear that the existing set of federal laws governing personal information were ineffective both because they were framed in terms of sectors of the economy, and because their provisions for redress of grievances were cumbersome at best. Most relevantly, the Fair Credit Reporting Act of 1970, as amended various times including by the Fair and Accurate Credit Transactions Act of 2003, set rules for consumer credit agencies and bureaus, as well as consumers' access and rights with respect to their credit reports.[11] The Gramm-Leach-Bliley Act of 1999 established regulations and procedures for financial institutions,[12] although the definition of a financial institution was incomplete.[13] Additionally, a number of other sectoral rules set security standards for personally identifiable information but did not require security breach notification; these included the Health Insurance Portability and Accountability Act if medical records were involved,[14] and the Driver's Privacy Protection Act of 1994 if state driving records were compromised.[15] In all of these cases the burden to learn about possible misuses of personally identifiable information was on the individual who would likely only discover that his or her information had been compromised after a misuse occurred. And any redress of the harm took place after the fact.

This sectoral approach to the protection of personal information has been a cornerstone of the U.S. approach to information privacy, largely in response to individual industry arguments that their personal information

---

NATIVES AND PUBLIC POLICY 1-4 (1997); Theodore J. Lowi, *American Business, Public Policy, Case-Studies, and Political Theory*, 16 WORLD POLITICS 677, 677-15 (1964).

11. Fair Credit Reporting Act, Pub. L. No. 91-508 (codified as amended at 15 U.S.C. § 1681); Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified at 15 U.S.C. § 1681).

12. Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, Title V, 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801-6827).

13. Title V, § 509(3) (excluding from the definition of "financial institution" any entity subject to the jurisdiction of the Commodity Futures Trading Commission; the Federal Agricultural Mortgage Corporation or any entity operating under the Farm Credit Act of 1971; or other secondary market institutions).

14. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 29, 42, 16, 26 U.S.C.).

15. Drivers Privacy Protection Act of 1994, Pub. L. No. 103-322, Title XXX, § 300001, 108 Stat. 2099 (codified at 18 U.S.C. §§ 2721-2725).

needs and practices were unique and should not be uniformly regulated.[16] But in the wake of the 2005 security breaches, this feature of U.S. policy was roundly criticized. For example, an information security company executive noted that the patchwork of policies was too "industry-specific" and that the focus of regulation should be on the type of data rather than the industry.[17] As the executive stated, "A credit card number or Social Security number has the same importance, regardless of the industry handling it."[18]

Weaknesses in the sectoral approach were especially obvious in the retail area, which was not subject to any sector-specific law protecting consumers, but which collected and transferred vast and detailed amounts of personal data. Data breaches at T.J. Maxx and Marshalls, revealed in 2007, allowed hackers to access credit and debit card data, driver's license numbers, and names and addresses.[19] Security analysts pointed out that retailers tended to keep more data than was necessary and that senior managers often did not even know what data were being retained in systems based on old programming.[20] A senior counsel for the American Bankers Association noted that banks were then "left having to pay for the mistakes of retailers" to cover the costs associated with reissuing cards and for any losses as a result of fraud.[21] These gaps in sector-specific laws mean that the burden of security breaches is distributed unfairly on certain industries.

A second aspect of the security breach notification issue was that the diversity of data management practices highlighted the need for federal legislation. Organizations were using different mechanisms to transfer personally identifiable data. Examples range from the high tech, encrypted high-speed digital communication, to the low tech, unencrypted compact discs transported by couriers or delivery services.[22] The security breach at Citigroup in-

16. *See generally* PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977) (discussing the Commission's attention to private sector organizations' interest in keeping their records free from unreasonable government interference); PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES AND PUBLIC POLICY (1995) (discussing the complexity of records-generating relationships in modern industry).

17. Zeller, *Breach Points Up Flaws in Privacy Laws, supra* note 6, at C1 (quoting Joseph Ansanelli, chief executive and co-founder of Vontu).

18. *Id.*

19. Ellen Nakashima, *Customer Data Breach Began in '05*, *Retailer Says*, WASH. POST, Feb. 22, 2007, at D1.

20. *Id.*

21. *Id.* (quoting Nessa Feddis).

22. *See*, *e.g.*, Dave Lenckus, *Spotlight: Information Security*, BUSINESS INSURANCE, May 21, 2007, at 13; Jonathan S. Ziss, *Commentary: Accidents Happen; Know Your Responsibilities When Client Data Goes Missing*, ACCOUNTING TODAY, April 14, 2008, at 6. *See generally* Identify Theft Resource Center, Data Breaches, http://www.idtheftcenter.org/artman2/publish/

volved tapes of unencrypted data, which is a particular security risk.[23] One data security executive, who provides services for federal agencies, pointed out that one of the reasons why data are transported on tapes and by trucks is that the sizes of the data files are too large to be transmitted over an organization's Internet connection and that the creation of secure, dedicated networks is very expensive.[24] Relatedly, the data storage practices of organizations vary widely and thus can make it relatively easy for hackers to gain access to databases containing sensitive personal information.[25] The range of data handling practices was so diverse that it was clear that policy specific to a practice or technology would not provide an appropriate target of policy any more than a particular sector would be an appropriate policy focus.

Finally, there was an existing California state law that was relatively effective in dealing with security breaches. The California law required all organizations, regardless of sector, who experienced a data breach to take positive action notifying the people whose information was compromised by the breach.[26] The California law focused congressional attention on notification as the appropriate policy response to a security breach because California already required this response. For example, after the 2005 breach, ChoicePoint was required by state law to inform the residents of California whose information was involved in its data breach and, after the incident received much publicity, also informed residents in other states.[27] The ChoicePoint incident generated interest in other states to pass laws similar to that in California, and provoked industry interest in a uniform federal law which would simplify their compliance with different requirements and standards in vari-

---

lib_survey/ITRC_2008_Breach_List.shtml (last visited July 3, 2009) (archiving articles from 2005-2009 on data security breaches containing detailed information on the range of security practices used by companies in storing and transferring personally identifiable information).

23. Zeller, *The Scramble to Protect Personal Data*, *supra* note 7, at C1.

24. *Id.* (quoting Anthony A. Caputo, chief executive of SafeNet, a provider of encryption technology for high-speed networks).

25. *Id.*

26. California Security Breach Notification Act, A.B. 700, 2002 Leg., (Cal. 2002) (codified at Cal. Civ. Code §§ 1798.29, 1798.82). The act requires that

> [a]ny person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system . . . to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Id. See also James F. Brelsford, *California Raises the Bar on Data Security and Privacy*, FINDLAW, Sept. 30, 2003, http://library.findlaw.com/2003/Sep/30/133060.html.

27. *See* Zach Patton, *Stolen Identities*, GOVERNING, Aug. 2005, at 39.

ous state laws.[28] The California law thus provided a model policy response to breaches—notification—and set the starting point for the policy deliberations in Congress and for similar conversations in other state legislatures.[29] As of June, 2009, forty-four states had passed a security breach notification law.[30]

Following the ChoicePoint incident, almost twenty bills involving security breach notifications were introduced in the House and the Senate in the 109th Congress.[31] In the first session, three congressional committees held hearings.[32] Senate committees passed three bills,[33] and a committee report was issued for one bill.[34] In the second session, House committees reported three bills,[35] with an effort to reconcile differences between two committee

28. The Business Software Alliance in May, 2005 proposed a federal security breach notification law as federal regulation that would prevent the development of "an onerous regulatory environment" that would likely result from various state laws. Patience Wait, *Industry Executives Ask for New Notification Law*, WASHINGTON TECHNOLOGY, May 18, 2005, http://washingtontechnology.com/Articles/2005/05/18/Industry-executives-ask-for-new-notification-law.aspx?Page=1; *see also* Jacob Freedman, *Industry Seeks One Law on Data Breach Alerts*, 64 CONG. Q. WKLY. REP. 314, 314 (describing how a uniform breach notification law has become one of the top priorities for banks and other financial companies); *cf.* CONSUMERS UNION, NOTICE OF SECURITY BREACH STATE LAWS (2007), http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf (summarizing state laws as of August 2007).

29. Kathleen Hunter, *California law on ID theft seen as model*, STATELINE, Apr. 4, 2005, http://www.stateline.org/live/ViewPage.action?siteNodeId=136&languageId=1&contentId=22828.

30. Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota are the only six states not to have done so. For a listing of the states and relevant legislation, see National Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last updated May 26, 2009).

31. GINA STEVENS, CONG. RESEARCH SERV., CRS REPORT NO. RL33273, DATA SECURITY: FEDERAL LEGISLATIVE APPROACHES 5-13 (2008) [hereinafter DATA SECURITY].

32. These included the Senate Committee on the Judiciary; the House Committee on Financial Services; and the Subcommittee on Commerce, Trade, and Consumer Protection of the Senate Committee on Energy and Commerce. *Id.* at 1 n.2.

33. Notification of Risk to Personal Data Act, S. 1326, 109th Cong. (2005) (reported by the Senate Judiciary Committee on October 20, 2005); Identity Theft Protection Act, S. 1408, 109th Cong. (2005) (reported by the Senate Commerce, Science and Transportation Committee on December 12, 2005); Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong. (2005) (reported by the Senate Judiciary Committee on November 17, 2005).

34. S. REP. NO. 109-203 (2005) (reporting on S. 1408).

35. Data Accountability and Trust Act (DATA), H.R. 4127, 109th Cong. (2005) (reported by House Committee on Energy and Commerce on May 4, 2006); Financial Data Protection Act of 2005, H.R. 3997, 109th Cong. (2005) (reported by House Financial Services Committee on May 4, 2006); Cyber-Security Enhancement and Consumer Data Protection Act of 2006, H.R. 5318, 109th Cong. (2006) (reported by House Committee on the Judiciary on June 22, 2006).

bills failing.[36] Additionally, the 109th Congress passed a law in response to the data breach by the Department of Veterans Affairs that compromised personal information on 26.5 million veterans.[37]

The issue of data security breaches returned to the congressional agenda in the 110th Congress. During the first session, Senate committees favorably reported three bills[38] and committee reports were issued for two bills.[39] During the second session, the House passed a bill, by voice vote and under suspension of the rules, which established new requirements on federal agencies and required the Office of Management and Budget (OMB) to notify individuals whose personal information may have been compromised or accessed during a government agency security breach.[40] Congressional action, and lack of action, underscored the difficulties of passing uniform legislation for security data breaches.

The 111th Congress adopted federal security breach notification requirements as part of the electronic health records stimulus provisions in the American Recovery and Reinvestment Act of 2009 (ARRA).[41] ARRA amended the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[42]—through provisions in the Health Information Technology for Economic and Clinical Health Act (HITECH Act)—expanding the scope of the privacy and security requirements for health data and requiring hospitals, providers, and other HIPAA covered entities to implement security breach notification requirements.[43]

---

36. *See* DATA SECURITY, *supra* note 31, at 2.

37. Veterans Benefits, Health Care, and Information Technology Act of 2006, Pub. L. No. 109-461, 120 Stat. 3403. Title IX requires the Department of Veterans Affairs to issue regulations regarding notices to veterans when a data breach with "reasonable risk" for misuses of information occurs. *Id.*

38. Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007) (reported by Senate Committee on the Judiciary, May 31, 2007); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007) (reported by Senate Committee on Judiciary on May 23, 2007); Identity Theft Prevention Act, S. 1178, 110th Cong. (2007) (reported by the Senate Committee on Commerce, Science and Transportation, Dec. 5, 2007).

39. S. REP. NO. 110-70 (2007) (reporting on S. 495); S. REP. NO. 110-235 (2007) (reporting on S. 1178).

40. Federal Agency Data Protection Act, H.R. 4791, 110th Cong. (2007) (passed the House on June 3, 2008).

41. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, Div. A., Title XIII, § 13402, 123 Stat. 260 (codified at 42 U.S.C.A. § 17932).

42. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 29, 42, 16, 26 U.S.C.).

43. *See* Jeffrey D. Neuburger & Sara Krauss, Will Congress Enact Data Security Breach Provisions This Year? Guess What, It Already Has, Proskauer Rose LLP Privacy Law Blog, http://privacylaw.proskauer.com/2009/03/articles/security-breach-notification-l/will-

Under the HITECH Act, signed by President Obama on February 17, 2009, the covered entities must notify affected individuals when there is a security breach of unsecured "protected health information."[44] Moreover, the entities must inform Health and Human Services (HHS) and the media if the breach involves more than 500 individuals.[45] The HITECH Act pre-empts contrary state laws but leaves intact stronger state laws, rendering HITECH a floor for security breach notifications, not a ceiling.[46] It also authorizes state attorneys general to take action if they believe that an interest of State residents has been threatened by someone who violated HIPPA Privacy and Security rules.[47] The Act requires the Secretary of HHS to issue interim final regulations within 180 days of passage of the legislation, by August 17, 2009. HHS issued guidance on unsecured protected health information on April 17, 2009 with a public comment period open through May 21, 2009.[48] HITECH also requires the Federal Trade Commission (FTC) to develop temporary provisions applying to vendors of personal health records.[49] On April 20, 2009 the FTC issued a proposed rule open to public comment through June 1, 2009.[50]

The 111th Congress has also taken action on the Data Accountability and Trust Act (House Bill 2221), a bill first introduced in the 109th Congress,[51] following the 2005 ChoicePoint data breach discussed above, and reintro-

---

congress-enact-data-security-breach-provisions-this-year-guess-what-it-already-has/ (Mar. 2, 2009).

44. 45 C.F.R § 160.103 (2006); *see* Neuburger & Krauss, *supra* note 43.

45. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, Div. A., Title XIII, § 13402(e)(3), 123 Stat. 260 (codified at 42 U.S.C.A. § 17932).

46. *Id.* § 13421(a); *see also* Neuburger & Krauss, *supra* note 43.

47. *Id.* § 13410(e)(1). Prior to passage of the HITECH Act, the Secretary of Health and Human Services was the only person authorized to pursue civil enforcement for HIPPAA's Privacy and Security rules. *See* GINA STEVENS & EDWARD C. LIU, Cong. Research Serv., CRS Report No. R40546, THE PRIVACY AND SECURITY PROVISIONS FOR HEALTH INFORMATION IN THE AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009, at 18 (2009).

48. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements, 74 Fed. Reg. 19,006 (Apr. 27, 2009) (to be codified at 45 C.F.R. pt. 160, 164).

49. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, Div. A., Title XIII, § 13407(g)(1), 123 Stat. 260 (codified at 42 U.S.C. § 17932).

50. Health Breach Notification Rule, 74 Fed. Reg. 17,914 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318); *see* Bureau of National Affairs, *FTC Issues Proposal on Consumer Notice for Breaches of Electronic Health Information*, HEALTH PLAN & PROVIDER REP., Apr. 22, 2009, http://healthcenter.bna.com/pic2/hc.nsf/id/BNAP-7RCKMD?OpenDocument&Print Version=Yes.

51. Data Accountability and Trust Act (DATA), H.R. 4127, 109th Cong. (2005) (placed on the Union Calendar on June 2, 2006).

duced in the 110th Congress.[52] House Bill 2221 would establish uniform requirements for businesses to notify individuals when an unauthorized party had access to personally identifiable information as a result of a security breach.[53] Hearings on this bill, sponsored by Representative Bobby Rush, were held on May 5, 2009 by the Commerce, Trade, and Consumer Protection Subcommittee of the House Energy and Commerce Committee. On June 3, 2009 the subcommittee forwarded an amended version of the bill to the full committee for its consideration.[54]

III. A TYPICAL CASE OF INFORMATION PRIVACY POLICY?

The definition and formulation of policies regarding security breach notifications appears in several respects to be similar to earlier information privacy policies, although there are some important differences. This Part considers these similarities and differences as they relate to the definition of the problem of security breaches, the proposed solution of notification, and the politics of congressional deliberations.

A. SIMILARITIES TO OTHER PRIVACY ISSUES

The emphasis on notices as a solution follows in the tradition of fair information principles that were first developed in 1973 by the Department of Health, Education and Welfare's Advisory Committee on Automated Personal Data Systems.[55] These principles have become the standard legislative and organizational response to the privacy of personally identifiable informa-

52. Data Accountability and Trust Act, H.R. 958, 110th Cong (2007) (referred to the House Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce on February 9, 2007 but no further action was taken).

53. Data Accountability and Trust Act, H.R. 2221, 111th Cong (2009).

54. The Library of Congress, http://thomas.loc.gov/cgi-bin/bdquery/z?d111:HR02221:@@@X (last visited July 23, 2009) (detailing the legislative history).

55. U.S. DEPT. OF HEALTH, EDUCATION & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, at xx-xxi (1973). The five basic principles include:

> There must be no personal record-keeping system whose very existence is secret. There must be a way for an individual to find out what information about him is in a record and how it is used. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent. There must be a way for an individual to correct or amend a record of identifiable information about him. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

Id.

tion, enshrined in privacy laws in many countries and in standard privacy statements on organizational websites and written materials.[56] Notice is the primary way in which individuals learn of the existence of data systems and the information handling practices of those systems. Such notices are consistent with a governance strategy that Sunstein terms "regulation through disclosure"[57] and Fung, Graham and Weil (Fung et al.) term "targeted transparency."[58] Fung et al. argue that the fundamental idea of such transparency "was not just the public deserved better information . . . [but] that the power of information would create a chain reaction of new incentives."[59] They also point out what has been long recognized by privacy scholars as a problem with notices as a method of informing individuals about the personal information practices of various organizations.[60] Targeted transparency policies can do "more harm than good" as the "political compromise" by which they are formulated is often the product of "incomplete, inaccurate, obsolete, confusing, or distorted" information.[61] However, there are also circumstances under which targeted transparency can be effective; this will be discussed later in Part IV of the Article.

The issue of security breaches is also similar to the policy processes associated with other information privacy legislation in that it is incident or crisis driven. As discussed above, security breach incidents revealed by the media and various public interest groups put pressure on policymakers to respond. Incidents have provided the catalyst for a range of previous privacy laws including the Privacy Act of 1974,[62] the Family Educational Rights and Privacy Act of 1974,[63] the Right to Financial Privacy Act of 1978,[64] the Video Privacy Protection Act of 1988,[65] and the Driver's Privacy Protection Act of 1994.[66]

---

56. Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L. J. 1183, 1185 (2003).

57. Cass R. Sunstein, *Informational Regulation and Informational Standing: Akins and Beyond*, 147 U. PA. L. REV. 613, 613 (1999) (exploring the intersection between the law of standing and our regulatory regime mandating public disclosure).

58. ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 2, 5 (2007).

59. *Id.* at 2.

60. *Id.* at 7-10. *See generally* REGAN, *supra* note 16; Gellman, *supra* note 56.

61. FUNG ET AL., *supra* note 58, at 7.

62. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a).

63. Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 484 (codified at 20 U.S.C. § 1232).

64. Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641 (codified at 12 U.S.C. § 3401).

65. Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710).

In each of these cases, anecdotes and media attention were critical to building public support and congressional pressure to take action.[67] Although there are shortcomings associated with such reactive policymaking,[68] it has indeed been the norm for information privacy legislation.

Because proposals for security breach notifications occurred as reactions to breaches and because the solutions were framed in terms of notices, both privacy advocates and those opposed to legislation viewed the issue through the conceptual lens of previous information privacy proposals.

B. DIFFERENCES FROM OTHER PRIVACY ISSUES

However, there were four key differences between the issue of data breach notification and earlier privacy issues: security, rather than privacy, became the dominant framework defining the problem; proposed solutions put the burden on organizations rather than individuals; harmed individuals were seen as a socially situated group; and proposed solutions treated all organizations similarly. Each of these differences affected congressional deliberations and is discussed briefly below.

Unlike other information privacy issues, the issue of data breach notification is defined primarily in terms of security rather than privacy. Although information privacy and information security have often been recognized as two sides of the same coin, in the United States, privacy has been the more prevalent paradigm for considering policy responses to problems involving personal information.[69] Framing the issue of data breaches in terms of "security" places the emphasis not on normative or tangible harms to individuals but instead on organizational practices. The organization is the evident cause of the problem and the target of legislation. Organizational practices provide

---

66. Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796 (codified at 18 U.S.C. §§ 2721-2725).

67. For example, the adoption of the Video Privacy Protection Act followed a Washington D.C. paper's publication of a list of the videotapes rented by Robert Bork, then a nominee for the Supreme Court. *See* REGAN, *supra* note 16, at 199.

68. *See generally* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1992) (describing how the United States' sectoral approach to privacy requires the formation of new coalitions and political conditions to legislatively address each new issue); DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES (1989) (describing how the lack of a permanent data protection framework in the U.S. has meant legislative policy responses to privacy issues are uncoordinated); REGAN, *supra* note 16 (describing how historically privacy issues have been on the congressional agenda for years and sometimes decades before Congress acts).

69. *E.g.*, REGAN, *supra* note 16, at 3 (explaining how the goal of protecting individual privacy has dominated policy debates around information security policy).

the focus for policy debate. And the focus of organizational practices is shifting as "PDAs, laptops and other mobile devices enable employees and others to remove data from the hardened interior, thus negating perimeter defenses."[70] This focus on security does not imply that privacy will be absent from the debate, but the shift in emphasis to security will affect both policy deliberations and what is believed to be an appropriate policy response.

A second difference from traditional information privacy issues is that proposed solutions put an affirmative requirement on organizations to respond to their security breaches by enhancing the care with which they handle personally identifiable information rather than by requiring them to provide broad notice to individuals. In general, the solution of security breach notification evaluates the effectiveness of an organization's security less on the basis of specific security practices, and more on the basis of how well the data is protected, or the results of those practices.[71] Security breach notification policies often provide organizations with discretion to adopt security practices that are most suited to their business model and information needs, but if those practices do not prevent security breaches, then notification of affected individuals is required.[72] The burden and cost of legislation is on the organization. This will likely shift the policy debate from the organization to the individual, as organizations will likely seek to minimize the costs on them and instead attempt to transfer those costs to individuals affected.

A third difference is that with security breaches, the proposed solution of notice is directed to the affected data subjects as a socially situated group who have had a similar experience. Because the individuals are notified as a result of harm to them as a group, the notice is likely to be more meaningful and timely, and there is a higher likelihood that affected individuals will pay attention. Perhaps more importantly, group notice emphasizes the social harm that has occurred as a result of the security breach. A security breach affects the relationship between an organization and a group associated with that organization, and therefore, the larger society has some legitimate claim to be informed of the breach. In many states and in some proposed federal legislation, notice is required not only to the group of affected individuals,

---

70. Dennis Hoffman & Ken Tyminski, *From Financial Services CISO to Chief Information Management Office: Tackling 360 Degrees of Enterprise Protection*, WALL ST. & TECH., April 26, 2007, *available at* http://www.wallstreetandtech.com/showArticle.jhtml?articleID=199201960.

71. David L. Silverman, *Data Security Breaches: The State of Notification Laws*, 19 NO. 7 INTELL. PROP. & TECH. L.J. 5, 5-12 (2007).

72. *Id.*

but must also be posted on an organization's website and revealed to a government entity and to the media.[73]

A final difference from other information privacy issues is that current policy proposals treat all organizations similarly, as opposed to the historical sectoral approach. Such an omnibus approach has not been typical in the United States, largely because organizations have lobbied that they have different information needs and practices, as well as different relationships with individuals, and thus should be treated differently.[74] In the case of security breaches, the harm to be corrected is that personally identifiable data has been compromised. As reflected in current proposals, this type of harm does not entail an analysis of the relationship of the individual to the organization or an understanding of the information needs of the organization. Such factors are not relevant because unauthorized release, theft, or loss of information is the common problem regardless of the type of relationship the data subject has with the organization experiencing the security breach.

IV. POLICY AND PROCEDURAL OBSTACLES TO A UNIVERSAL BREACH NOTIFICATION LAW

Although the issue of security breaches and the policy solution of breach notifications arrived relatively recently on the congressional agenda, it is not too soon to analyze congressional deliberation thus far and to identify substantive areas that have caused disagreement and will require resolution for passage of any legislation. This Part will first consider several procedural factors which have historically complicated congressional processes and then examine relevant substantive issues.

A. PROCEDURAL FACTORS

The issue of security breaches touches all organizational sectors, and therefore, bills designed to broadly address all sectors will be referred to multiple congressional committees. In the 109th Congress, eight congressional committees had jurisdiction over data security, data breach notification, and data privacy. On the Senate side, three committees had jurisdiction: Banking,

73. For example, the New York breach notification law requires notification to affected New York residents, the state attorney general, consumer protection board, and New York Office of Cyber Security and Critical Infrastructure Coordination, as well as to national consumer reporting agencies if the breach involves more than 5,000 New York residents. Erika S. Koster & Aaron Scott, *Breach and Tell: Security Breach Notification Laws*, THE COMPUTER & INTERNET LAWYER, March 2006, at 5. The North Carolina law similarly requires notification to the Consumer Protection Division of the attorney general's office and all national consumer reporting agencies. *Id.*

74. *See supra* note 16.

Housing, and Urban Affairs; Commerce, Science, and Transportation; and Judiciary.[75] On the House side, five committees had jurisdiction: Energy and Commerce; Financial Services; Government Reform; Judiciary; and Ways and Means.[76] A similar lineup of committees was involved in the 110th Congress and is likely to be involved in the 111th Congress. With such a combination, jurisdictional disputes are likely to occur. For example, in the 110th Congress, Senator Jeff Sessions took the position with respect to the Personal Data Privacy and Security Act of 2007, Senate Bill 495, that "some of the items that [Senate Bill] 495 addresses fall within the jurisdiction of the Senate Banking Committee, and are inappropriate topics for Senate Judiciary Committee legislation."[77] In 2006, a "turf war" occurred between the House Financial Services Committee, supporting House Bill 3997, and the House Energy and Commerce Committee, supporting House Bill 4127.[78] Each committee stripped the other committee's version of a security breach and data privacy bill and substituted its own committee's version, making it more unlikely that action on the House floor would be successful.[79]

Another procedural factor, related to the breadth of committee jurisdiction on privacy issues, is that members of Congress have taken differing approaches in drafting proposed legislation, which complicates the lawmaking process. Some members have approached the issue of security breaches as a new area for legislation and have drafted stand-alone bills,[80] while other members have framed their bills as amendments to existing legislation.[81] For example, several bills amend the Gramm-Leach-Bliley Act and require financial institutions to notify customers, consumer reporting agencies, and federal authorities when there is a breach.[82] Other bills take the approach of amending the Fair Credit Reporting Act to establish data security standards.[83] Another approach is to amend the Racketeer Influenced and Corrupt Organ-

75. DATA SECURITY, *supra* note 31, at 1.

76. *Id.*

77. S. REP. NO. 110-70 (2007), at 26.

78. Seth Stern, *House Panels Move Competing Data Privacy Bills After Text Swap*, 64 CONG. Q. WKLY. REP. 1484, 1484 (2006).

79. *See id.* Both were subsequently sent to the House floor but were not considered. The Library of Congress, http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.03997: (last visited July 23, 2009) (detailing the legislative history of HR 3997); The Library of Congress, http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.04127: (last visited July 23, 2009) (detailing the legislative history of HR 4127).

80. *See*, *e.g.*, Notification of Risk to Personal Data Act of 2005, S. 115, 109th Cong. (2005).

81. DATA SECURITY, *supra* note 31, at 5-13.

82. *See*, *e.g.*, Financial Privacy Breach Notification Act of 2005, S. 1216, 109th Cong. (2005).

83. *See*, *e.g.*, Financial Data Protection Act of 2005, H.R. 3997, 109th Cong. (2005).

izations Act.[84] Still others amend the Federal Criminal Code to prohibit unauthorized access to computer files or passwords, and to punish concealment of security breaches.[85] Not surprisingly, several bills amend more than one piece of existing legislation. The range of legislative approaches makes it more challenging to craft a consensus approach because sponsors and co-sponsors have voiced differing policy approaches in their own bills.

A third procedural factor is the partisan politics associated with congressional consideration of issues involving business regulation generally, including the issue of security breach notification. Democratic members of Congress were first to initiate legislative action in response to the 2005 ChoicePoint data security breach[86] and the 2006 theft of a government laptop from the home of a Veterans Affairs employee.[87] Although some bills have been co-sponsored by Democrats and Republicans, something of a party-line position seems to have emerged in several debates at the committee level.[88] Republicans often seem reluctant to impose what are viewed as burdens on companies for what is regarded as less than clear benefits for consumers who may be subject to over-notification.[89] Democrats, on the other hand, want regulators, and not companies, to decide when companies need to notify consumers of a security breach[90] and are opposed to federal legislation that would pre-empt the strong standards in state legislation.[91] A 2005 debate and party line vote in the House Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection well illustrates the partisan differences.[92] Democrats criticized the Republican supported bill for containing too many loopholes, using a lax standard for when notification is required, preventing state attorneys general from assuming an enforcement role, and

84. *See*, *e.g.*, Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong. (2005).

85. *See*, *e.g.*, Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007).

86. Seth Stern, *Data Brokers Scramble to Limit Regulation*, 63 CONG. Q. WKLY. REP. 881, 882 (2005).

87. Rebecca Adams, *Turning the VA's Loss Into Political Gain*, 64 CONG. Q. WKLY. REP. 1601, 1601 (2006).

88. *See*, *e.g.*, Amol Sharma, *Data Security Bill Approved Over Democrats' Objections*, 63 CONG. Q. WKLY. REP. 2998, 2998 (2005); Adams, *Supra* note 87 at 1601-02.

89. Alabama Republican Jeff Sessions noted during the November 2006 Senate Judiciary Committee's markup of an identity theft bill that "[n]otices can come so often that we become numb to them." Seth Stern, *Identity Theft Bills Offer Choices*, 64 CONG. Q. WKLY. REP. 1032, 1032 (2006).

90. Sharma, *supra* note 88, at 2998.

91. Michael R. Crittenden, *Bill Sets Standard for Data Security*, 64 CONG. Q. WKLY. REP. 775, 775 (2006).

92. Sharma, *supra* note 88, at 2998.

preempting stronger state laws.[93] Similarly, in 2006 several Democratic members of the House Financial Services Committee preferred the stronger and more comprehensive security breach notification requirements in the House Energy and Commerce bill over their own committee's bill.[94]

The President, the OMB, and the FTC have also joined policy discussions at the federal level, providing an alternative forum for policymaking which could lessen the perceived need for congressional action as incremental policy changes can occur through those processes.[95] In May 2007, the OMB issued a directive to federal agencies giving them 120 days to define their notification policies ,[96] which was issued in response to a report, "Combating Identity Theft: A Strategic Plan,"[97] submitted to the President by the President's Identity Theft Task Force.[98] The FTC, primarily using powers granted to it under the Gramm-Leach-Bliley Act, has been somewhat more active in taking actions against financial institutions, including retailers, who have not adequately protected customer information. For example, in 2005 the FTC settled with BJ Wholesale Club and with DSW because the two retailers were not providing effective security for customer records.[99]

These procedural issues involving questions of competing and overlapping congressional committee jurisdictions, the range of available legislative approaches to legislation, partisan differences on government regulation of business and the appropriate government role in the area of security breaches, and the involvement of other policy actors set the stage for consideration of specific substantive questions.

B. SUBSTANTIVE POLICY ISSUES

In addition to procedure, debates about policy content are critical in congressional deliberations and in determining the likelihood that any legislation passes. At least four substantive issues have been the focus of congressional

---

93. *See* Jonathan Krim, *Parties Split on Data-Protection Bill*, WASH. POST, Nov. 4, 2005, at D04.

94. Stern, *supra* note 78, at 1484.

95. Jacqueline Emigh, *Tackling Identity Theft*, GOV'T SECURITY, Aug. 1, 2007, at 6.

96. Memorandum, Office of Mgmt. & Budget, Exec. Office of the President, Safeguarding Against and Responding to the Breach of Personally Identifiable Information OMB M-07-16, (May 22, 2007).

97. PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN (2007), http://www.idtheft.gov/reports/StrategicPlan.pdf.

98. The President's Identity Theft Task Force was created in 2006 to develop a strategic plan for the federal government to combat identity theft. Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 10, 2006).

99. Jason Krause, *Stolen Lives*, 92 A.B.A. J. 36, 39-40 (2006).

debates thus far and are likely to remain hurdles to any legislative success on a breach notification law.

1. Federal Preemption

Policy conflicts and political alliances around the issue of security breach notification must be understood in the context of federalism. The passage of security breach notification legislation in California in 2002[100] reflects what federalism scholars have referred to as a recent upsurge in state government policy activism.[101] Dale Krane, for example, identifies several motivations that states have to pursue policy independently of the federal government: to fill a policy void that the federal government has chosen to not fill, to correct or modify perceived defects in federal policy, and to signal problems to the federal government.[102] In the wake of the 2005 ChoicePoint security breach, California's law requiring notification to affected individuals was widely perceived as an effective solution.[103] It was the only state with such legislation, and other states quickly followed California's example in passing similar laws.[104] By early 2006, twenty states had enacted security breach notification legislation.[105] By June, 2009, forty-four states had passed security breach notification laws, largely modeled on California's.[106]

Congressional consideration of the issue raised the fundamental question of whether federal legislation would weaken existing state requirements, eliciting a strong reaction among the states. Ed Mierzwinski, director of consumer programs for U.S. Public Interest Group, commented generally that the federal effort represented "another arrogant piece of federal legislation that proposes to strip states of their role as laboratories of democracy and hand corporations a huge giveaway."[107] In October, 2005, "47 state attorneys general sent a letter to Congress urging the creation of a tough, far-reaching

100. A.B. 700, 2002 Leg. (Cal. 2002) (codified at Cal. Civ. Code §§ 1798.29, 1798.82).

101. *See generally* John Dinan, *The State of American Federalism 2007–2008: Resurgent State Influence in the National Policy Process and Continued State Policy Innovation,* 38 PUBLIUS 381 (2008) (summarizing a variety of recent state efforts implementing state policies and influencing national policy-making).

102. Dale Krane, *The Middle Tier in American Federalism: State Government Policy Activism During the Bush Presidency*, 37 PUBLIUS 453, 462 (2007).

103. Erika S. Koster & Aaron Scott, *Breach and Tell: Security Breach Notification Laws*, COMPUTER & INTERNET LAW., March 2006, at 1, 2; Silverman, *supra* note 71, at 5.

104. Hunter, *supra* note 29.

105. Koster & Scott, *supra* note 103, at 2.

106. The only states with no security breach law are Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota. *See* National Conference of State Legislatures, *supra* note 30.

107. Kavan Peterson, *States Failing to Secure Personal Data*, STATELINE, July 12, 2006, http://www.stateline.org/live/details/story?contentId=126215.

bill."[108] States rights proponents and consumer advocates were also opposed to a national law that would preempt stronger state laws; as California State Senator Joe Simitian, the author of the California breach legislation, put it, "Let's not sacrifice the standard set in California on the altar of federal regulation."[109]

Many members of Congress are quite aware of the industry push to weaken state laws through federal preemption. In 2006, Barney Frank, the ranking Democrat on the House Financial Services Committee, said, "Whenever [the business community] feels threatened by the energy level of the states, then they come here and get pre-emption."[110] On the other hand, congressional supporters of federal preemption argued in the Financial Services Committee in 2006 that "'rogue' state governments could abuse" a law that gave them an active role in consumer notification.[111] In general, proponents of federal preemption believe that uniform standards are necessary to avoid confusion for industry and consumers.[112] Industry decries the "patchwork of state laws," arguing instead for a "uniform system across state lines" that "temper[s] mass notifications with an assessment of the actual risk that personal information will fall into the hands of data pirates."[113]

2. Policy Goal

To successfully enact federal breach legislation, the policy goal(s) to be achieved must be agreed upon, requiring an understanding of the problem being addressed.

If the problem is, as many have argued, reducing identity theft, then the focus is to determine the scope of identity theft, its causes, and an analysis of whether proposed alternatives effectively address those causes. The issue of identity theft has been of concern to the FTC, GAO, several congressional committees, and numerous interest groups since the 1990s. In 1998, Congress passed the Identity Theft and Assumption Deterrence Act, which made it illegal to steal another individual's personal information with the intent to make use of that information in a fraudulent manner.[114] The law established

108. Tom Zeller Jr., *Data Security Laws Seem Likely, So Consumers and Businesses Vie to Shape Them*, N.Y. TIMES, Nov. 1, 2005, at C3.

109. Jon Swartz, *Tech Experts Plot to Catch Identity Thieves; Politicians to Security Gurus Offer Ideas to Prevent Data Breaches*, U.S.A. TODAY, Feb. 9, 2007, at 7B.

110. Crittenden, *supra* note 91, at 775 (brackets in original).

111. *Id.*

112. Joe Hutnyan, *Moves to Toughen Data Theft Bill Put Pressure on Industry*, SEC. WK, Nov. 14, 2005, at 1.

113. Freedman, *supra* note 28, at 314.

114. Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007.

that the victims of identity theft were the individuals whose identity was stolen, not the companies that lost money, and charged the FTC with establishing a clearinghouse and educating consumers.[115] The issue of identity theft has remained on the congressional agenda since the 1990s, with for example, seventeen bills introduced in the 107th Congress.[116] Identity theft provided a logical frame of reference for policy deliberations about security breach notifications because it was a prominent part of the ongoing policy discussions about the security of personally identifiable information and because the personal costs were tangible. Several security breach notification bills contained identity theft in their titles, and congressional hearings cast security breach notification as an "innovative solution" for the evolving problem of identity theft.[117] Congressional Research Service (CRS) reports[118] and media coverage[119] also linked identity theft and security breach notification, publicizing this connection.

If the policy problem is defined not as reducing identity theft but as correcting lax or ineffective organizational data security, then the policy goal of legislation is to improve data security practices. For some time, observers have pointed out that organizations tend to underestimate the intricacies of data security, and consequently under-invest in security protections.[120] Since data subjects do not "see" the value of data security protections, they do not demand those protections. If there has not been a costly security breach, then organizations do not have incentives to incur preventative security en-

115. *Identity Theft: Hearing Before the H. Comm. on Banking and Financial Services*, 105th Cong. (2000) (statement of Betsy Broder, Asst. Director for the Division of Planning and Information of the Bureau of Consumer Protection, FTC), *available at* http://www.ftc.gov/os/2000/09/idthefttest.htm (summarizing the law and the role of the FTC).

116. ANGIE A. WELBORN, CONG. RESEARCH SERV., CRS REPORT NO. RL 31752, IDENTITY THEFT: AN OVERVIEW OF PROPOSED LEGISLATION IN THE 107TH CONGRESS (2003) (listing and describing "Senate Bills: S. 848, S. 1014, S. 1399, S. 1723, S. 1742, S. 2541, S. 3100, House Bills: H.R. 220, H.R. 1478, H.R. 2036, H.R. 3053, H.R. 3368, H.R. 4513, H.R. 4678, H.R. 5424, H.R. 5474, H.R. 5588").

117. *See, e.g.*, *Identity Theft: Innovative Solutions for an Evolving Problem: Hearing before the Subcomm. on Terrorism, Tech., and Homeland Sec. of the H. Comm. on the Judiciary*, 110th Cong. (2007) [hereinafter *Hearing*].

118. DATA SECURITY, *supra* note 31, at 1 ("Because concerns about possible identity theft resulting from data breaches are widespread, Congress spent a considerable amount of time in the 109th Congress assessing data security practices and working on data breach legislation that would require companies to safeguard sensitive personal data and notify consumers about data security breaches.").

119. *See, e.g.*, Stern, *supra* note 78, at 1484; *Special Report: Identity Theft Prevention*, CONG. Q. WKLY. REP. 2324, 2324 (2005).

120. *See, e.g.*, Jacques S. Gansler & William Lucyshyn, *Improving the Security of Financial Management Systems: What are We to Do?*, 24 J. ACCT. & PUB. POL'Y 1, 4 (2005).

hancements. Many organizations "get by" with more minimal protections.[121] In effect, when left to its own devices, the "market" under-supplies security for data. Security breach notifications can be viewed as a mechanism for correcting that market imperfection by bringing to the organization's attention the cost of not adequately protecting data.[122]

Alternatively, the problem can be defined as lack of public awareness about the ways in which personally identifiable information is collected, exchanged, or retained.[123] In this view, the problem is that the public does not know about something that it arguably has a "right to know" about, and again the existing market and organizational incentive structure do not provide sufficient information for the public. This information asymmetry affects not only individuals' ability to protect themselves, but also, as Stacey Schreft points out, the public good of payment system integrity and efficiency.[124] One important component of personal information flows that has received more widespread attention, in part resulting from the existing state notification laws, is that a range of organizations handle and exchange personally identifiable information. Individuals themselves often do not have a direct relationship with these organizations and fail to recognize the complexity of the financial payment systems underlying their consumer relationships and purchases. This is particularly true with respect to entities with whom financial and retail organizations outsource operations, such as data brokers like ChoicePoint.[125] A definition of the problem as a lack of public awareness includes the following considerations: the ability, or lack thereof, of individuals to make wise personal decisions with respect to their dealings

---

121. *See* Andrew Conry-Murray, *PCI and the Circle of Blame*, INFO. WK., Feb. 25, 2008, at 30 (explaining how compliance with certain industry security standards helps a company appear protected without actually improving the security of their data stores).

122. *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 925-31 (2007) (identifying and explaining three forces pressuring companies: regulatory, economic, and reputational).

123. *See* ROBERT O'HARROW JR., NO PLACE TO HIDE 44-45 (2006) (describing the increase in information acquisition and corresponding lack of individuals' awareness using Acxiom as an example); Dennis Hoffman & Ken Tyminski, *From Financial Services CISO to Chief Information Management Office: Tackling 360 Degrees of Enterprise Protection*, WALL ST. & TECH., April 26, 2007 (showing the "gap" in knowledge of financial institutions); Melanie Rodier, *Locking the Back Door*, WALL ST. & TECH., Nov. 1, 2007, at 26 (giving examples of "major security hole[s]" companies are overlooking).

124. Stacey L. Schreft, *Risks of Identity Theft: Can the Market Protect the Payment System?*, 92 ECON. REV. FED. RES. BANK KAN. CITY 5 (2007).

125. *See generally* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595 (2004) (describing the relationship, or lack thereof between the "individual" and the "organization" in relation to information privacy).

with other individuals because of lack of knowledge, and the competence of the public as a whole to understand the dynamics and contours of the information social and economic environment in which they operate on a daily basis. The goal is to enable individuals, singularly and collectively, to make more informed and more socially desirable decisions.

Notification of security breaches is a solution that can address each of these policy problems. The question of the effectiveness of security breach notices as a solution is next analyzed in terms of the likelihood of such notices achieving these different policy goals.

3. Effectiveness of Notices

a) Critics and Supporters

Some critics have argued that the effectiveness of notices is over-stated and that individuals will ignore the notices, especially if notices are sent for relatively minor breaches or sent too often. As the president of the Information Technology Association of America, Harris Miller, noted, "it's like crying wolf . . . . You're actually undermining the companies' ability to get customers to pay attention when there's a real data breach."[126] Pointless notices can also impose unnecessary costs on consumers if they cancel credit cards, place fraud alerts on credit files, or obtain new driver's license numbers.[127] Other critics have pointed out that "[n]otification letters supply only incomplete, discontinuous, and non-comparative information about data security," sending consumers a "fuzzy signal about future behavior and the likelihood of additional data security breaches."[128] Still others emphasize, as Fred Cate does, that notice "is always a *response* to an event after it has occurred, rather than the *prevention* of that event."[129] In general, industry is opposed to broad notification requirements, seeing them as "expensive, embarrassing, confusing to consumers and often unnecessary."[130] Instead, industry prefers notice in instances where there is a significant chance of harm to the individual with industry being the main determinant of when that might be.

---

126. Patton, *supra* note 27.

127. *Data Breaches and Identity Theft: Hearing Before the S. Comm. on Commerce, Science and Transportation* 109th Cong. (2005) (statement of Deborah Platt Majoras, Chairman, FTC), *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf.

128. Schwartz & Janger, *supra* note 122, at 947.

129. Fred H. Cate, *Information Security Breaches: Looking Back and Thinking Ahead*, Centre Info. Pol'y Leadership Hunton & Williams LLP, at 6 (2008) (emphasis in original), http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf.

130. Jacob Freedman, *Industry Seeks One Law on Data Breach Alerts*, 64 CONG. Q. WKLY. REP. 314, 314 (2006).

Conversely, supporters of notice requirements see enormous value in providing an incentive for an organization to protect sensitive information and encouraging organizations to audit their own security measures. Notice is a mechanism not only for informing individuals who are the subject of a data breach, but also the press and other industry players. Indeed, one could argue that the legislative interest in security breach notification, at both the state and federal level, would not have occurred without the notices that resulted from the California law. Moreover as Representative Janice D. Schakowsky (D-Ill.) pointed out, concern about over-noticing is "disingenuous" as "[t]he right response to over-notification is not to restrict information and to keep consumers and Congress in the dark. If we want to stop over-notification, then corporations need to clean up their act so consumers' personal information is not compromised in the first place."[131]

b) Effectiveness in meeting policy goals

As introduced above, security breach notifications are offered as a solution to a policy problem that has been defined in at least three different ways. The effectiveness of notices is next considered with respect to each of these problems—reducing identity theft, improving organizational data security, increasing public awareness—and the corresponding policy goal.

First, consider notification as a way of reducing identity theft. There is some question about the extent to which security breaches cause instances of identity theft.[132] A survey conducted by Javelin in 2007 revealed that respondents attributed very few reported incidents of identity theft to security breaches.[133] Similarly, the GAO found that based on available data and interviews with law enforcement and industry representatives, most security breaches did not result in detected incidents of identity theft, particularly in the unauthorized creation of new accounts.[134] In only three of the twenty-four largest security breaches between January, 2000 and June, 2005 did the GAO find evidence of misuse of personal information and in only one breach was there evidence of identity theft.[135] Romanosky, Telang, and Ac-

131. Krim, *supra* note 93, at D04.

132. *See* Brendan St. Amant, *Recent Development: The Misplaced Role of Identity Theft in Triggering Public Notice of Database Breaches*, 44 HARV. J. ON LEGIS. 505, 520-22 (2007) (discussing the difficulty in measuring the risk of identity theft).

133. CATE, *supra* note 129, at 8 (citing JAVELIN STRATEGY AND RESEARCH, IDENTITY FRAUD SURVEY REPORT (2007)).

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

135. *Id.*

quisti analyzed the impact of data breach disclosure laws on identity theft for the years 2002 to 2006 and found that the laws had no statistically significant effect on reducing identity theft.[136]

If one finds this evidence convincing, then security breach notification is unlikely to be directly effective in reducing identity theft. There may, however, be indirect positive effects on the reduction of identity theft, as individuals who receive security breach notifications will generally be more cognizant of ways to protect their information.[137] Increased information about security breaches may raise individuals' awareness of the risks of inadvertent disclosure of their information and in the uncertainties about information handling practices—and this may change their individual behavior, reducing their risk of identity theft.[138] Anecdotal evidence and public opinion surveys tend to support the indirect positive effects from security breach notifications and the concomitant media and public attention.[139] A 2006 survey conducted for the Chief Marketing Officers Council concluded that consumers have become more concerned about security and that "[t]hese concerns seem to be driven by personal experiences with security problems, which in turn have been made more prevalent by the personal notification of security breaches."[140]

Second, security breach notification is viewed as a means of improving organizational data security practices. Although notice is not effective in preventing the security breach that triggered the notice, it can act as a deterrent against future events by that specific organization and other similarly situated organizations. Security breach notification may be effective in encouraging a "culture change" within organizations so that data security becomes more of

136. Sasha Romanosky et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, (Seventh Workshop on the Economics of Information Security, Working Paper, 2008), at 13-14, *available at* http://weis2008.econinfosec.org/papers/Romanosky.pdf (noting the possibility of reporting bias for identity theft and the possibility that there are "other means by which this law could (and should) be evaluated").

137. Olive Huang et al., *Security Breach Notification Laws: Views from Chief Security Officers*, SAMUELSON L., TECH. & PUB. POL'Y CLINIC, Dec. 2007, at 24, *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/cso_study.pdf.

138. *Id.*

139. *See* PRIVACY RIGHTS CLEARINGHOUSE, HOW MANY IDENTITY THEFT VICTIMS ARE THERE? WHAT IS THE IMPACT ON VICTIMS? (2007), http://www.privacyrights.org/ar/idtheftsurveys.htm#Jav2007 (summarizing recent surveys to show identity theft trends); *see also* FEDERAL DEPOSIT INSURANCE CORPORATION, PUTTING AN END TO ACCOUNT-HIJACKING IDENTITY THEFT (2004), http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

140. Huang et al., *supra* note 137, at 23 (citing CHIEF MARKETING OFFICER COUNCIL, SECURE THE TRUST OF YOUR BRAND: ASSESSING THE SECURITY MINDSET OF CONSUMERS 8 (2006)).

a priority and more integral to business practices. As security breach notification entails a number of real and potentially significant costs to an organization, including "damage to brand reputation, loss of current [or] future customers, liability under state laws, and [] possible lawsuits,"[141] organizations should seek to avoid or lower these costs by decreasing their number of security breaches. A Ponemon Institute survey in 2007 found that forty percent of retail customers would consider terminating a relationship with a company that experiences a data breach, although only nineteen percent actually did so.[142] Similarly, a 2007 survey of 1200 debit card customers by Javelin Strategy and Research found that three out of four would stop shopping at a store where a data breach occurred and more than three-quarters said they would shop at stores that were security leaders.[143] The reputational harm, or "public shaming,"[144] alters the environment in which organizations find themselves operating. The harm may provide opportunities for those organizations with more effective data security policies and practices to use them competitively.

Third, security breach notifications are seen as a technique for increasing public awareness about the ways in which personally identifiable information is collected, exchanged, and retained. There is evidence that notices are effective in this respect. For example, the simple fact that so many states followed the example of California in passing such laws after the ChoicePoint breach (and the state-law mandated consumer notification of the breach) lends support to the effectiveness of notification in increasing public awareness.[145] Notices are also effective in alerting the media and the advocacy community. In a study conducted by the Samuelson Law, Technology and Public Policy Clinic, "organizations noted concerns that a public notification of a breach would damage their organizations' reputation and the trust behind their name."[146] In their interviews with chief security officers, they also found that,

---

141. Patrick R. Mueller, *How to Survive Data Breach Laws*, NETWORK COMPUTING, June 8, 2006, at 8.

142. Patrick R. Mueller, *Changing Landscape of Data-Breach Notification*, NETWORK COMPUTING, May 14, 2007, at 18.

143. Larry Greenemeier, *Data Theft, Pushback and the TJX Effect – Details of the Largest Customer Data Heist in U.S. History are Beginning to Emerge*, INFO. WK., Aug. 13, 2007, at 36.

144. Zeller, *The Scramble to Protect Personal Data*, *supra* note 7, at C1. *See also* BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 37-38 (Paperback ed. 2004) (describing the reputational dangers to companies of security attacks).

145. *See*, *e.g.*, Zeller, *Another Data Broker Reports a Breach*, *supra* note 7, at C1; Zeller, *Breach Points Up Flaws in Privacy Laws*, *supra* note 6, at C1; Zeller, *The Scramble to Protect Personal Data*, *supra* note 7, at C1 (describing the impacts of consumer notifications following security breaches by data brokers). *See generally* Nakashima, *supra* note 19 (describing the state of security breach notification laws in early 2007 in the context of the security breach at T.J. Maxx and Marshalls retail stores).

146. Huang et al., *supra* note 137, at 15.

with the passage of security breach notification laws, organizations were being advised to invest in encryption.[147] Without notices, less information about breaches would be available; therefore they are effective in reducing the information gathering costs for the public. In this way security breach notifications operate in a similar fashion to notices in the environmental and consumer areas.[148] Indeed, the Samuelson study found that as a result of security breach notification letters and media coverage, security and information privacy was a "hot topic in consumer protection discussions."[149]

c) Lessons from other attempts at "targeted transparency"

The response to the shortcomings that have been identified with security breach notifications need not be to dismiss notification letters as ineffective, but rather to strive to identify ways in which they can be made more effective. In providing notices to individuals, it is critical that the notice be worded in such a way that the individual is not overloaded with irrelevant information, and that the form and content of the notice is understandable. In terms of fashioning effective notices, the research and findings of Fung et al. are particularly instructive, noting that interest in transparency policies is increasing because the more conventional forms of government intervention are not well suited to policy areas that involve "risks and performance flaws" and characterized by wide differences in consumers' preferences, such as consumer decisions about, for example, the relationship between saturated fats and heart disease.[150] Rather than direct government intervention, such as taxing or banning certain products, requiring notification to consumers is seen as an effective role for government.[151] They also point out that the Internet has generated more interest in transparency as "the Internet provides new ways to customize and share information about the risks companies create and the quality of the products and services they provide."[152]

---

147. *Id.* at 17-18.

148. *See*, *e.g.*, Michael S. Baram, *The Right to Know and the Duty to Disclose Hazard Information*, 74 AM. J. PUB. HEALTH 385, 385 (1984) ("[T]he Occupational Safety and Health Administration['s] . . . rule imposes on these employers the duty to disclose such privately held information."); Judith A. Garretson, *Effects of Nutrition Facts Panel Values, Nutrition Claims, and Health Claims on Consumer Attitudes, Perceptions of Disease-Related Risks, and Trust*, 19 J. PUB. POL'Y & MARKETING 213, 223 (2000) (discussing the Nutrition Labeling and Education Act's objective in mandating nutrition labels to "provide information that consumers can use effectively to make more healthful food judgments and choices").

149. Huang et al., *supra* note 137, at 23.

150. FUNG ET AL., *supra* note 58, at 14.

151. *Id.*

152. *Id.* at 14-15.

Through a detailed analysis of fifteen targeted transparency systems, Fung et al. sought to explain what made the difference between a successful policy and an unsuccessful one.[153] They point out, for example, that effective policies provide facts in ways that people want in times, places, and ways that enable them to act.[154] Traditional privacy notices are often crafted with detailed information regarding detailed aspects of information handling which individuals do not see as relevant.[155] Fung et al. also note that effective policies increase knowledge that informs choice rather then providing information that is not directly related to an action.[156] And they argue that there need to be sanctions for non-reporting and misreporting.[157]

4. Scope of Policy

The fourth substantive policy issue regarding proposed federal security breach notification legislation involves the larger context in which such notifications would operate. There are several controversial questions involved here which this Article will only briefly touch. Each, however, has been, and is likely to continue to be controversial.[158] The most controversial question is what standard should be used to "trigger" a notification, including whether the seriousness of the breach should be "reasonably likely" or "reasonably possible," and whether the standard of risk should be that the information could be "misused" or that the breach poses a "significant risk of identity theft" or a "material risk of harm." Predictably, consumer groups support a lower standard, such as "reasonably likely" while companies favor a higher standard, such as "substantial" or "significant."[159] A related question to when notifications would be required involves whether the breach has to affect a certain number of individuals. Finally, related to the issue of triggers for notification is the question of whether encrypted data should be exempted. The

153. *Id.* at 12-13, 183-208 (including analysis of transparency systems spanning a wide range of areas such as terrorism, environmental hazards, personal safety, finance and lending, and food and beverage safety).

154. *Id.* at 11; *accord* David Gibson, Carla Hall & Sylvia Harris, *Healthy Credit*, N.Y. TIMES, May 24, 2009, at WK9 (comparing new credit card policies to food packaging nutrition labels to be "written with the cardholder in mind").

155. George R. Milne et al., *A Longitudinal Assessment of Online Privacy Notice Readability*, 25 J. PUB. POL'Y & MARKETING 238, 245-46 (2006).

156. *See* FUNG ET AL., *supra* note 58, at 177.

157. *Id.* at 179.

158. *See generally* DATA SECURITY, *supra* note 31 (reviewing and summarizing these issues and relevant congressional bills).

159. Stern, *supra* note 89, at 1032.

possibility of an exemption of this kind has sparked debate about the appropriate level of encryption that should be required.[160]

Congressional and public deliberations regarding security breach notifications have also involved questions about several related issues that are often included in policy proposals. Prominent among these are restrictions on use of Social Security Numbers (SSN), which are widely recognized as critical to information security. More controls on, and less use of, SSNs will reduce the dangers to data subjects if their data is compromised. Several congressional bills dealing with security breach notifications have also included restrictions on SSNs, such as eliminating their use as an identifier or authenticator, which are resisted by some organizations because they would impose costs of reconfiguring systems.[161] Another controversial issue has involved whether consumers can freeze their consumer credit reports after a security breach, enabling consumers to block unauthorized third parties from accessing their credit reports. Consumer groups argue that such credit freezes protect consumers from someone fraudulently opening credit in the name of someone whose data have been breached.[162] Business groups argue that such freezes are not necessary as consumers can request fraud alerts under the Fair Credit Reporting Act.[163]

In general, notices are not a "stand-alone" solution, but rather they provide the centerpiece of a more comprehensive policy response that also includes some public reporting, often to a government entity charged with overseeing the policy, and civil fines and criminal penalties if an organization knowingly covers up a breach. For example the Florida security breach notification law fines companies $1,000 a day for each day they fail to disclose a

160. *See Hearing*, *supra* note 117, at 113-14 (citing Bill Watkins, Chief Information Officer for Seagate Technologies in a March 21, 2007 statement recommending that legislation should include a "safe harbor" from regulation if an organization used "hard disc drive-based full encryption" on stored information). In the proposed regulations for implementing the HITECH Act, the FTC and HHS would exempt encrypted stored data from notification requirements if they meet the NIST standards set forth in Publication 800-111 *Guide to Storage Encryption Technologies for End User* and data in transmission if they comply with the requirements of Federal Information Processing Standards (FIPS) 140-2, which include the standards set forth in NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations;* 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs, or other guidance* validated by FIPS 140-2. Thomas J. Smedinghoff & Shannon M. Travis, *HHS and FTC Issue Proposed Regulations on Breach Notification Requirements for Health Records*, WILDMAN HAROLD CLIENT BULLETIN, May 20, 2009, http://www.wildman.com/bulletin/05202009.

161. *See*, *e.g.*, Identity Theft Protection Act, S. 1408, 109th Cong. (2005); Personal Data Privacy and Security Act, S. 1332, 109th Cong. (2005).

162. Stern, *supra* note 89, at 1033.

163. *Id.*

breach, with a monthly fine of $50,000 after thirty days.[164] A Montana law punishes failures to disclose with fines of $10,000 per violation and possible criminal charges.[165] Several congressional bills incorporate similar civil and criminal penalties.[166] Additionally the public reporting to an oversight entity is an important component of most state laws, which generally require reporting to the state attorney general.[167] In congressional bills, reporting is often to the relevant regulatory commission or to the FTC,[168] but the efficacy of such oversight depends on whether these organizations have the personnel and budget to shoulder these new responsibilities. Providing new oversight responsibilities without adequate resources is not likely to be effective. In this respect, Schwartz and Janger propose the establishment of a Coordinated Response Agent (CRA) which would oversee the notification process.[169]

V. CONCLUSION: LIKELIHOOD OF PASSAGE

By mid-2007, there was some sense that the policy window that opened for passage of security breach notification laws had already closed without policy action.[170] As states continued to fill the void left by federal inaction and passed more state laws, it appeared to some that federal action was unnecessary and potentially dangerous for consumers.[171] Evan Hendricks, editor of *Privacy Times*, noted that "[w]ith so many conflicting agendas from the financial industry, data brokers and security companies, there is the danger any bill could be watered down."[172] The likelihood that security breach notification bills will be watered down is very real and very much to be expected given that they fit the classic pattern of regulatory policies, imposing costs on a smaller, well-defined group and providing benefits for a largely dispersed (and often inattentive) group.[173] In order for such policies to pass, it is important that there are groups advocating in support of the policies. Moreover,

164. FLA. STAT. § 817.5681(1)(b) (2009).

165. MONT. CODE ANN. § 30-14-142 (2007).

166. *E.g.*, Financial Privacy Breach Notification Act, S. 1216, 109th Cong. (2005) (authorizing a customer injured by a violation to institute a civil action to recover damages).

167. *E.g.*, N.H. REV. STAT. ANN. § 359-C:20(I)(b) (2009).

168. *E.g.*, Data Accountability and Trust Act (DATA), H.R. 4127, 109th Cong. (2005); Identity Theft Protection Act, S. 1408, 109th Cong. (2005).

169. Schwartz & Janger, *supra* note 122, at 960.

170. Jon Swartz, *Lawmakers Get Less Combative on Data-Breach Bills: Change from Previous Years*, U.S.A. TODAY, March 1, 2007, at 5B.

171. *Id.*

172. *Id.*

173. *See* RANDAL B. RIPLEY & GRACE A. FRANKLIN, BUREAUCRACY AND POLICY IMPLEMENTATION (1982); JAMES Q. WILSON, POLITICAL ORGANIZATIONS (1974); Lowi, *supra* note 9.

such policies are more likely to pass when there has been a crisis or event that brings public attention to the harms that have occurred and that would be redressed by the policies under discussion.

By mid-2009, the odds for passage of security breach notification laws may well have increased.[174] Not only have interest groups continued to advocate for passage, but incidents of security breaches continue to occur and to receive media attention. Perhaps more importantly, the current political climate and financial crisis—with a policy response that emphasizes transparency and accountability, as well as disparagement for those who are causing "moral hazards"—is more conducive to the passage of some legislation.

Recent congressional actions on the HITECH Act and the Credit Card Act of 2009, which requires a forty-five day notice of changes in terms for credit cards,[175] as well as House subcommittee action on the Data Accountability and Trust Act of 2009 are evidence of a more receptive congressional response to legislation that places restrictions on financial institutions that have benefited at significant cost to consumers and the economy as a whole. If security breach notification legislation is viewed by members of Congress through this new perceptual lens, then the likelihood that the previous barriers to passage will be overcome is increased.

174. *See* Neuburger & Krauss, *supra* note 43 (describing the relevant HITECH Act provisions for "protected health information" passed this year, indicating passage of federal security breach notification laws).

175. Phil Mattingly, *Credit Card Restrictions Enacted*, CONG. Q. WKLY. REP., May 25, 2009, at 1214.

ARE "BETTER" SECURITY BREACH NOTIFICATION LAWS POSSIBLE?

By Jane K. Winn†

I. INTRODUCTION

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

---

11. *Id.* at 3.

12. *Id.* at 11.

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

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

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

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

II. WHAT MAKES "BETTER" REGULATION BETTER?

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

---

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

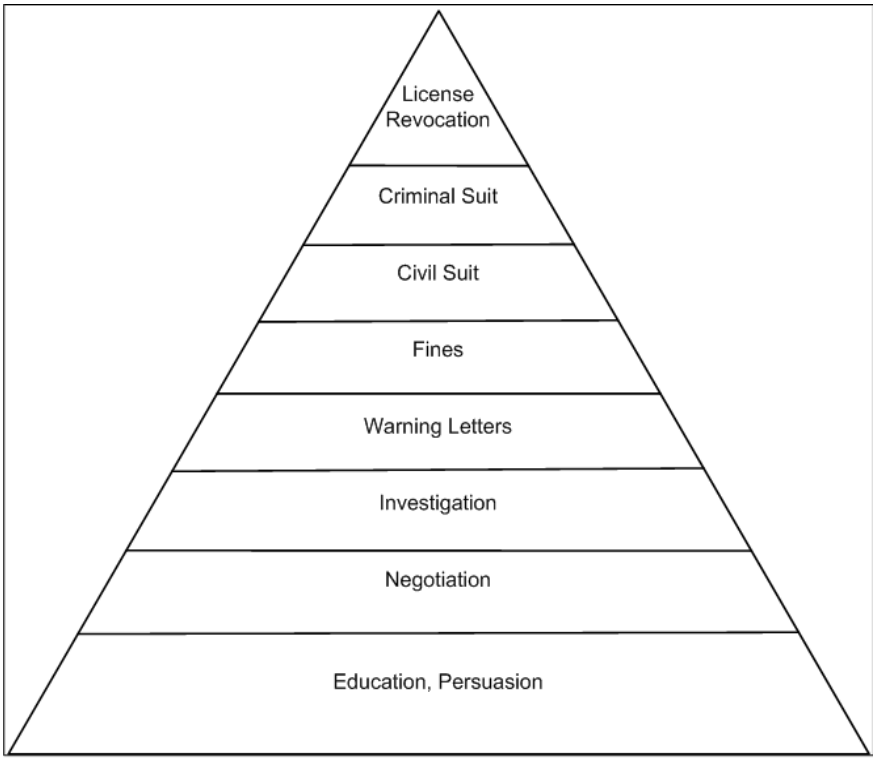
16. IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE (1992).

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

18. *Id.* at 40.

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

Figure 1: Regulatory Pyramid



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

19. *Id.* at 35.

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

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

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

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

---

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

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

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

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

24. *Id.* at 11-15.

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

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

---

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

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

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

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

29. *Id.* at 12.

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

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

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

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

---

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

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

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

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

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

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

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

III. CALIFORNIA'S SECURITY BREACH NOTIFICATION LAW

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

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

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

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

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

42. *Id.*

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

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

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

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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

60. *Id.*

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

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

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

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

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

---

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

Id.

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

---

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

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

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

Id.

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

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

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

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

---

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

78. *Id.* at 461.

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

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

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

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

IV. CHALLENGES OF REDUCING SECURITY BREACHES

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

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

---

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

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

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

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

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

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

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

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

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

87. *Id.* at 244.

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

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

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

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

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

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

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

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

93. 2-37 Banking Law § 37.04.

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

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

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

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

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

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

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

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

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

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

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

100. 18 U.S.C. § 1514(a) (2009).

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

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

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

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

---

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

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

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

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

106. MICHAEL PORTER, COMPETITIVE ADVANTAGE (1985).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

V. CAN SBNLS GET "BETTER?"

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

124. *Id.* at 198-206.

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

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

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

128. 15 U.S.C. § 1681c(g)(1) (2009).

129. 15 U.S.C. § 1681c(g)(3) (2009).

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

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

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

---

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

131. 15 U.S.C. § 1681n (2009).

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

133. *Id.*

134. *Id.*

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

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

VI. CONCLUSION

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

135. *Id.*

136. *Id.*

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

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

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

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

PEEPING

By Peter P. Swire[†]

TABLE OF CONTENTS

---

† Special Assistant to the President for Economic Policy, the National Economic Council; C. William O'Neill Professor of Law, Moritz College of Law of the Ohio State University (on leave). The text of this paper was completed before the author entered the United States Government, and the views expressed herein are entirely his own. My thanks to Annie Anton, David Brin, Jonathan Cantor, and Miranda Johnson Haddad for comments from participants at the Berkeley Conference on Security Breach Notification Six Years Later and the Privacy Law Scholars Conference 2009. Special thanks to my research assistants Joseph Buoni, Anthony Frost, Leah Stoecker, and Peter Williams for their good cheer in tracking down sources ranging from Lord Tennyson to technical papers from the Association of Computing Machinery.

Passport peeping—more than just curiosity?[1]

Turns out a lot more people than George Clooney and his girlfriend were hurt by the Hollywood hunk's motorcycle accident last month. As many as 40 doctors and other employees at the Palisades Medical Center in North Bergen, N.J., got suspensions for allegedly leaking confidential medical information about the couple.[2]

Government computers used to find information on Joe the Plumber: Investigators trying to determine whether access was illegal.[3]

I. INTRODUCTION

The 2008 presidential campaign focused unprecedented attention on "employee snooping" into personal files, from the candidates' passports, to Obama's cell phone records, to Joe the Plumber's child support payments.[4] In the same period, a rash of intrusions into celebrities' medical files led to a new California law that imposes monetary sanctions for unauthorized looking into a person's medical files.[5]

This Article explores this phenomenon of employee snooping, a practice I call "peeping."[6] A "peep" may seem a small thing, defined as "to peer slyly or secretly; take a hasty, furtive look."[7] The "peep" is hasty, just taking a moment. It is furtive, suggesting that the person knows that he or she is

---

1. Employees look at passport records of candidates Clinton, McCain, and Obama. Zachary Coile, *Passport Peeping—More Than Just Curiosity?*, S.F. GATE, Mar. 22, 2008, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/03/21/MN43VODTF.DTL&type=politics.

2. Leo Standora, *Staff Suspended for Leaking George Clooney Medical Records*, N.Y. DAILY NEWS, Oct. 10, 2007, http://www.nydailynews.com/gossip/2007/10/10/2007-10-10_staff_suspended_for_leaking_george_cloon.html.

3. Randy Ludlow, *Government Computers Used to Find Information on Joe the Plumber: Investigators Trying to Determine Whether Access was Illegal*, COLUMBUS DISPATCH, Oct. 24, 2008, http://www.dispatch.com/live/content/local_news/stories/2008/10/24/joe.html?sid=101 [hereinafter *Government Computers*].

4. *See infra* Part II.

5. *See infra* Section V.B.2.

6. An earlier term for this phenomenon was "browsing." *See* Beverly Woodward, *The Computer-Based Patient Record and Confidentiality*, 333 NEW ENG. J. MED. 1419, 1420 (1995). That term was primarily used, however, before the every-day use of web browsers. Essentially, we all "browse" now, so I think the term "browsing" should not be the label for a category of questionable or even criminal behavior.

7. WEBSTER'S NEW WORLD COLLEGE DICTIONARY (June 2009 revisions).

doing something shameful or blameworthy. "Peep" is further defined as "a look through a narrow aperture . . . into a larger space."[8] In the physical world, that can mean the Peeping Tom who stares out at Lady Godiva. In our computerized world, to "peep" means to look through your computer screen into the large expanses of modern databases.

This Article draws on mythology and literature to show the ancient roots of the phenomenon of peeping. There is a profound ambivalence about how seriously we should treat peeping. The motives to peep are as varied as human nature—to see a handsome or beautiful person, gossip with friends about what you have seen, use the information against your foes, sell the gossip for cash, and perhaps even blackmail someone. As understandable as the impulse is, however, the word "peep" also refers to "furtive" and thus blameworthy activity. As we will see, the penalty to Peeping Tom himself was very severe—a lifetime of blindness.[9] When the foundational story for a phrase imposes such a severe penalty, then we have an important clue that something important is at stake.

Part II of the Article discusses the recent political and celebrity peeping incidents. Part III describes three increasingly harmful types of peeping: the *gaze*, the *gossip*, and the *grab*. Part IV asks: "Why now?" Human curiosity, especially for the titillating or about the famous, is as old as human nature. There are specific reasons, however, why these peeping incidents are coming to our attention now. First, the number of detailed databases, accessible by numerous employees, has climbed sharply in recent years. Second, once a peeping incident occurs, the perpetrator can easily post the evidence to a blog or social networking site. Finally, databases increasingly include logging and auditing software, so that the peepers can be caught after the fact. In short, both the opportunity for peeping and the possibility of catching the peeper have climbed. As a society, therefore, we are newly facing the question of how to respond when we catch the perpetrators.

Part V explores what to do about this increase in peeping. The traditional penalty for peeping was blindness, but that seems a bit excessive. Many of the most promising approaches are technical safeguards, including systems that limit employee access except where authorized and auditing systems to deter, detect, and punish those who break the rules. There are also useful administrative safeguards, from training employees to considering expanding the new California's security breach notification laws to include a notice requirement in the event of a peep.

---

8. OXFORD ENGLISH DICTIONARY (June 2009 revision).
9. *See infra* Section III.A.

Finally, Part VI applies these insights to a major current area of controversy: behavioral advertising on the Internet. A significant source of concern about tracking the Internet usage of individuals is that they will become subject to peeping, as happened for instance to Obama's cell phone records once he became famous. This risk of what Jeffrey Rosen has called "The Unwanted Gaze"[10] gives good reason to assure that effective anti-peeping measures are in place for any behavioral advertising systems that are deployed.

The topic of peeping is fascinating. We all can understand the temptation to peep at something intriguing. We also know that we do not want to be peeped at in our modern hospital, phone, online surfing, or other databases. Perhaps this Article can encourage more discussion about peeping from many fields beyond law and technology, including literature, mythology, sociology, anthropology, psychology, and more.

II. RECENT PEEPING INCIDENTS

Many of the recent stories about peeping arose in the 2008 presidential campaign and in incidents where the medical records of celebrities were compromised. This Article highlights some of the more notable recent incidents before turning to what these incidents mean and what should be done to reduce their effects.

On March 20, 2008 the State Department announced that two employees were fired and a third was disciplined for improperly accessing Senator Barack Obama's passport files.[11] Senior department officials said they learned of the incidents only in response to a reporter's inquiry.[12] Upon investigation, they discovered that contractors for the State Department had improperly accessed the files on at least three occasions.[13] In each instance, the improper access was flagged by a computer-monitoring system that creates special alerts for access to the records of high-profile individuals.[14] The front-line

10. *See generally* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000).

11. Glenn Kessler, *Two Fired for Viewing Obama Passport File: State Department Investigating Whether Contractors Broke Law*, WASH. POST, Mar. 21, 2008, at A03.

12. *Id.*

13. *Id.*

14. The computer-monitoring system for prominent individuals was created after a 1992 incident in which State Department employees improperly accessed the passport records of then-candidate Bill Clinton, apparently in hopes of finding 1960s-era information that would have been damaging to his presidential campaign. *Passport Breach Being Investigated*, WASH. TIMES, Mar. 21, 2008, http://www.washingtontimes.com/news/2008/mar/21/passport-breach-being-investigated/.

managers, however, apparently did not report the peeping incidents to higher-level managers.

The State Department investigation determined that files of Senators Hilary Clinton and John McCain had also been improperly accessed.[15] In addition to the disciplining of the workers, Secretary of State Condaleeza Rice apologized personally to the three presidential candidates.[16] The incident generated widespread attention, and triggered my own interest in peeping as a research topic. In an interview with the Wall Street Journal, I said, "At least they actually had the systems in place to catch it and they took it seriously."[17] I emphasized that the passport flap, and the firing of employees, could help educate our society about the problem: "It's sending a signal to every data clerk in the country that you shouldn't browse."[18]

Another much-publicized peeping incident occurred after Samuel Wurzelbacher, known as "Joe the Plumber," received repeated mention in the October 15, 2008 presidential debate between John McCain and Barack Obama.[19] Wurzelbacher initially drew public notice when he claimed, in speaking on video with Obama, that Obama would raise his taxes.[20] In the days following the debate, information on Wurzelbacher's driver's license and his sport utility vehicle was retrieved from the Ohio Bureau of Motor Vehicles three times, according to the Columbus Dispatch.[21] The Ohio Department of Job and Family Services admitted that the agency checked whether Wurzelbacher was behind on child support payments, as well as whether he was receiving welfare assistance or owed unemployment compensation taxes.[22] These peeping incidents immediately sparked political controversy within both parties.[23] The Columbus Dispatch reported that "the agency's actions drew outrage throughout the nation."[24]

---

15. Helene Cooper, *Passport Files of 3 Hopefuls are Pried Into*, N.Y. TIMES, Mar. 22, 2008, at A1.

16. *Id.*

17. Amy Schatz, *U.S. News: Congress Raises Call for Data Safeguards*, WALL ST. J., Mar. 31, 2008, at A4.

18. *Id.*

19. *See* Wikipedia, *Joe the Plumber*, http://en.wikipedia.org/wiki/Joe_the_Plumber (last visited June 19, 2009).

20. *Id.*; *see also 'Joe the Plumber' Becomes Focus of Debate* (AP television broadcast Oct. 15, 2008), http://www.youtube.com/watch?v=PUvwKVvp3-o (last visited Aug.1, 2009).

21. Ludlow, *Government Computers*, *supra* note 3.

22. Randy Ludlow, *Checks on 'Joe' more extensive than first acknowledged*, COLUMBUS DISPATCH, Oct. 29, 2008, http://www.dispatch.com/live/content/local_news/stories/2008/10/29/joe30.html.

23. The Ohio spokesman for the McCain campaign said, "It's outrageous to see how quickly Barack Obama's allies would abuse government power in an attempt to smear a pri-

An investigation ensued, which produced no evidence that the Obama campaign had sought Wurzelbacher's records. The multiple accesses to his records, however, led to the resignation of the Director of the Ohio Department of Job and Family Services, the firing of the Deputy Director, and the resignation of an Assistant Director.[25] In addition, Ohio enacted a law in early 2009 creating civil and criminal penalties for improper access of personal information in state databases.[26]

One other notable peeping incident also arose from the 2008 presidential campaign. In late November, CNN reported on an internal company email from a senior Verizon Wireless official revealing that "the personal wireless account of President-elect Barack Obama had been accessed by employees not authorized to do so."[27] Obama spokesman Robert Gibbs said that anyone viewing the records would likely have been able to see phone numbers and the frequency of calls, but that "nobody was monitoring voicemail or anything like that."[28] The Verizon official said that employees who accessed the account for "anything other than legitimate business purposes will face disciplinary action, up to and including termination."[29] Those active in the development of privacy law called for further legal protections; Lee Tien of the Electronic Frontier Foundation remarked that "it's time" to give protection to unauthorized access of phone records "because it really is a violation of privacy to have those kinds of records looked at."[30]

Along with these political peeping incidents, there has been a rash of recent peeping into the medical files of celebrities. In May 2007, the National Enquirer reported that television star Farah Fawcett had suffered a relapse of

---

vate citizen who dared to ask a legitimate question." Ludlow, *Government Computers*, *supra* note 3. The Obama campaign responded, "Invasions of privacy should not be tolerated. If these records were accessed inappropriately, it had nothing to do with our campaign and should be investigated fully." *Id.*

24. *Id.*

25. Posting of Catherine Candisky to Columbus Dispatch, UPDATED: Jones-Kelley Quits, Two Others Departing Over Joe the Plumber Searches, http://blog.dispatch.com/dailybriefing/2008/12/joneskelley_quits_over_joe_the.shtml (Dec. 17, 2008 18:49 EST).

26. H.R. 648, 127th Gen. Assem. (Ohio 2008).

27. *Obama's Cell Phone Records Breached*, CNN, Nov. 20, 2008, http://www.cnn.com/2008/POLITICS/11/20/obama.cell.breach/index.html.

28. *Id.*

29. *Id.*

30. Posting of Jordan Light to 60-Second Science Blog, Obama's Cell Phone Hacked, Privacy Issues Murky, http://www.sciam.com/blog/60-second-science/post.cfm?id=obamas-cell-phone-hacked-privacy-is-2008-11-21 (Nov. 21, 2008 18:05).

cancer, before she had even told her son and closest friends.[31] A UCLA employee was fired for unauthorized access to the files.[32] In October, 2007, actor George Clooney and his girlfriend suffered a motorcycle accident in New Jersey. As many as forty doctors and other employees received suspensions for allegedly leaking Clooney's confidential medical information.[33] Then in March, 2008, UCLA Medical Center took steps to fire at least thirteen workers, and disciplined others, for looking at singer Britney Spears's confidential medical files.[34]

III. THREE KINDS OF PEEPING: THE GAZE, THE GOSSIP, AND THE GRAB

As a typology of peeping, the initial step is "the gaze"—looking where one is not supposed to look, such as Tennyson's Peeping Tom gazing at Lady Godiva or a modern-day Peeping Tom sneaking a peep through a bedroom window. A step worse is "the gossip"—telling others about what one has seen. Either accurate or inaccurate gossip can spread information beyond the original peeper, potentially harming a person's reputation. Even worse is "the grab." It occurs when an employee grabs the personal information for profit, such as through blackmail, often at the behest of an outsider. A recent example is where the National Enquirer paid an employee at the UCLA Medical Center to turn over celebrities' medical records on over thirty occasions.[35]

---

31. Charles Ornstein, *Fawcett's Cancer File Breached: The Incident Occurred Months Before UCLA Hospital Employees Were Caught Snooping in Britney Spears' Files*, L.A. TIMES, Apr. 3, 2008, at 1.

32. *Id.*

33. Leo Standora, *Staff Suspended for Leaking George Clooney's Medical Records*, N.Y. DAILY NEWS, Oct. 10, 2007, http://www.nydailynews.com/gossip/2007/10/10/2007-100_staff_suspended_for_leaking_george_cloon.html.

34. Charles Ornstein, *Hospital to Punish Snooping on Spears: UCLA Moves to Fire at Least 13 for Looking at the Celebrity's Records*, L.A. TIMES, Mar. 15, 2008, at 1.

35. Phillippe Naughton, *Lawanda Jackson pleads guilty to selling celebrity medical records*, TIMES ONLINE, Dec. 2, 1008, http://www.timesonline.co.uk/tol/news/world/us_and_americas/article5272883.ece. For additional details of the Jackson indictment, *see Celebrity Medical Files Indictment*, THE SMOKING GUN, Apr. 29, 2008, http://www.thesmokinggun.com/archive/years/2008/0429082ucla1.html.

A. THE GAZE

The simplest form of peeping is merely to look. Literary scholars, of whom I am not one, call this "the gaze."[36] The presence of the gaze is pervasive in western culture, finding roots in mythology, Judeo-Christian teachings, and English common law.

The stories of Tiresias and Peeping Tom show the mythological and psychological importance of "just looking." In Greek mythology, the young poet Tiresias happens upon the goddess Athena while she is bathing. As told by Alfred, Lord Tennyson:

> And all her golden armor on the grass,
> And from her virgin breast, and virgin eyes
> Remaining fixt on mine, till mine grew dark
> For ever, and I heard a voice that said
> "Henceforth be blind, for thou hast seen too much,
> And speak the truth that no man may believe."[37]

Simply for looking, Tiresias is blinded for life. The stories of Lady Godiva and Peeping Tom are strikingly similar. According to the story, the Lady Godiva pleaded with her husband to cease his crushing taxation on the city of Coventry. He agreed, on the condition that she ride unclothed through the city.[38] The townsfolk agreed to shut their doors to protect the modesty of the Lady during her ride. As told once again by Tennyson, however, a low-born churl named Tom looked when he should not have:

> Then she rode back, clothed on with chastity;
> And one low churl, compact of thankless earth,
> The fatal byword of all years to come,
> Boring a little auger-hole in fear,
> Peep'd—but his eyes, before they had their will,
> Were shrivel'd into darkness in his head.[39]

---

36. Special thanks to literary scholar and friend Miranda Johnson Haddad for her assistance with this section. For an extended and thoughtful analysis of the importance of "the unwanted gaze," see ROSEN, *supra* note 10.

37. ALFRED LORD TENNYSON, THE POETIC AND DRAMATIC WORKS OF ALFRED LORD TENNYSON 489 (2004).

38. Wikipedia, *Lady Godiva*, http://en.wikipedia.org/wiki/Lady_Godiva (last visited June 19, 2009).

39. TENNYSON, *supra* note 37, at 95.

From these stories, even this non-literary law professor can make a few observations. First, what was it about Tennyson and these stories? I leave that for scholars of romantic poetry. Second, we learn the traditional penalty for peeping—a lifetime of blindness. There is a poetic and psychological justice to this punishment, what one might call "an eye for an eye-ing."

The power of "just looking" is echoed in our mythological and religious traditions. In Greek mythology, gazing directly upon Medusa could turn the person to stone.[40] In the Bible, Lot's wife is told not to turn back to gaze at Sodom and Gomorrah. She cannot resist the temptation to look, however, and is turned into a pillar of salt.[41] Gazing is forbidden out of respect for the object. In some cultures, those approaching the king were required to abase themselves, and not gaze directly at the king's face.[42]

Similarly, as explained by Alan Westin in his forthcoming history of privacy in western civilization, the ancient Hebrews created a number of protections against the inappropriate gaze.[43] In the nomadic period, the Hebrews were taught to align their tents so that one family could not see directly into another tent.[44] Later, this requirement of physical privacy was exemplified by the command not to look into a neighbor's courtyard.[45] This meant, in practice, that dwellings were built with special walls, to prevent inadvertent peeping into the dwelling of the neighboring family.[46] Westin writes that this preservation of a private space for the family was part of a cultural regard of privacy that was historically and culturally linked to the individual's rights within the Jewish legal system.[47] Respect was due not only to the king, but also to each individual and family, so rules against inadvertent and disrespectful gazing applied to everyone.

Dislike of the inappropriate and unwelcome gaze extended into western legal culture. As Judge Blackstone commented:

> Eaves-droppers, or such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to

---

40. Wikipedia, *Medusa*, http://en.wikipedia.org/wiki/Medusa (last visited June 19, 2009).

41. *Genesis* 19:26.

42. *See generally* Gary T. Marx, *Forget Big Brother and Big Corporation: What About the Personal Uses of Surveillance Technology as Seen in Cases Such as Tom I. Voire?*, 2 J. LEGAL TECH. RISK MGMT. 24 (2007).

43. ALAN F. WESTIN, PRIVACY IN WESTERN CIVILIZATION: FROM THE HEBREWS AND GREEKS TO THE INTERNET AGE (forthcoming 2010).

44. *Id.*

45. *Id.*

46. *Id.*

47. *Id.*

> frame slanderous and mischievous tales, are a common nuisance, and presentable at the court-leet, or are indictable at the sessions, and punishable by fine and finding sureties for their good behavior.[48]

Such behavior found legal protection: peeping and eavesdropping were punishable under English common law.[49] Peeping and eavesdropping have been punished under a variety of causes of action, including trespass, window peeking, secret peeping, eavesdropping, indecent viewing or photography, violation of privacy, voyeurism, and unlawful photographing.[50] Sometimes prosecutions have occurred under less specific claims, such as disorderly conduct, breach of peace, or prowling.[51] In reviewing the cases, Lance Rothenberg writes, "[C]ourts actively employ the lexicon of privacy rights in the prosecution of these crimes. Therefore, it is clear that criminal law serves as a vehicle for the substantive protection of individual privacy."[52]

B. THE GOSSIP

The next step beyond just looking ("the gaze") is to tell someone what you saw ("the gossip"). In this Article, I resist the law professor's impulse to develop a universal theory of gossip. For our purposes, we first recognize that gossip can cause more types of harm than the gaze. When an individual gazes upon the nude form of Athena or the titillating facts in a celebrity's medical files, he is invading the privacy of the object of the gaze. When the individual tells others, however, additional harms may result to the object of the gaze. The object's reputation may be damaged, with embarrassing results: "Did you know that so-and-so has such-and-such a condition!?" The gossip might spread, leading to loss of employment, denial of insurance, being cast out of a social circle, or other concrete harms.

Even Jewish law recognized the harms of gossip, which in Hebrew is *l'shon hara* or the "evil tongue." The term is synonymous with slander and evil

---

48. DAVID J. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY 2-4 (1978).

49. *Id.* at 4. For other legal discussions of the topic, see generally Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 491-92 (2006); Maria Pope, *Technological Arms Peeping Toms with a New and Dangerous Arsenal: A Compelling Need For States to Adopt New Legislation*, 17 J. MARSHALL J. COMPUTER & INFO L. 1167 (1999); Bill Prewitt, *The Crimination of Peeping Toms and Other Men of Vision*, 5 ARK. L. REV. 388 (1951).

50. Lance E. Rothenberg, *Re-Thinking Privacy: Peeping Toms, Video Voyeurs, and Failure of the Criminal Law to Recognize a Reasonable Expectation of Privacy in the Public Space*, 49 AM. U. L. REV. 1127, 1144 (2000) (collecting cases under each heading).

51. *See generally* H. Morley Swingle & Kevin M. Zoeller, *Criminalizing Invasion of Privacy: Taking a Big Stick to Peeping Tom*, 52 J. MO. B. 345 (1996).

52. Rothenberg, *supra* note 50, at 1144 (citations omitted).

gossip.[53] Jewish religious leaders equate the harm of gossip, a "heinous crime," to that of murder and idolatry.[54] Rabbis recognized that *l'shon hara* harmed three individual: he who told it, he who heard it, and he who was slandered.[55] One commentator, poignantly remarked, "If [the Rabbis] were horrified by *l'shon hara* in their day, when news took months or years to circulate, consider how they would react today, when words are flashed around the world in an instant."[56]

A political incident from 2008 illustrates the harm of truly awful (great?) gossip. Congressman Vito Fosella from Staten Island was arrested in Northern Virgina for driving under the influence.[57] As it turns out, the Congressman was in there to visit his long-time girlfriend who lived there with their preschool-aged, out-of-wedlock daughter.[58] His girlfriend had to come down to the station house to bail him out because his wife was up in Staten Island with his three acknowledged children.[59] The Vito Fossella story was too good to keep secret. This sort of story could have led to serious professional damage in any era. In our modern era of blogs and 24-hour cable TV, the story spread almost instantly, and the Congressman announced he would not run for re-election.[60]

The negative effects of gossip, however, go far beyond this sort of dramatic story about a public figure.

C. THE GRAB

The most serious form of peeping is the "grab," where an employee accesses records for personal gain, rather than to gaze or gossip. Compared to the gossip, the grab is worse in two respects. First, the law regularly treats an action undertaken for financial gain as more serious. The Health Insurance Portability and Accountability Act[61] (HIPAA) privacy rule, for instance, prohibits the disclosure of medical records, and the Computer Fraud and Abuse

---

53. EDITH SAMUEL, YOUR JEWISH LEXICON 86-87 (1982).

54. *Id.*

55. *Id.*

56. *Id.*

57. Allison Klein, *Fossella Pleads Guilty to DUI in Alexandria*, WASH. POST, Apr. 13, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2009/04/13/AR2009041301007.html; *see also* Tom Jackman, *N.Y. Congressman Convicted of DUI: Whether Jail Required Up to Va. Judge*, WASH. POST, Oct. 18, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/10/17/AR2008101700339.html.

58. *Id.*

59. Klein, *supra* note 57.

60. Jonathan P. Hicks, *Fossella Is Said to Be Ending Re-election Bid*, N.Y. TIMES, May 20, 2008, at B1.

61. 42 U.S.C. § 1320d-6 (2006).

Act[62] punishes unauthorized access to computers. Second, the law also punishes outsiders who bribe or persuade employees to violate a duty owed to their employer. This sort of activity by the outsider is essentially theft from the employer, such as a bribe of a public official[63] or misappropriation of an employer's property.[64]

The two recent instances involving personal information of celebrities exemplify this sort of "grab" of personal information. According to her guilty plea, the National Enquirer paid LaWanda Jackson $4,600 to disclose UCLA Medical Center records on thirty-three occasions in 2006 to 2007.[65] The Enquirer got the medical dirt on celebrities.[66] Jackson got indicted and later pled guilty for a criminal violation of the HIPAA medical privacy rules.[67] The second involves the spectacular wiretapping prosecution against "private investigator to the stars" Anthony Pellicano. Pellicano was convicted in 2008 of carrying out numerous wiretaps in Hollywood, including on behalf of Hollywood stars and executives.[68] Pellicano had a variety of techniques for gaining cooperation from current or former telephone company employees, including acquiring company keys, and having a "ladies' man" develop a group of women employees who would reveal phone records when asked.[69]

This sort of grab of personal records is repugnant. According to the guilty plea, the National Enquirer bribed Ms. Jackson to violate her duty to the hospital and the patients, and Pellicano's clients paid for violations of the wiretap laws. This is similar to the way a blackmailer or other evildoer in a Victorian novel might bribe a servant to steal the personal letters of the master or mistress.

The law not only imposes punishments on the employee who grabs and the outsider who induces the grab. The law may also impose a duty on the employer to take precautions against such grabs. One intriguing discussion of

---

62. 18 U.S.C. § 1030(c)(2)(B) (Supp. 2008).

63. 18 U.S.C. § 201 (2006).

64. United States v. O'Hagan, 521 U.S. 642, 643 (1997) (accepting misappropriation theory of insider trading).

65. Phillippe Naughton, *Lawanda Jackson pleads guilty to selling celebrity medical records*, TIMES ONLINE, Dec. 2, 1008, http://www.timesonline.co.uk/tol/news/world/us_and_americas/article5272883.ece. For additional details of the Jackson indictment, see *Celebrity Medical Files Indictment*, THE SMOKING GUN, April 29, 2008, http://www.thesmokinggun.com/archive/years/2008/0429082ucla1.html.

66. *Id.*

67. *Id.*

68. David M. Halbfinger, *Investigator to the Stars is Convicted in Wiretaps*, N.Y. TIMES, May 16, 2008, at C1.

69. David M. Halbfinger, *In Pellicano Case, Lessons in Wiretapping Skills*, N.Y. TIMES, May 5, 2008, at C6.

this duty appears in a Federal Trade Commission's letter issued after a data breach affected customers of Novastar Financial, Inc. and Novastar Mortgage, Inc.[70] The FTC's investigation considered "whether NovaStar failed to implement reasonable procedures or review its employees' access to consumer reports," in violation of the Fair Credit Reporting Act[71] or the Safeguards Rule of the Gramm-Leach-Bliley Act.[72] The FTC used the letter to highlight the risks created by "rogue employees," and described potentially far-reaching obligations on employers to monitor peeping by employees.[73] It suggested that employers would need to "adjust their information security programs" with the changing tide in technology and risks over time.[74] The FTC suggested that "for companies that allow employees access to highly sensitive data" such measures include,

> depending on the circumstances: tailored access limitations based on an employee's position, functions, and workload; periodic supervisory review of an employee's activity; employee training and clear warnings regarding wrongful access to or disclosure of data; and/or the use of software or other means to monitor employee access to consumer data, place restrictions on such access, or flag suspicious activity.[75]

IV. WHY NOW?

This year's rash of high-visibility peeping cases raises two related questions: has peeping become more common, or is it the *discovery* of peeping that is becoming more common? I offer reasons to believe that both are occurring.

Peeping may have become more common because of a shift in the balance of elements of the classic TV detective questions: did the suspect have the means, motive, and opportunity to commit the crime.[76] While human motives change slowly, the means and opportunity for peeping have risen in recent years. The means of peeping is generally to have access to an intri-

---

70. Letter from Joel Winston, Associate Director, Division of Privacy and Identity Protection, Federal Trade Commission to Garrett Rasmussen, Apr. 4, 2008, http://www.ftc.gov/os/closings/staff/080404novastar.pdf [hereinafter Winston Letter].

71. 15 U.S.C. § 1681 (2006).

72. 16 C.F.R. § 314 (2003).

73. Winston Letter, *supra* note 70.

74. *Id.*

75. *Id.*

76. Larry Rogers, *Cybersleuthing: Means, Motive, and Opportunity* (2000), http://www.sei.cmu.edu/news-at-sei/columns/security_matters/2000/summer/security-sum-00.htm.

guing database: the hospital database about the celebrity, the Verizon database about cell phone calls, or the passport database about the presidential candidate. As scholars have frequently noted, the number, size, and granularity of personal-information databases has grown rapidly over time.[77] The opportunity is provided to every employee that can access the database. In the old paper-based world, official records clerks often were involved in each retrieval of a paper file. In the world of mainframe computers, sophisticated technicians assisted in data retrieval. Today, by contrast, the spread of desktops, laptops, and intranets means that numerous employees often have access to the corporate databases. The cliché is that data can be retrieved "at the click of a mouse." Retrieval is not only simple, but can be done furtively from the safety of one's own desk. No nosy file clerk or computer technician stands in the way of peeping into the file.

As technology has increased the mode and opportunity of peeping, so too has it amplified the ability to discover this presumably furtive peeping. The prevalence of electronic files and the ease of dissemination of such files, coupled with the growing presence of data breach laws, have all contributed to the visibility of a once more clandestine act.

The shift from paper to electronic files has increased both the ease of searching for files in a database, and the likelihood of after-the-fact detection of a violation. First, the ease of searching in a database and the lack of the need for physical intrusion into forbidden space makes it easier for an employee to peep on impulse. In the physical world, it takes a significant amount of nerve to walk into a locked room or to open a locked file drawer. On a computer, a person might peep at those George Clooney pictures or Obama records all in an instant. People acting on impulse can easily underestimate the likelihood that their unauthorized access will come to the attention of an audit system at a later date.[78]

---

77. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007); SIMSON GARFINKLE, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY (2001); Jack Lerner & Deirdre Mulligan, *Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3, 15 (2008).

78. Even if they correctly estimate the risk, people who act on impulse, similar in this respect to addicts, may act contrary to their self interest when giving into the impulse. *See generally* Robert Cooter, *Models of Morality in Law and Economics: Self-Control and Self-Improvement for the 'Bad Man' of Holmes*, 78 B.U. L. REV. 903 (1998). A related insight comes from Katherine Strandburg, who describes reasons why people may wish to take privacy-protecting actions but do not achieve their wishes. Katherine J. Strandburg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 RUTGERS L. REV. 1235, 1241-42 (2005).

The shift to electronic files and databases has also allowed for a more easily traceable electronic footprint. In the past, when an employee goes into a locked room or a locked file drawer to look at forbidden files, the chance of detection after an incident of peeping was usually slight. By contrast, few employees know all the intricacies of the logging and audit software in a modern computer system. In many systems, the audit logs might be reviewed much later, perhaps after suspicion of an incident. Once the investigation begins, a peep can potentially be detected, even months or years later.

Furthermore, peeping gets discovered more often now because of the ease of disseminating information. In the paper-based world, the peeper would often keep the knowledge close, perhaps gossiping with a few friends. In the world of blogs and the Drudge Report, the barriers to propagation are much lower. Juicy gossip by its nature is often repeated. When the gossip is in a blog or an often-forwarded email,[79] the details in the original revelation can be readily spread to a mass audience. Once the peeping is widely known, as with the examples cited at the beginning of this Article, there is greater pressure to "do something" to punish the violator.

With this greater pressure to act, the shift from paper files to electronic, audited systems also affects the way that peepers are detected and punished. In a paper-based world, the perpetrator is caught locally, such as by a co-worker who happens to spot a violation. The punishment is likely to be local as well—the sort of shaming or administrative sanction that occurs for other local and non-criminal violations. By contrast, a peeper into the electronic database may be discovered by an auditing specialist or in the course of an actual investigation. The informal sanctions within the work community can then give way to more formal sanctions within the hierarchy.

Finally, the growing prevalence of data breach laws and reports of peeping in the press have likely increased the official attention paid to peeping incidents in an organization. Managers and IT administrators now run a greater risk of criticism if they become aware of a peeping violation but do nothing about it.

---

79. My own perspective on often-forwarded emails is formed in part by the widely circulated email exchange from 2000 of Ms. Claire Swire (no relation) and her male friend, Bradley Chait. The story of the off-color email is told at Snopes.com. *Under the Yum-Yum Tree*, SNOPES, http://www.snopes.com/risque/tattled/swire.asp (last visited June 19, 2009). On the day of this writing, the charming email comes up next to my own home page on a Google search for "Swire."

V. WHAT TO DO ABOUT PEEPING?

This Article on peeping seeks to focus our attention at the issue—to gaze at it—rather than to perform a comprehensive cost/benefit analysis of the possible response. The discussion above indicates that peeping is likely more common in our database-filled world and that it is likely to be detected more often, especially because of the audit and logging features of modern computer systems.

At least two contradictory impulses affect our opinion of peeping. The first is whether the "harm" is a serious one. One strand of privacy law in recent years has focused on the concrete, and often financial, "harms" caused by privacy invasions. Enforcement efforts have focused on topics such as identity theft, where an individual can have a bank account hijacked or suffer other monetary loss. Other regulatory efforts have focused on sensitive medical and financial information, where improper leaks of medical data might lead to loss of insurance, or improper data in a credit history could lead to mistaken denial of a mortgage or other loan. By contrast, there is usually no similar financial harm from simple peeping, whether it is an employee looking at the Obama passport photo, Joe the Plumber's motor vehicle records, or an ordinary individual's records. On the view that "harm" means concrete economic harm, peeping appears like a trivial matter, unworthy of legal or policy attention.

The contradiction arises when the press reports, for Joe the Plumber's records, that "[t]he agency's actions drew outrage from across the nation."[80] The stories of Tiresias and Lady Godiva suggest a deep historical and psychological concern about peeping—something important is going on here.

A parallel contradiction arises in terms of the appropriate punishment for peeping. Along with the ancient stories that impose harsh punishments for peeping, there exists federal precedent for treating peeping quite seriously. Unauthorized inspection of federal tax returns, for instance, can lead to imprisonment for up to a year, and federal employees are stripped of civil service protections and mandatorily dismissed from office upon conviction.[81] In addition, federal agency codes of conduct under the Privacy Act provide that records may only be disclosed to employees who have a legitimate need to access the records in the course of official duties.[82] On the other hand, any employee who quickly peeped at George Clooney's x-rays would believe that

80. *See supra* note 24.

81. 26 U.S.C. § 7213A (2006).

82. *E.g.*, Social Security Administration Employee Standards of Conduct, 20 C.F.R. § 401, App. A, (54d)(1)(c) (2007).

blindness, or even a year in jail, is an excessive punishment. The employee would argue that the peeping was at most a social misdemeanor, something one should not do perhaps, such as gossiping a bit too much or too nastily, but not an offense that would warrant such severe sanctions.

In facing these contradictory impulses, the prudent course is to find ways to prevent the temptation to peep and reduce its prevalence. A basic principle of privacy law is that there should be "appropriate administrative, technical, and physical safeguards." Such language appears, for instance, in the Privacy Act of 1974[83] and in the HIPAA medical privacy rule.[84] Many of the most promising responses to the risk of peeping are either technical or administrative safeguards. Though physical safeguards, such as preventing a stranger from seeing a celebrity's medical records, they are appropriate going forward, they are less likely to be the crucial measures for preventing peeping into databases.

A. TECHNICAL SAFEGUARDS

Many of the best responses to peeping are technical safeguards. Although a complete security system includes numerous safeguards, the discussion here will briefly examine four of them: role-based access control, special treatment for famous or very important persons (VIPs), masking and de-identification techniques, and audit logs. Each of these measures is used by state-of-the-art systems today. These measures are more commonly deployed in the health care sector, which is regulated and has a long history of confidentiality. However, the risk of peeping suggests that these safeguards should be deployed more widely and consistently.

1. Role based access controls.

Role based access control (RBAC), also called role-based security, is a computer security technique for assuring that only people in authorized "roles" can do particular activities in a computer system.[85] Effective deployment of RBAC, for instance, could limit who could access the files of a celebrity or other individual. The academic understanding of RBAC has devel-

---

83. 5 U.S.C. § 552a(e)(10) (2006). The statute says that the safeguards are to protect "against any anticipated threats or hazards" that "could result in substantial harm, *embarrassment*, inconvenience, or unfairness to any individual on whom information is maintained." *Id.* (emphasis added) The inclusion of "embarrassment" on the list shows recognition of a sort of harm that can happen to a person from peeping, even if there is no tangible financial loss.

84. 45 C.F.R. § 164.530(c) (2006).

85. National Institute of Science and Technology, Computer Security Division, Computer Security Resource Center, Role Based Access Control (RBAC) and Role Based Security, http://csrc.nist.gov/groups/SNS/rbac/ (last visited June 19, 2009).

oped considerably in the past fifteen years.[86] The American National Standards Institute adopted an industry consensus standard for RBAC in 2004,[87] and most information technology vendors have now incorporated RBAC into their product lines.[88]

The increased use of RBAC, perhaps combined with purpose-based access controls,[89] would reduce the range of employees in an organization who could peep into an individual's files. For instance, persons treating a patient or doing customer service for an individual would have access to files, but other employees would not. The HIPAA privacy rule contained a requirement that only the "minimum necessary" personal health information be used or disclosed by a hospital or other covered entity.[90] The rule announced the principle of role-based access:

> A covered entity must identify: (A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and (B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.[91]

Currently, RBAC is likely deployed most commonly in sophisticated computer systems and those that are regulated by HIPAA to use or disclose only the minimum necessary information. RBAC is less widely used in smaller and less sophisticated systems, including for smaller medical practices.[92]

---

86. National Institute of Science and Technology, Computer Security Division, Computer Security Resource Center, Role Based Access Control—Frequently Asked Questions, http://csrc.nist.gov/groups/SNS/rbac/faq.html (last visited June 19, 2007).

87. INCITIS, AMERICAN NATIONAL STANDARD FOR INFORMATION TECHNOLOGY—ROLE BASED ACCESS CONTROL 359 (2004), *available at* http://www.cs.purdue.edu/homes/ninghui/readings/AccessControl/ANSI+INCITS+359-2004.pdf.

88. National Institute of Science and Technology, Computer Security Division, Computer Security Resource Center, Role Based Access Control (RBAC) and Role Based Security, http://csrc.nist.gov/groups/SNS/rbac/ (last visited June 19, 2009).

89. Computer scientist Annie Anton commented that role-based access (e.g., doctor, IT manager) should be enhanced with purpose-based access (treatment, system security), which may be more granular and less subject to a highly privileged role getting access to too many records. For a discussion of purpose-based access, see Naikuo Yang et al., *A Purpose-Based Access Control Model*, 1 J. INFO. ASSURANCE & SEC. 51 (2008).

90. 45 C.F.R. § 164.514(d)(2) (2006).

91. *Id.* The requirement to comply with these minimum necessary standards, however, does not mean that all health care providers have implemented the formal, complete systems that researchers would consider fully RBAC systems.

92. The HIPAA privacy rule is "scalable," meaning that entities may take into account the cost burden of implementation, consistent with the entity's size and sophistication, when

However, a significant limitation of RBAC remains. Peeping can occur by all those whose "roles" allow them access to the full file. For instance, a number of the medical peeping incidents involved doctors and nurses whose role provided them access to the files (but who were not supposed to be looking at non-patients such as the celebrities at issue).[93]

Regardless, RBAC is a promising path for reducing the range of employees who can peep into files. In short, RBAC should be more widely deployed in the future, and will provide a significant but incomplete protection against peeping.[94]

2. VIP Treatment

The experiences of Senator Obama and movie stars such as George Clooney are recent evidence that VIPs are especially likely to be the subject of peeping. One logical response is to provide additional safeguards for these VIP files.

Based on my experience with medical providers and others, this sort of VIP treatment was often done in paper-based records. In a paper-based world, the safeguards are relatively easy to create: a supervisor and perhaps a small set of trusted persons have keys to the special file cabinet. In that way, file clerks and other employees cannot gain access to the VIP files except with the permission of the supervisor.

Creating a VIP system is more complex in a modern computerized system, such as a health system where a wide range of persons often has access to a patient record for purposes of treatment, payment, and health care oper-

---

deciding how to comply with certain provisions. 45 C.F.R. § 164.306(b) (2006). In addition, HHS has provided considerable flexibility about how to implement the role-based requirements: "[T]he Privacy Rule provides the covered entity with substantial discretion with respect to how it implements the minimum necessary standard." U.S. Dept. of Health & Human Services, Health Information Privacy, HIPAA, Frequently Asked Questions, http://www.hhs.gov/ocr/privacy/hipaa/faq/limited/208.html (Last visited Oct. 7, 2009).

> [The] covered entity is in the best position to know and determine who in its workforce needs access to personal health information to perform their jobs. Therefore, the covered entity may develop role-based access policies that allow its health care providers and other employees, as appropriate, access to patient information, including entire medical records, for treatment purposes.

Id.

93. *See supra* Part II (discussing recent medical peeping incidents).

94. For a recent account of RBAC, which is generally consistent with the approach in this essay, see Brian Cleary Aveksa, *Peeping on Celebrity Files—How to Gain Control*, ZDNET, Feb. 24, 2009, http://news.zdnet.com/2100-9595_22-272326.html.

ations.[95] Because such a wide range of employees has reason to access a medical record, and employees expect instant access to do their jobs, it can become a daunting technical challenge to enable effective care, billing, and other services for the VIP while not exposing the VIP's records to a large number of employees.

Despite these technical challenges, major health care organizations have recognized the importance of creating special handling procedures for VIPs. The American Health Information Management Association, for instance, states: "Special circumstances may arise in which patient identification or access to individual patient records may require anonymity or special precautions, such as in the case of celebrity or high-profile individuals, workplace privacy, domestic violence, child or vulnerable adult abuse, litigation, organ donors, and prisoners."[96] Similarly, the importance of VIP treatment is built into the coding system for health care records developed by Health Level 7 (HL7), a major health standards body.[97] HL7 has developed a structured code set to govern access to confidential medical records. The code set includes a "C" for "celebrity," and states: "Celebrities are people of public interest (VIP) including employees, whose information require special protection."[98]

In many respects, creating special rules for access to VIP files is an example of role-based access—the rules are stricter about which "roles" are able to access those records. VIP procedures can employ a variety of techniques. For instance, the VIP might use an alias, her records might not be visible in the system unless a code is provided, the record might say that a supervisor's permission is needed for access, or there could be a warning that access is audited and unauthorized access will lead to penalties. VIP files might also be subject to more intensive auditing, as discussed further below.

Looking ahead, the increased incidence of peeping suggests there should be renewed attention by software designers and system administrators to the

---

95. For analysis of the wide range of uses of a modern health record in the United States, see Charles Safran et al., *Toward a National Framework for the Secondary Use of Medical Information*, AMERICAN MEDICAL INFORMATION ASSOCIATION, Sept. 2006, *available at* http://www2.amia.org/inside/initiatives/healthdata/2006/finalpapertowardanationalframeworkforthesecondaryuseofhealthdata_09_08_06_.pdf.

96. Linda Barbera et al., *Ensuring Security of High-Risk Information in EHRs,* 9 J. AHIMA 79 (2008), *available at* http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_039956.hcsp?dDocName=bok1_039956.

97. "Health Level 7 is one of several American National Standards Institute (ANSI)-accredited Standards Developing Organizations (SDOs) operating in the healthcare arena." Health Level 7, *What is HL7?*, http://www.hl7.org/ (last visited June 10, 2009).

98. Health Level 7, *High-Level Overview of the Health Level Seven (HL7): Consent related vocabulary including Confidentiality Codes*, http://www.oasis-open.org/committees/download.php/30930/hl7confidentialitycodes.doc (last visited June 10, 2009).

usefulness of VIP sub-systems within larger computer systems.[99] Creating manageable VIP systems may deserve greater attention in information sharing systems, such as proposed new national systems for electronic medical records. It may seem un-egalitarian and perhaps even un-American to give "special" treatment to the records of some individuals. The experience of Joe the Plumber, who suddenly became famous and then was subject to peeping in the same week, shows the need for good systems that apply to all persons. Nonetheless, the recent peeping incidents have largely involved persons who were already famous, and we should update our ways to handle those records securely.

3. Masking and de-identification

A promising way to stop peeping is to use technical measures that mask the identity of the individual or perhaps entirely de-identify the records. Masking techniques such as encryption and one-way hashes should be strongly encouraged for many security reasons, as well as to reduce the incidence of peeping.

To take a well-known example, data can be encrypted on a hard drive or when being sent to another person. If the hard drive is lost, or a hacker intercepts the communication, the encryption can make it difficult or impossible for the outsider to read the data. This sort of encryption can be effective as well at preventing employees from peeping at data. For instance, if an employee gains access to a hard drive or computer file, but does not have the encryption key, then the employee cannot peep at the data.

Another important category of masking techniques is called the "one-way hash."[100] Essentially, this technique employs mathematical functions that are simple to compute in one direction but very hard to compute in the opposite direction. Applied to personal information, a one-way hash would convert "Peter Swire" to something like "X145-GHWR-T89G." The same one-way hash could be computed each time that "Peter Swire" was run through the mathematical calculator, but it would be very difficult to figure out the name "Peter Swire" if you only have the "hash" of that name.

---

99. One response by the State Department to the passport peeping incidents was to increase the number of persons on the list of people subject to VIP procedures. United States Department of State and the Broadcasting Board of Governors, Office of Inspector General, *Review of Controls and Notification for Access to Passport Records in the Department of State's Passport Information Electronic Records System (PIERS)*, AUD/IP-08-29, 39-42 *available at* http://oig.state.gov/documents/organization/109112.pdf (last visited June 10, 2009).

100. For a concise explanation of one-way, or cryptographic, hashes, see Wikipedia, *Cryptographic Hash Function*, http://en.wikipedia.org/wiki/One-way_hash (last visited June 10, 2009).

These one-way hashes can be useful in a wide range of settings where a person's data is shared but only with the person's identity masked by the one-way hash. If the information sharing is structured properly, then the sharing can allow linkage of records of the same person's records, and most or all of the people involved will not know the actual identity of the person. For medical records and other records that today are shared in multiple systems, greater use of one-way hashing will permit the data usage to go forward while masking the identity of the individuals. In short, there can be a range of data uses, while avoiding the risk of peeping.[101]

I recently drafted comments on this topic with the Markle Foundation, the Center for Democracy and Technology, and others.[102] U.S. Department of Health and Human Services (HHS) has proposed the first national guidelines for data breaches involving personal health information. The proposed guidelines include an exclusion for entities employing strong encryption: where effective encryption is in place, covered entities will not need to send notices in the event of a data breach. However, our recently drafted comments emphasize that such notice exclusions should be available only to databases and data formats resistant to unauthorized access.[103] These limited exclusions should incentivize entities who store personal health care data to use state of the art protections and technologies.[104] By encouraging use of effective encryption and one-way hashing, there will be stronger technical barriers in place to prevent peeping.

While we should encourage the use of masking technologies, they are certainly no panacea. Modern computer security researchers, including LaTanya Sweeney,[105] have shown serious challenges to successful masking of data. This research provides strong reason to consider administrative safeguards, such as nondisclosure contracts, in addition to technical measures for de-identifying data.[106] The basic insight from the researchers is simple and

---

101. For applications to the health care sector, see PETER P. SWIRE, RESEARCH REPORT: APPLICATION OF IBM ANONYMOUS RESOLUTION TO THE HEALTH CARE SECTOR (2006), *available at* http://www.peterswire.net/anon.resolution.whitepaper.pdf.

102. Peter P. Swire, *CAP Comments on HHS Health Data Breach Guidelines*, CENTER FOR AMERICAN PROGRESS, May 22, 2009, *available at* http://www.americanprogress.org/issues/2009/05/data_breach_comments.html. The filed comments are available at http://www.americanprogress.org/issues/2009/05/pdf/MarkleCDTCAPGuidanceComments.pdf.

103. *Id.*

104. *Id.*

105. Dr. Latanya Sweeney's Home Page, http://privacy.cs.cmu.edu/people/sweeney/ (updated Fall 2007).

106. I have participated in a process with the Health Privacy Project of the Center for Democracy and Technology to make recommendations on how to update the de-identification provisions of the HIPAA privacy rule. One theme emerging from this process

profound. In a world of effective search engines, a researcher can often narrow down the identity of people using information available on the Web, and those searches become even more likely to be effective in a world of social networking, where individuals regularly reveal their date of birth and other revealing information.[107]

Although techniques exist to unmask data in some circumstances, peeping will be less common if masking techniques are widely adopted. The above discussion of "the gaze" and "the gossip" showed that peeping can arise from a spur-of-the-moment impulse to see something intriguing or tell others about the tidbit. This sort of peeping is far less likely to occur if the cost of peeping includes tricky encryption research to unmask the hidden identity of individuals. As stated in the recent comments, the use of masking techniques such as encryption and one-way hashing will result generally in better data protection than their absence. The possibility of attacks by determined experts should not detract from the usefulness of protections that prevent accidental or casual data losses.

4. Logging and audits

Effective auditing is a crucial safeguard against peeping. Computerized systems can readily log actions by employees and audit those logs after the fact. Auditing provides the ability to deter, detect, and prove violations of a security policy.[108] The ability to perform audits serves as a deterrent because system users would know in advance that logging and auditing are being used to identify policy violations, such as peeping. The perception that a system is effectively logged and will be audited can thus reduce violations by users.

---

is the important of supplementing technical measures with data use agreements and other administrative safeguards. *See* Posting of Lygeia Ricciardi to PolicyBeta Blog, Health Data De-Identification Rules in Need of Update?, http://blog.cdt.org/2008/11/13/health-data-de-identification-rules-in-need-of-update/ (Nov. 13, 2008).

107. Date of birth is especially individuating because it splits the population into over 25,000 categories (366 days of birth times 80 years equals 28,880 categories). By contrast, a data field for gender splits the population into two categories in most systems; so labeling someone "male" or "female" is far less likely to identify an individual uniquely than providing date of birth.

108. The discussion here closely follows an auditing paper for which technologist Jeff Jonas and I were lead authors. Markle Foundation, Markle Task Force on National Security in the Information Age, *Implementing a Trusted Information Sharing Environment: Using Immutable Audit Logs to Increase Security, Trust, and Accountability*, 6 (2006), *available at* http://www.markle.org/downloadable_assets/nstf_IAL_020906.pdf. For auditing in the context of sharing of electronic health records, see *Auditing Access to and Use of a Health Information Exchange*, *in* THE CONNECTING FOR HEALTH COMMON FRAMEWORK (Markle Foundation, 2006), *available at* connectingforhealth.org/commonframework/docs/P7_Auditing_Access.pdf.

Detection occurs when an actual policy violation is uncovered after the fact. Detection can occur as a result of sampling, when one of the transactions selected for random audit reveals a violation. Detection can also occur in the context of a specific investigation, when the actions of a suspect are examined carefully and a violation is detected. If there is a credible record-keeping system in place, audits can be used to create evidence of a violation.

The ability of logging and auditing to deter, detect, and prove policy violations is enhanced for computer-based as compared to paper-based systems. It is true that paper-based systems create logs of activities: "sign here to take out this file or library book." In practice, however, logs of computer activity are generally more automatic and comprehensive. For instance, modern software systems routinely audit each access to a corporate database, generate reports for managers of anomalous activity, and provide detailed logs in the event of an investigation.[109] The amendments to HIPAA in the American Recovery and Reinvestment Act of 2009, for instance, require greatly increased accounting of access to files for all computerized systems as of January 1, 2014.[110] Few paper-based systems in practice match this level of detailed logging and auditing.

As discussed above, the existence of computerized logging and auditing is a major reason to expect greater detection of peeping in the future. With the increased investment over time in computer security,[111] detailed logging and auditing are becoming increasingly standard features of a wider range of computerized activities.

This increased deployment of logging and auditing is a good trend for computer security in general and addressing peeping in particular. Auditing can raise issues of employee privacy, and best practices should be deployed so that the auditors themselves do not peep.[112] To address peeping, however, perhaps the best single policy to use with audits is to announce to employees that the logging and auditing are occurring. For instance, users of a hospital computer system might see a warning once a week or once a month such as this: "Your access to patient medical records is audited. Accessing patient

109. I gained experience with database audit systems when I served on the Advisory Board to Sentrigo, Inc., a software company that provides database security solutions. SENTRIGO, www.sentrigo.com (last visited June 10, 2009).

110. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).

111. On the relatively recent rise of cybersecurity as a policy concern, see Peter P. Swire, *Elephants and Mice Revisited: Law and Choice of Law on the Internet*, 153 U. PA. L. REV. 1975, 1977-78 (2005).

112. My previous work on audits has addressed this concern in various ways, including proposals for how to audit the auditors. Markle Foundation, *supra* note 108.

records outside of those needed for your work will be detected and can lead to serious consequences, including termination of employment. For further information, see our organization's auditing policy." This sort of warning, along with appropriate training, can improve the deterrence effect of auditing on peeping.[113]

B. ADMINISTRATIVE SAFEGUARDS.

Administrative safeguards complement the available technical measures. These administrative safeguards include: training and employment sanctions; a data breach requirement for peeping; and possibly other measures that help teach employees that peeping is not appropriate.

1. Training and Employment Sanctions

One obvious measure to address peeping is to train employees not to do it. The recent high-profile cases can send this message to employees in stark terms: the State Department fired contractors who looked at the passport files, UCLA fired people who looked at Britney Spears' files, over forty employees were suspended for looking at George Clooney's medical files, and a senior official in Ohio resigned in the wake of peeping into Joe the Plumber's files. This sort of training is exceptionally easy: show intriguing pictures of Britney Spears and George Clooney to get everyone's attention, followed by a simple slide: "FIRED".

I suggest that the recent peeping cases are analogous to the Anita Hill case. The language we use about peeping is similar to the way sexual harassment was often described prior to the 1991 confirmation hearings for Justice Clarence Thomas, where Anita Hill presented evidence of sexual harassment when she worked for Thomas.[114] The description goes roughly like this: "It may be a bit improper, but it is a normal part of the workplace. People are just like that, and give in to the understandable temptation to do it. It is not worth making a big legal fuss over, though, and people certainly shouldn't be fired or pay large damages due to it." Read that quote as it applied to sexual harassment before 1991, and as it applies to peeping today.

I am not saying that peeping at a person's files is the same as sexually harassing that person. Instead, I am pointing out there are episodes when our society comes to realize that behavior is occurring that deserves to be treated more seriously than previously. The Clarence Thomas hearing was such a

113. If an auditing program is announced to employees, but employees learn over time that no enforcement occurs, then the deterrence effect would obviously be reduced.

114. *See* Susan K. Hippensteele, *Mediation Ideology: Navigating Space from Myth to Reality in Sexual Harassment Dispute Resolution*, 15 AM. U. J. GENDER SOC. POL'Y & L. 43, 44-45 (2006).

moment for sexual harassment, and the recent passport and other episodes may constitute such a moment for peeping. There are various reasons for believing peeping is a significant issue worth addressing—the concluding discussion in this paper, about online behavioral advertising, suggests that controlling peeping is a key part of controlling the enormous new data collections that occur with modern computer technology.

In terms of policy recommendations, training about peeping can become a more regular part of the training that many organizations already provide about computer security, including complying with medical, financial, and other specialized privacy and security laws. Training should be especially prominent for employees who have regular access to many celebrity and other sensitive records. Institutions should consider writing formal policies about peeping, as they have done for sexual harassment and other compliance issues. And suspension, firing, and other job actions should continue to be imposed, as they have been in recent peeping cases.

2. Data breach notices for peeping

Since California enacted the first data breach statute in 2003, the vast majority of states have passed laws requiring notice to individuals when unauthorized persons breach security and gain access to Social Security Numbers, financial account numbers, and other sensitive information.[115] The rising incidence of peeping poses the question of whether such statutes should extend to peeping.

There is at least one significant distinction, however, between the traditional data breach notice and a peeping notice. One rationale for the data breach notice is that it alerts the individual to possible identity theft, such as where the Social Security Number or credit card number has been compromised.[116] The notice can thus prompt individuals to monitor their credit history more closely or take other protective measures. By contrast, it is unclear what an individual should do upon receipt of a peeping notice.

That question returns us to the issue of appropriate punishment for peeping. California once again broke new ground by passing what I believe is the first statute requiring notices for peeping. Governor Schwarzenegger signed Senate Bill 541 and Assembly Bill 211 on September 30, 2008, and the

115. *See* Milton Sutton, *Security Breach Notifications: State Laws, Federal Proposals, and Recommendations*, 2 ISJLP 927 (2006) (collecting and analyzing state data breach laws). Perhaps the Governor's own celebrity status made him more inclined to support a law that responded to peeping into celebrities' medical files.

116. Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 955-58 (2007).

laws took effect on January 1, 2009.[117] The new laws are somewhat complex.[118] For our purposes, the key definition is what counts as "unauthorized access." It is "the inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment, or other lawful use."[119] For this peeping, this "unauthorized access," a report must be sent to the affected patient or patient's representative and to the California Department of Public Health (CDPH) no later than five calendar days after violation has been detected by the facility.[120] CDPH may assess an administrative penalty of up to $25,000 per patient whose medical information was unlawfully or without authorization accessed, used, or disclosed, and fines of $100 per day can begin after the five days.[121]

The new California laws impose administrative fines on the organization, and the organization quite possibly will suspend, fire, or impose other employment penalties on the person who peeps. In my view, the California approach to penalties is a plausible one.[122] Appropriate responses by the organ-

---

117. S.B. 541, 2007–2008 Reg. Sess. (Cal. 2008); A.B. 211, 2007–2008 Reg. Sess. (Cal. 2008).

118. For two law firm analyses of the new bills, see Shirley P. Morrigan & M. Leeann Habte, *California AB 211, SB 541 with Guest Foley & Lardner*, Feb. 25, 2009, http://www.fairwarningaudit.com/documents/2009-0225-AB211-SB541-FW-FOLEY-FULL.pdf; Kevin D. Lyles & Colin Leary, *California Expands Medical Privacy Laws with New Standards, Oversight, and Administrative Penalties*, JONES DAY, Dec. 2008, http://www.jonesday.com/pubs/pubs_detail.aspx?pubID=S5675.

119. CAL. HEALTH & SAFETY CODE § 130201(e) (2008).

120. CAL. HEALTH & SAFETY CODE § 1280.15(b)(1)-(2) (2008).

121. CAL. HEALTH & SAFETY CODE § 1280.15(a), (c) (2008).

122. CAL. HEALTH & SAFETY CODE § 1280.15 (2008). As one additional administrative measure, we can consider a suggestion raised in conversation with me by David Brin, the science fiction writer who wrote The Transparent Society. DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998). One of Brin's major themes is reciprocity. For instance, he suggests that the remedy for too many police video cameras is for the public to be able to watch video feeds of the police offices as well. For peeping, Brin asked me to imagine that the peeper's own records would be turned over to the person who was the subject of peeping. For instance, a file clerk who peeped at George Clooney's records would have her own records sent to him. I don't think I support this as an actual public policy matter. But I find it an intriguing thought experiment. Brin is essentially enforcing the Golden Rule, where you should do unto others as you would have them do unto you. Brin is using an age-old device of the parent to the misbehaving child: "Don't look at that person's photos and file. How would you like it if the kids at school were looking at those awful pictures of you from when you were sick last year?" Brin's suggestion shows the element of personal moral choice that the person faces when he or she is tempted to peep. This essay suggests a number of technical and administrative safeguards to reduce the problem of peeping. A related "safeguard" is to raise awareness about why peeping is not appropriate, and to find a fuller set of ways to communicate that it is wrong to peep. Otherwise, in our world of pervasive databases, the incidence of peeping may become unnecessarily great. The Anita Hill incident exemplifies how a con-

ization can reduce the fine, and small organizations are not held to as strict a standard for their systems as large organizations. In short, the approach is to have significant enough financial penalties to induce compliance, but to limit the size of the penalties so they do not spiral out of control.

An intriguing question is whether California's new peeping bill will spread across the country the way that its data breach bill did. One advantage of the peeping bill is that it sends a clear message of public morality—employees are not supposed to peep at patients' medical records.[123] A related argument for the peeping notice bill is that the notices will prompt organizations to take peeping more seriously, helping ensure that technical and other safeguards are put in place.[124] From my own experience working with organizations on data breaches, a breach and the accompanying notices prompt management and employees to examine their practices and often to change them. For instance, it might be easier for an organization to justify investing in masking and auditing technologies once it has gone through the experience of sending notices about a data breach or peeping incident. This improvement in data practices may well justify adopting the California peeping notice approach to a wider range of circumstances.

VI. PEEPING , PRIVACY "HARMS," AND BEHAVIORAL ADVERTISING

This Article has tried to begin a conversation about the topic of peeping. The Article has discussed our deep ambivalence about the phenomenon—it is a serious violation to peep at the records of candidate Obama, Joe the Plumber, or a movie star, but then again it is an understandable human foible that leads us to peep and then gossip about it.

---

sciousness-raising incident can educate a broader public that a practice, such as sexual harassment, is illegal. On consciousness-raising, see Judith Resnick, *Gender, Race, and the Polictics of Supreme Court Appointments: The import of the Anita Hill/Clarence Thomas Hearings: Hearing Women*, 65 S. CALIF. L. REV. 1333, 1333-35 (1992); Noelle Brennan, *Hostile Environment Sexual Harassment: The Hostile Environment of a Courtroom*, 44 DEPAUL L. REV. 545, 545 (1995).

123. On the ability of law to express norms and moral values, see Richard H. McAdams, *The Legal Construction of Norms: A Focal Point Theory of Expressive Law*, 86 VA. L. REV. 1649, 1717-19 (2000); Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338, 397-400 (1997).

124. For evidence that data breach notice laws have led to greater funding for computer security and stricter data practices, see CHRIS JAY HOOFNAGLE & JENNIFER KING, SECURITY BREACH NOTIFICATION LAWS: VIEWS FROM CHIEF SECURITY OFFICERS 20-21 (Samuelson Law, Tech. & Pub. Pol'y Clinic 2007), *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/cso_study.pdf.

Upon reflection, I have come to the view that we do sympathize with the employee who gives in to temptation and peeps at the intriguing file. But we also want the *system* to protect us from being the target of peeping.

This insight—the importance of the system protecting us from peeping—bears directly on important current privacy debates and the definition of what counts as a privacy "harm." A major current debate concerns behavioral advertising online.[125] The FTC states that "[o]nline behavioral advertising involves the tracking of consumers' online activities in order to deliver tailored advertising."[126] Proponents of behavioral advertising cite various benefits. Individuals can benefit from personalization, such as by having content or advertisements that better fit the individual's interests.[127] Companies can benefit from targeted advertisements, getting their messages out to the most relevant consumers.[128] Even more broadly, an emerging argument is that behavioral advertising is essential to pay for "free" content online—this type of advertising is the last, best hope for the newspaper industry to pay for investigative journalism and the other expenses of an independent news media.[129]

Defenders of privacy have offered various explanations about what is worrisome about behavioral advertising. One line of argument, advanced by Jeff Chester and others, is that behavioral advertising is bad due to the manipulation inherent in other types of advertisement, only more so.[130] A First Amendment argument, to counter the idea that advertising helps newspapers,

---

125. *See* F.T.C. STAFF, SELF REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 47-48 (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf; Peter P. Swire & Annie I. Antón, *In Regards to the FTC Staff Statement, 'Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles,'* April 10, 2008, *available at* http://www.ftc.gov/os/comments/behavioraladprinciples/080410swireandanton.pdf; *see also* PeterSwire.net, Behavioral Advertising, http://www.peterswire.net/psbehavioraladvertising.htm (last visited June 20, 2009) (papers from seminar on Behavioral Advertising).

126. F.T.C. STAFF, SELF REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 8, (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

127. *Id.*

128. *Id.* at 3.

129. Thomas M. Lenard & Paul H. Rubin, *In Defense of Data: Information and the Costs of Privacy*, TECH. POL'Y INST. 23 (2009), *available at* http://www.techpolicyinstitute.org/files/in%20defense%20of%20data.pdf. For a somewhat similar approach, see J. Howard Beales III, Public Goods, Private Information, and Anonymous Transactions: Providing a Safe and Interesting Internet (May 7, 2009) (on file with author).

130. Posting of Jeff Chester to Digital Destiny, Tracking You Offline for Better Targeting You Online: Why the FTC and Congress Need to Protect Consumers, http://www.democraticmedia.org/jcblog/?p=817 (May 26, 2009); *see generally* Postings of Jeff Chester to Digital Destiny, http://www.democraticmedia.org/jcblog/.

is what Julie Cohen has called the "right to read anonymously."[131] Under this argument, and as recognized historically by special privacy laws for cable television and newspapers,[132] it is risky to have the content of what we read or see be subject to surveillance. Next, there are concerns that the government might seize the browsing data for national security, law enforcement, or other surveillance purposes. The most widely made privacy argument to date, perhaps, has been the reaction that it is somehow "creepy" to have everything we browse go into giant databases.[133]

I suggest that this article's analysis of peeping contributes a major insight to the behavioral advertising debate. If there is widespread peeping into the behavioral advertising databases, then that is a big problem. In a world with a lot of peeping, the price of celebrity climbs steeply. Peeping struck candidate Obama for his passport and cell phone records, and Joe the Plumber for becoming prominent in a presidential debate. Going forward, would peeping apply to every website the next candidate or suddenly famous person ever visited?

Writing in 2000, before the current state-of-the-art of behavioral advertising, Jeffrey Rosen in *The Unwanted Gaze* emphasized the problem that one incident could be taken out of context to caricature an individual and harm that person's entire career or reputation.[134] When it comes to web surfing, very many individuals have gone to some site that would be embarrassing or worse if it became known to co-workers, family members, or voters. I submit that a major concern about behavioral advertising is this thus-far-badly-articulated fear of peeping. In a world where a database exists that contains such detailed surfing history, a large portion of us could be harmed by a peeping incident.

As a policy response, effective anti-peeping measures are thus a logical part of whatever form of online advertising develops in the coming years. Technical measures can be put in place, including role-based access, audit

---

131. *See generally* Julie E. Cohen, *A Right to Read Anonymously: A Close Look at 'Copyright Management' in Cyberspace*, 28 CONN. L. REV. 981 (1996); Julie Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 BERKELEY TECH. L.J. 161 (1997).

132. Privacy Protection Act of 1980, 42 U.S.C. § 2000aa (2006) (limiting access to records of newspapers and other media); Cable Television Privacy Act of 1984, 47 U.S.C. § 551 (2006) (limiting access to cable television programs viewed by subscribers); *see also* Tattered Cover, Inc. v. City of Thorton, 44 P.3d 1044, 1053 (Colo. 2002) (setting higher standard for discovery of books and other reading material).

133. *E.g.*, Neil Munro, *The Ever-Expanding Network of Local and Federal Databases*, 45 COMM. ACM 17, 17-19 (2002).

134. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000).

logs, masking of individual identity, and deletion after a relatively short time. Legal and administrative measures can also be implemented, including training, announcement of job sanctions for peeping, and perhaps the notices of peeping discussed above.

For behavioral advertising, it has become technically very complex for an individual to avoid the tracking done in the name of online advertising. When individual choice is difficult to implement, then the challenge is how to build a *system* that protects the individual's interests. Unless the systemic problem of peeping is effectively addressed, then critics of behavioral advertising retain a powerful critique of current practices. We have seen instances of peeping into supposedly sensitive databases such as medical and phone records, so we should not blithely assume it will be absent from the oh-so-interesting databases now being created of every web site that we ever visit.

More optimistically, the risks from behavioral advertising are reduced if we have effective technical and administrative controls against peeping. If the system is trustworthy, then the harms from the databases of surfing are less. It is relatively rare for the government or a litigant to need access to a record, and even rarer for the advertising database to be the subject of a search warrant or subpoena. (Once a police investigation or civil litigation gets started, the prime databases are likely to be a bank or telecommunications provider, rather than advertisers who may have set a cookie to track where a user browsed.)

The recent experience of our political and entertainment celebrities, however, does not support such optimism. Peeping seems increasingly common, and we will need to work much harder to pull down the blinds and otherwise create peace of mind that we will not fall victim to it.

VII. CONCLUSION

Phenomena such as peeping, gossip, and voyeurism are social and psychological issues rather than purely legal ones. With the increasing prevalence of detailed databases, a far larger number of employees can have access to the pictures, reading habits, and activities of politicians, celebrities, neighbors, family members, and anyone else.

Technical and administrative measures that can reduce the incidence of peeping. Probably even more importantly, high-profile examples of peeping should be lessons for our society. The traditional punishment for peeping was blindness for Tiresias and Peeping Tom, and being turned into stone for Lot's wife. The power of these stories is to teach us, or remind us, of the seriousness of the unwanted gaze.

PRIVACY AND THE THIRD HAND: LESSONS FROM THE COMMON LAW OF REASONABLE EXPECTATIONS

By Richard A. Epstein[†]

TABLE OF CONTENTS

I. INTRODUCTION

The purpose of this Article is to offer some reflections on the Third-Party Doctrine as it has evolved under the Fourth Amendment.[1] This

---

† James Parker Hall Distinguished Service Professor of Law, The University of Chicago; the Peter and Kirstin Bedford Senior Fellow, The Hoover Institution; and visiting professor at New York University School of Law. My thanks to Paul Schwartz, for his valuable comments on an earlier draft of this Article, and Orin Kerr and Erin Murphy for their insightful presentations at the Berkeley Center for Law & Technology 2009 Privacy Lecture: Confronting the Third Party Doctrine and the Privacy of Personal Information at the Berkeley Center for Law & Technology (March 18, 2009). I should also like to thank Jean Bisnar, NYU School of Law, class of 2010 for her usual expert research assistance.

1. U.S. CONST. amend. IV. The Amendment protects

doctrine holds that an individual who passes information on to some third party cannot claim any Fourth Amendment protection when the government, with an eye to criminal prosecution, seeks to obtain that information from the third party. The received judicial wisdom is that any person who chooses to reveal information to a third person necessarily forfeits whatever protection the Fourth Amendment provides him. Orin Kerr's formulation captures the breadth of the rule: "By disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed."[2] As Kerr notes, the Supreme Court puts the rule in broad terms:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[3]

In other words, "a person cannot have a reasonable expectation of privacy in information disclosed to a third party."[4]

This conclusion has been widely attacked.[5] Professor Kerr's recent defense, which sought to bolster the rationales offered by the Supreme Court, has enlivened the debate. My job on this occasion is to review the debate as someone who comes to the problem from outside the field of criminal procedure, but with a strong commitment to the principles of limited government. In dealing with the vexing question of whether a person has a reasonable expectation of privacy in information disclosed to a third party, I do not think it is necessary to come down clearly on one side or the other. It is more important to parse the arguments in order to develop a

---

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Id.

2. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009). As stated, the term "information" is intended to cover both oral communication and the transfer of documents, of whatever kind or description. *See generally id.*

3. United States v. Miller, 425 U.S. 435, 443 (1976).

4. Kerr, *supra* note 2, at 563.

5. For a list of the references, *see* Kerr, *supra* note 2, at n.5.

unified approach to this question that can win adherents both within the field and beyond it.

In the current debate, Kerr is quite right to note that it is difficult to defend the current rule on the grounds that the subject of investigation has assumed the risk that the disclosed information will be used as evidence. Thus it surely begs the central point to insist, as the Court has, that "[b]ecause the depositor [in *Miller*] 'assumed the risk' of disclosure, . . . it would be unreasonable for him to expect his financial records to remain private."[6] Yet at the same time, it is tempting to do so, for Kerr's own revised justification for the rule turns on the notion of consent that is subject to parallel objections. He writes: "The Supreme Court should have accepted this consent-based formulation of the third-party doctrine . . . . So long as a person knows that they are disclosing information to a third party, their choice to do so is voluntary and the consent valid."[7]

Some support this rule by appealing to the common law distinction between fraud in factum and fraud in the inducement.[8] The former goes to the nature and quality of the act, and is thus said to vitiate consent, by denying its existence.[9] The latter takes the opposite tack and assumes that consent has occurred, and then sets it aside against the party who induces it. Since fraud in the inducement still allows for the rescission of the contract, this distinction is immaterial in any dispute between the two parties in ordinary contract law. The difference only manifests itself when third party rights are involved. A holder in due course of a negotiable instrument takes free and clear of the claims of the party who wrote the check if there is only fraud in inducement, but gets no title where there is a fraud in factum, because there is no right to transfer.[10] Under standard doctrine, the consent should not be binding against the party whose fraud induced the revelation.

---

6. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979).

7. Kerr, *supra* note 2, at 588-89 (discussing Hoffa v. United States, 385 U.S. 293 (1966)).

8. Kerr, *supra* note 2, at 588-89; ROLLIN M. PERKINS & RONALD N. BOYCE, CRIMINAL LAW 1079 (3d ed. 1982).

9. *See* MODEL PENAL CODE § 213.1(2)(c) (holding that a type of rape is committed if a male has sexual intercourse with a female when "he knows that she is unaware that a sexual act is being committed upon her . . ."). For more discussion on the role of consent with regards to rape, see PERKINS & BOYCE, *supra* note 8, at 1079-80.

10. *See, e.g.*, UNIF. COMMERCIAL CODE § 3-305(2)(c), cmt. 7 (noting that this section "follows the great majority of the decisions under the original Act [on negotiable instruments] in recognizing the defense of 'real' or 'essential' fraud, sometimes called fraud in the essence or fraud in the factum, as effective against a holder in due course.").

In Fourth Amendment cases, this party is the government, so we are back at square one.

Accordingly, in Part II of this Article, I shall examine the twin rationales of assumption of risk and reasonable expectations to assess the extent to which they can afford some basis of understanding the relevant doctrine. In so doing there are two key moves that drive the overall analysis. First, it is necessary to explain why and how the reasonable expectations test should work. It is commonly conceived of as a cross between the subjective and objective understandings of the relevant actors, usually persons who are the subject of a search. Second, I advance an alternative conception from my own work on rights to privacy in connection with the common law tort of invasion of privacy, which avoids the solipsism of identifying reasonable expectations with the position or desires of a single person.[11] Instead the central approach is to use the language of reasonable expectations as a way to forge a sensible set of rules that optimizes social welfare with respect to a given kind of problem. In essence the task is finding that set of rules which, when laid down generally, produces the best mix of privacy and security that can be obtained in light of the limited available knowledge, taking into account that the Fourth Amendment protects not only the guilty, but also innocent persons who may have been swept into a search.

Part III of this Article examines how this abstract framework applies to the range of situations, dealing with both documents and words, which are traditionally governed by the third-party rule. In doing so, I address the different types of cases separately in order to make a more precise calibration of the relevant interests. There is no reason why the level of constitutional protection that is attached to documents placed in the hands of third persons for storage should necessarily attach, for example, to the use of secret agents who carry wires. The boundary lines between these various areas are for the most part relatively clear, so that the borderline interpretation issues should not muddy the overall inquiry. This allows us to preserve the ease of application that Kerr, for example, sees in the categorical, if overbroad, rule that holds that all third-party communications lie outside the scope of the Fourth Amendment.[12]

---

11. *See generally* Richard A. Epstein, *Deconstructing Privacy: And Putting It Back Together Again*, 17 SOC. PHILO. & POL'Y. 1 (2000); Richard A. Epstein, *Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism*, 52 STAN. L. REV. 1003 (2000).

12. *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976).

II. TRADITIONAL DOCTRINES

A. ASSUMPTION OF RISK AND CONSENT

One of the great temptations in political theory generally is to see if various claims of rights and duties can be predicated on some bedrock element of individual assumption of risk, or consent. This approach proves to be so durable and attractive because assumption of risk and consent offer the strongest ground on which to base obligations to others: the obligation is accepted by the party to be charged. One central idea in political theory is that autonomous individual agents of full capacity should be entitled to decide which risks to assume and which not.[13] That position lies at the root of contract law generally, where any individual decision to make a promise or to assume a risk is held binding on the party who made it. After all, if that form of contractual freedom is denied, then individuals will not be able to assume any risk in advance in order to secure greater benefits.

However, these autonomy-based principles do not always control. For instance, in the realm of trade, persons cannot part with their labor or their capital if they are deemed to lack the capacity to do so. Likewise, in the area of medical services, the inability to assume the risk because of incapacity leads to the creation of an "emergency" exception to the general rule of consent so that they can receive the services that they desperately need on the same terms and conditions to which ordinary persons would agree. To facilitate receipt of these services, the universal rule announced in *Schloendorff v. Society of New York Hospital* juxtaposes the autonomy rule with the ubiquitous emergency exception:

> Every human being of adult years and sound mind has a right to determine what shall be done with his own body; and a surgeon who performs an operation without his patient's consent commits an assault, for which he is liable in damages. This is true, except in cases of emergency where the patient is unconscious, and where it is necessary to operate before consent can be obtained.[14]

The clear negative implication is that the surgery can take place either with consent or when the conditions of necessity relax the rules of property and contract, as they generally do.

---

13. Schloendorff v. Soc'y of N.Y. Hosp., 105 N.E. 92, 93 (N.Y. 1914).
14. *Id.*

It is also critical to guard against the undue extension of the notion of voluntary consent. The first potential source of abuse is the false equation of knowledge of a risk with the assumption of the risk. Courts began to recognize this distinction in the Industrial Revolution in order to deal with workplace accidents prior to the adoption of the workmen's compensation laws. The cases consistently emphasized the difference between *volenti non fit iniuria* and *scienti non fit iniuria*.[15] The acceptance of a risk does not follow from knowledge of the risk. The difference here is not one of mere words, but of substance. Each day I walk down the street I know that some automobile may hurt me. Yet I do not assume the risk of which I am fully aware. There is no bargain between the random motorist who hits me and myself, and as a result, the entire dispute is resolved by the general principles of tort law that regulate the affairs of strangers.

The same kinds of arguments can apply with respect to workplace injuries. If a worker knows that a dangerous condition has been introduced into the plant, this knowledge will not bar recovery. The standard rule allows the worker time to issue a complaint and applies the assumption of risk doctrine only where the resulting interchange with the employer makes it clear that the complaint has been rejected, and that the worker can keep his position only if he agrees to waive the action in question.[16] The requirement of waiver is critical because it suggests that there is some quid pro quo in the relationship. Knowledge in the absence of consent precludes that possibility, because all the gain goes on one side and all the costs go on the other.

The abuses of the notice principle carry over to other areas as well. For instance, the concept of notice is overextended in cases dealing with the eminent domain power. Thus it is sometimes said that retroactive legislation is constitutional because settled expectations that private arrangements will continue do not condemn such legislation to irrationality,[17] or that some new zoning regulation limiting the right of future construction is valid solely

---

15. *See* SIR FREDERICK POLLOCK, THE LAW OF TORTS: A TREATISE ON THE PRINCIPLES OF OBLIGATIONS ARISING FROM CIVIL WRONGS IN THE COMMON LAW: TO WHICH IS ADDED THE DRAFT OF A CODE OF CIVIL WRONGS PREPARED FOR THE GOVERNMENT OF INDIA 153 (Stevens & Sons 2d ed. 1895).

16. *See, e.g.*, Lamson v. Am. Axe & Tool Co., 58 N.E. 585, 585 (Mass. 1900).

17. *See, e.g.*, Usery v. Turner Elkorn Mining Co., 428 U.S. 1, 15-17 (1976). In speaking of the black lung disease provisions of the Coal Mine Health and Safety Act of 1969, 30 U.S.C. § 932, Justice Marshall wrote: "And it may be that the liability imposed by the Act for disabilities suffered by former employees was not anticipated at the time of actual employment. But our cases are clear that legislation readjusting rights and burdens is not unlawful solely because it upsets otherwise settled expectations." *Id.* at 16.

because of the advance notice given by the state. The difficulty here is that the notice argument is so powerful that it leaves nothing to the underlying substantive right at all. The government need only decide to give notice in order to restrict rights of other individuals, and give standing notice to restrict them altogether.[18] However, free options of condemnation that invalidate use rights are utterly inconsistent with a notion of limited government that protects any individual rights in property. Perhaps people ought to be required to mitigate their losses in the face of government notice, but if so, they should recover the costs of mitigation plus the residual loss, which may be smaller than the losses that would be realized if no protective action were taken at all.

These arguments work not only with respect to takings and the Fifth Amendment, but also apply equally well to the analogous searches and seizures under the Fourth Amendment. Thus suppose the government gave notice to the world that it would engage in surveillance of all private activities at will; so draw your curtains, but the government can still peek through. People would have to alter their conduct in order not to assume the risk. No one would accept such unilateral legislative declaration as sufficient to undermine constitutional rights that are intended to limit the scope of permissible government action. Nor can the government eliminate this abuse by offering certain types of quid pro quos in order to obtain the needed consents. The entire doctrine of unconstitutional conditions rests on the implicit assumption that there is something deeply wrong with a state declaration that allows the state to issue licenses for use of the public highway on condition that an individual waive his Fourth Amendment protections against unreasonable searches and seizures.[19]

Monopoly power cannot be used to extract rights from all citizens. Rather it should be understood that the government operates much like a common carrier that carries with it the same duty to guarantee access as private carriers holding the same position. Rules of the road that improve the ex ante utility of all persons who use the system are allowable, but extractions that increase state power without an allocative improvement are not. Assumption of risk has no traction in those situations at all.

---

18. *See, e.g.*, Connolly v. Pension Benefit Guar. Corp., 475 U.S. 211, 227 (1986). "Those who do business in the regulated field cannot object if the legislative scheme is buttressed by subsequent amendments to achieve the legislative end." *Id.* (quoting FHA v. The Darlington, Inc., 358 U.S. 84, 91 (1958)).

19. For discussion of these points, see RICHARD A. EPSTEIN, BARGAINING WITH THE STATE 161-75 (1993).

The same argument runs through many Fourth Amendment cases. The government's stated position is that anytime one individual talks to another, he necessarily assumes the risk that any person with whom he talks will speak to the government.[20] The principle has no autonomy-based roots, because the law provides no way for an ordinary person to contract out of the rule. Thus giving the information in confidence with an explicit promise from its recipient that he will not turn it over to the state, or that he will not use a wire that allows a government agent to record the conversation, does not give the target of a criminal investigation an action in damages if the information is released to the government. Nor could that person ever obtain an injunction against turning the information over. The supposed assumption of the risk is forced on individuals by positive law. It is not consensually assumed.

Whatever one thinks of Kerr's conclusions, his analytical approach is wrong for its excessive reliance on consent. It is improper to claim that "[a]lthough the third-party doctrine has been framed in terms of the reasonable expectation privacy test, it is better understood as a consent doctrine."[21] The entire area of the Fourth Amendment cannot be rendered coherent unless its consensual base is modified. To be sure, there are many cases where the consent of the party searched meets the standard of individualized consent developed in private law settings. But in other cases the nominal consent is presumed on the ground that on balance people are better off from the ex ante perspective if they are forced to submit to some searches against their will. Insofar as Kerr shifts away from reasonable expectations to either assumption of risk or to consent, he cannot build an adequate foundation for Fourth Amendment Law. We have to look elsewhere to get a better grasp of the reasonable expectations test that he rejects.

B. REASONABLE EXPECTATIONS

Generally we do look elsewhere when we shift the analysis from assumption of risk to reasonable expectations of privacy in an effort to move the inquiry away from autonomy-based regimes. But to what end and why? One common line of thought treats this approach as an intellectual dead end

---

20. *See, e.g.*, Lewis v. United States, 385 U.S. 206, 208-10 (1966); Hoffa v. United States, 385 U.S. 293, 301-02 (1966); Lopez v. United States, 373 U.S. 427, 438 (1963); Lee v. United States, 343 U.S. 747, 752 (1952).

21. Kerr, *supra* note 2, at 565.

on the ground that the entire exercise turns out to be perfectly circular.[22] Once one knows what the law requires, it is possible for individuals to develop reasonable expectations as to how they should behave. The conclusion seems to follow that divining the reasonable expectations needed to frame the legal rule requires knowledge of the legal rule in advance. But the reasonable expectations that flow from knowledge of the law cannot explain how that law should be configured in the first place.

One can observe this point in many substantive contexts. In dealing with product liability law, for example, one question is what expectations a manufacturer should have about how the product user will behave. This involves the aptly named "consumer expectations" test.[23] If the law allows the user to recover only if he makes normal and proper use of the product in accordance with its design specification and instructions, the reasonable expectation is that the product user will in fact comply with the applicable norms for the use of the product, whether they be learned from reading instruction manuals or following the standard practices of the trade. Similarly, Justice Scalia invokes some undifferentiated sense of this term when dealing with land in *Lucas v. South Carolina Coastal Commission* to ask what limitations on the use of land rise to the level of compensable takings:

> The answer to this difficult question may lie in how the owner's reasonable expectations have been shaped by the State's law of property—i.e., whether and to what degree the State's law has accorded legal recognition and protection to the particular interest in land with respect to which the takings claimant alleges a diminution in (or elimination of) value.[24]

Yet this formulation does not escape circularity because it does not explain how the state law of land should define property in the first place. The point matters because the definition of property rights rests heavily on state law: "Property interests, of course, are not created by the Constitution. Rather, they are created and their dimensions are defined by existing rules or understandings that stem from an independent source such as state

---

22. For my critique, see generally Richard A. Epstein, *Lucas v. South Carolina Coastal Council: A Tangled Web of Expectations*, 45 STAN. L. REV. 1369 (1993).

23. RESTATEMENT (SECOND) OF TORTS § 402A cmt. i (1965) (providing a judicial discussion of the test); Barker v. Lull Eng'g Co., 573 P.2d 443, 454-56 (Cal. 1978) (unraveling the test).

24. 505 U.S. 1003, 1016 n.7 (1992); *see* Epstein, *supra* note 22 (offering a critique of this case).

law . . . ."[25] Justice Scalia expresses a similar sentiment with relation to regulations that prevent all use of land: "Any limitation so severe cannot be newly legislated or decreed (without compensation), but must inhere in the title itself, in the restrictions that background principles of the State's law of property and nuisance already place upon land ownership."[26] Once again, the question is whether these remarks are idle statements that simply push the inquiry back one level, without explaining why the state law evolved in the manner it did.

An odd thing about these common criticisms is that they have not limited the use of the phrase "reasonable expectations" in any of the contexts in which it arises. In light of this fact, the mere persistence of the term should suggest that it has more content than the circularity provision of the law suggests. And I believe that this is the case.

Return for the moment to our product liability case. There, the economic business problem faced in the sale and manufacture of new products is a coordination problem. The correct approach is to specify those obligations that fall on each party that, if discharged, will maximize the value of the goods sold, i.e. the sum of consumer and producer surplus. Here the tradeoff runs as follows: if the rule chosen is one that allows the user to deviate from proper use without forfeiting the right of recovery, then the manufacturer is put into the position of having to design a product sufficiently able to prevent these deviations from resulting in harm. That enterprise, however, is far from costless, because once the product design features and warnings are incorporated to cope with the deviant user, the product becomes less valuable to the user who is able to follow instructions to a T. In dealing with ordinary consumer products, the users are a diversified class with uneven abilities, so that some tolerance or margin of safety has to be built into the system to prevent innocent mishaps from having dangerous consequences. Users want an extra margin of safety for consumer products like toasters and cars. But by the same token, it does not make sense to force the manufacturer to guard against reckless disregard by consumers or users if this will impair the value of a product for those who can keep their conduct out of the zone of danger. There is surely willful misconduct if someone uses a buzz saw to cut off a mole, just as there is in workers' compensation cases. But a saw that is intended for softer wood should be durable enough to deal

25. Bd. of Regents of State Coll. v. Roth, 408 U.S. 564, 577 (1972).

26. *Lucas*, 505 U.S. at 1029. Scalia does not further clarify the meaning of the phrase "inhere in the title."

with harder wood as well. Just which excesses should be guarded against is a tricky problem. The one point of confusion is that an unexamined notion of "foreseeability" is a familiar crutch that unfortunately will not provide the answer. The term only defines the scope of the problem. It does not indicate who should bear which of the foreseeable risks, of which there are many.[27]

However, consumers strike a different balance of convenience when dealing with goods that are supposed to be used by highly trained specialists. The fact patterns behind two controversial recent decisions give rise to consternation. In *Riegel v. Medtronic, Inc.*, the question was whether a tort action should be allowed against the manufacturer of a balloon angioplasty device that was overinflated by a physician and used on a patient who was not a suitable candidate for the procedure.[28] In this case, following the lenient rule for ordinary consumers makes no sense, given the exacting standards for training specialists. To maximize flexibility upstream, downstream professional users should be strictly required to follow rules to a T. Wholly without regard to any issue of federal preemption, the situation is one in which courts should not find tort liability against the device manufacturer, lest the value of the device be reduced.

The same approach should have controlled in *Wyeth v. Levine,* where the defendant drug manufacturer was held responsible for the maladministration of the drug Phenergen by a physician's assistant in the face of clear warnings about the risk of the procedure.[29] Neither the Vermont court nor the Supreme Court discussed the implicit causal premise of the case, which was that tort rules of joint causation allowed a plaintiff to recover from the original drug manufacturer. That rule is not consistent with the proper understanding of reasonable expectations, which allows each party to act on the assumption that the other party knows what it is doing, unless it has actual knowledge of the prior error. That constraint would surely bind a physician that administered a drug known to be defective. Similarly, it would also apply to a manufacturer who sold the drug through outside channels to an improper user. The net effect of this ruling in *Wyeth v. Levine* is to impose

---

27. *See* Richard A. Epstein, *Beyond Foreseeability: Consequential Damages in the Law of Contract*, 18 J. LEGAL STUD. 105 (1989) (discussing who should bear the foreseeable risk in the allocation of contract losses).

28. 128 S. Ct. 999, 1005 (2008).

29. 129 S. Ct. 1187 (2009), *aff'g* 944 A.2d 179 (Vt. 2006). The Supreme Court decision noted the risks of inadvertent error, but did not allude to the admitted negligence of the physician's assistant. 129 S. Ct. at 1192. *See* Brief for the Petitioner at 20, *Wyeth*, 129 S. Ct. 1187 (2009) (No. 06-1249).

on manufacturers inordinate pressures to take defensive steps that reduce the availability of drugs that may be desperately needed. The normal and proper use standard—the very standard that was originally announced in *Escola v. Coca-Cola*,[30] only to be forgotten—should have been applied in this case.[31]

The same logic applies to the use of reasonable expectations in the takings area. One common "realist" line is that the standard bundle of rights over a particular object—the rights of possession, use, and disposition—should not be considered unassailable, but rather should be treated as though they were an arbitrary assemblage. But that point misses the reason for the durability of this conception; linking the three incidents of the land together minimizes the transaction costs of getting the asset to its highest value use. Why incur the costs of dealing with holdout issues if the right of possession is lodged in one person, the right of use in another, and the right of disposition in a third? The unity of rights permits a single person to enter into transactions that can create divided interests—lease or mortgage—which will increase the value of the asset without hampering any third party rights. The law goes astray when it takes the position that the loss of the rights to dispose of property should be treated in the same, non-compensable way, as the losses that arise from lawful competition.[32] Competition is a positive sum game; land use restrictions reduce value without producing offsetting gains. The idea of reasonable expectations is useful in understanding the traditional configuration of property rights because it maximizes the value of the relevant interests, and thus avoids the charge of circularity that normally dogs this field.

III. REASONABLE EXPECTATIONS AND THE FOURTH AMENDMENT

There is then good reason to think that the idea of reasonable expectations could have promise in the Fourth Amendment area. Concerned with "*unreasonable* searches and seizures," the Fourth Amendment veritably invites use of a reasonable expectations test.[33]

---

30. 150 P.2d 436, 444 (Cal. 1944) ("The manufacturer's liability should of course be defined in terms of the safety of the product in normal and proper use.") (Traynor, J., concurring).

31. *Id.* at 440-44.

32. For the devastatingly incorrect articulation of this supposed equivalence, see the decision of Brennan, J. in Penn Cent. Transp. Co. v. City of New York, 438 U.S. 104, 136 (1978).

33. *See, e.g.*, Katz v. United States, 389 U.S. 347, 361 (1967).

The matter is of course massively complicated because of the imperfect integration of the basic prohibition against unreasonable searches and seizures with the warrant clause and its own heightened standard of probable cause. The "and" that links the two clauses represents the most unfortunate use of conjunctions. Making the matter more difficult, the collection of information received by the third party rule extends beyond the "persons, houses, papers and effects"[34] that are covered by the Fourth Amendment's initial guarantee against unreasonable searches and seizures. There are two questions left open by the first clause of the Fourth Amendment. First, to what extent does the Fourth Amendment limit the conduct of police officers (to whom it is not explicitly limited) in public spaces where none of the enumerated elements is obviously implicated, as in cases of routine surveillance? Second, is it possible, under the opening clause, to escape the dilemma between unregulated government conduct and the strict probable cause standard used for breaking into closed spaces that are manifestly covered by the Amendment?

The conceptual problem asks how to address these two difficulties without obliterating the libertarian baseline derived from assumption of risk and consent. This libertarian baseline, when faithful to the private law notions, cannot be the last word because it in effect makes all forms of criminal investigation illegal without the consent of the parties who are investigated. But from John Henry Wigmore forward, virtually everyone has recognized that any sound social system requires the incremental increase of state power even before any conviction is obtained. After all, the standard for getting a warrant is "probable cause" while that for getting a conviction is "beyond a reasonable doubt." The basic pattern is that in principle, it should take more to convict than it does to arrest, and more to arrest than it does to search, and more to search than it does to investigate. Only if we take this progression seriously can we escape the hard all-or-nothing choices in this area: either probable cause or nothing.

In the end, the only way to formulate a sensible set of constitutional procedures is to be systematic about the introduction of the "reasonable suspicion" standard of *Terry v. Ohio*, which applies to police stops of suspects on the street.[35] What follows is an elaboration of that position, starting with the treatment of privacy in the private law of contract, trade secrets, and tort.

---

34. U.S. CONST. amend. IV.
35. 392 U.S. 1, 30-31 (1968).

A. THE PRIVATE ANALOGIES

My earlier writings on the tort of invasion of property and privacy have real application in the Fourth Amendment setting by offering one way to escape from the libertarian dead end.[36]

The key analytical insight starts from the assumption that it is never possible for the government to obtain universal consent to introduce a system of criminal investigation. Yet at the same time, it is clear from the ex ante perspective that some greater use of state power puts all people in a better position (even net of costs), because any system that is forced to rely exclusively on decentralized means of private enforcement must ultimately break down.[37] A rule that is accepted behind the veil of ignorance that allows the state to search for murder weapons with a warrant will contribute more to the security of all individuals than it will harm their loss of liberty.[38] Asking people to display licenses on the back of their cars is a trickier case because in some instances that information can be used for bad purposes as well as good ones. But on average the practice sticks because it offers the police more scope to enforce the law than private wrongdoers to violate it; otherwise, with systematic public abuse, the requirement would have faded a long time ago. Therefore, actions of case-by-case compensation are unnecessary because in the fashion of the Lockean social contract, the gains to each actor from the security of the system will outweigh their private costs. The implicit-in-kind compensation moves folks to a higher level of welfare than they could achieve by working solely through voluntary agreements.[39]

Just this logic helps explain the emergence of the modern tort of invasion of privacy. It undergirds the *Katz* rule that bars the overhearing of telephone calls without a warrant by relying heavily on reasonable expectations.[40] The early history of the law of privacy sought to tie the protection of privacy to

---

36. For a somewhat different attack on the same issue, see Richard A. Epstein, *A Common Lawyer Looks at Constitutional Interpretation*, 72 B.U. L. REV. 699 (1992). That article notes that the interpretive strategies used in constitutional law track point for point those that the Romans used in the explication of their central tort statute, the Lex Aquilia. *Id.*

37. As recognized as early as JOHN LOCKE, A SECOND TREATISE OF GOVERNMENT (1690).

38. *See* RICHARD A. EPSTEIN, BARGAINING WITH THE STATE 63-69 (1993) (discussing the implicit prisoner's dilemma game).

39. *See* Richard A. Epstein, *Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism*, *supra* note 11, at 1012-13 (discussing how this principle works in privacy contexts).

40. *See* Katz v. United States, 389 U.S. 347, 358-59 (1967).

the common law tort of trespass that hinged on a physical entry onto the property of another.[41] If one walked onto the land of another individual to observe their private (even intimate) behavior, the trespass lay in the entry for which the consequential damages resulted from that entry. Thus early cases accepted the rule that there was no recovery for simple mental distress that was unaccompanied by a physical invasion.[42] But those damages for mental distress did become actionable if "they [arose] out of a trespass upon the plaintiff's person or possession."[43] From there it was a small step to make the action turn on the improper collection of information consequent on the trespass,[44] including its subsequent public dissemination.[45] It may be puzzling that the physical invasion is of no importance in that the real complaint was directed to the parasitic losses derived from the collection and dissemination of the information.[46] Physical intrusion and private information shared an uneasy harness.

The tension between the two became acute when the same information was collected by a camera with a zoom lens that was used by an individual

---

41. *See* Daugherty v. Stepp, 18 N.C. 371 (1835) ("[E]very unauthorized [sic], and therefore unlawful entry, into the close of another, is a trespass.").

42. *See, e.g.*, Mitchell v. Rochester Ry., 45 N.E. 354 (N.Y. 1896) (holding no recovery for mental distress for a pregnant woman who was nearly run over by a team of horses). That decision is widely rejected today for mental distress for persons who are in the zone of danger. *See, e.g.*, Dillon v. Legg, 441 P.2d 912 (Cal. 1968).

43. Bouillon v. Laclede Gaslight Co., 129 S.W. 401 (Mo. Ct. App. 1910) (holding defendant's agent, a meter reader, liable for causing plaintiff to have a miscarriage from fright and mental anguish after wrongfully entering plaintiff's apartment).

44. For an early English case that deals with the interaction of trespass and information, see Hickman v. Maisey, (1900) 1 Q.B. 752, 756, where the defendant walked back and forth along a public highway in order to observe how the plaintiff's racehorses performed on his private land. The technical English doctrine treated the highway as though it were owned to the median strip by each of its abutting owners, so that members of the public enjoyed an easement of safe passage, which did not include within its scope the right to spy on the plaintiff's activities with an eye toward acquiring information of commercial value. *Id.* The English court found that the defendant's actions were an actionable trespass. *Id.* But however right the decision was in the individual case, it was insufficient as a matter of principle. *Id.* The same harms arise if the defendant stood a few feet further away from the plaintiff's land, or if he owned the land on the other side of the highway from which he made the same observations. *Id.*

45. Dietemann v. Time, Inc., 449 F.2d 245 (9th Cir. 1971) (upholding liability for publication of pictures obtained by fraudulent entry).

46. THOMAS ATKINS STREET, THE FOUNDATIONS OF LEGAL LIABILITY; A PRESENTATION OF THE THEORY AND DEVELOPMENT OF THE COMMON LAW 466 (1906) (introducing the phrase "parasitic damages" and defining it as "[a] factor which is today recognized as parasitic will, forsooth, tomorrow be recognized as an independent basis of liability").

who did not commit any common law trespass. The same interests were invaded, but they could no longer be treated as parasitic on some traditional tort.[47] They had to stand or fall in their own right. But how? It is relatively easy for people not to snoop with cameras or parabolic microphones in an effort to gather information. Yet it is devilishly difficult to guard against their use. We already know from the cases of physical invasion that a consensus emerged that the loss of privacy should be protected, given the subjective harms that snooping causes to others.[48] Yet there are crosscurrents here, for at the same time that the expanded law of privacy covers these cases, an expanded newsworthiness privilege under the First Amendment tends to eviscerate it.[49] This privilege covers the collection of information by trespass, and necessarily it also covers collection without resorting to trespass.[50] If the original collection is allowed, so too is its subsequent publication by a third person with knowledge that the information has been illegally acquired.[51] It is clear therefore that the calculations do not change just because the information intrusion is separated from the physical entry. To be sure, the First Amendment newsworthiness privilege too often restricts the scope of the privacy interest. But when that issue is put to one side, as it is in most

---

47. *See, e.g.*, Howell v. New York Post Co., Inc., 612 N.E.2d 699 (N.Y. 1993). In that situation the defendant trespassed on plaintiff's land to take a picture of another resident at the facility, Hedda Nussbaum, who had received massive publicity as the "adoptive" mother of Lisa Steinberg who had died of prolonged child abuse. *Id.* The plaintiff's picture was published over the desperate pleas of the operation of the facility that said it would wreak huge damage on the plaintiff and her family, but the court rejected claims for both intentional infliction of emotional distress and invasion of privacy. *Id.*

The result is wrong because of the exaggerated role that it gives to the newsworthiness privilege under the First Amendment. But for the purposes here, the key point is simply this: if *Howell* had come out the other way in the trespass scenario, the action would have been allowed if the defendant's photographer had used a more powerful telephoto lens from either a public highway or someone else's property. Note too that since the plaintiff could have surely enjoined the entry, it makes no sense to deny him the damage action when the entry has taken place. *But see, e.g.*, Pearson v. Dodd, 410 F.2d 701 (D.C. Cir. 1969).

48. *See* Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193-94 (1890) (tracing the origins of the right to privacy in the common law torts of trespass, assault and nuisance).

49. Virgel v. Time Inc., 527 F.2d 1122, 1128-29 (9th Cir. 1975) (discussing broad newsworthiness in the Restatement (Second) of Torts, § 652D of constitutional stature).

50. *See, e.g.*, De May v. Roberts, 9 N.W. 146 (Mich. 1881) (allowing action against a man who posed as a physician's assistant to gain access to a private home in which the plaintiff had given birth. The fraud vitiated the consent to the entry).

51. *Pearson*, 410 F.2d at 705-06 (holding newspaper publication of information by theft of plaintiff's papers is protected).

Fourth Amendment cases, all the pieces are in line for a general rule that requires all persons to refrain from snooping by these devices in exchange for the like surrender of the right to snoop by other parties.[52] This conclusion produces across the board gains from the ex ante perspective.

It is also capable of generalization. Consider the social conventions that define reasonable expectations in restaurants. Often these facilities are crowded and people can hear what is said at other tables. Yet it is not good form to lean off and cock one's ear in order to hear everything that other people are saying. It is not that people do not violate this norm. Instead, the implicit rule of proper social conduct does not depend on explicit consent and is regarded as authoritative. It may not be wise to hold top-secret merger negotiations at a public location, but it hardly follows that the rule should be abandoned because some people might do so. At the edges, the social norm improves the overall situation, and so it establishes a powerful custom that is observable and justifiable. We do not have to treat the phrase "reasonable expectations," as an open sesame that opens any and all doors.

The next question that arises is how this term gets carried over to the criminal context. The first observation starts from a modest premise that ultimately proves to be unsustainable: it does not matter who is doing the eavesdropping at the house or the restaurant. The same restrictions apply to government agents as to ordinary individuals. And just what do these restrictions entail? You cannot spy on people with a hidden camera or microphone. However, you can observe who is in attendance, when they arrived, and what their demeanor was. While people may draw curtains and claim privacy in their home, they necessarily forfeit some of that privacy in the social commons for a simple reason: the cost of compliance would be far higher if people have to avert their gaze from whoever is present. Stalking is out, watching is in.[53]

This first approximation therefore gives us some information of the kind of activities that the police can engage in without the benefit of any special grant of state power (i.e. without a warrant). The police can do what any other individuals can do. Once these ground rules are established, all are bound by them, just as all are bound by traffic rules. Notice of a social convention that works for mutual convenience carries over to the police or

52. *See, e.g.*, Roach v. Harper, 105 S.E.2d 564 (W. Va. 1958).
53. *See e.g.*, Nader v. Gen. Motors Corp., 255 N.E.2d 765 (N.Y. 1970).

their agents, and to private individuals who collect information that they then turn over to the public.[54]

Thus in *Terry v. Ohio*, the Supreme Court was correct to indicate that the police were allowed to follow around suspects on public streets to see if they were casing certain locations for holdups.[55] Once the police found that there were good reasons to believe that the suspects were casing locations, the police could stop and search these persons without a warrant so long as they had reasonable suspicion of wrong doing.[56] The use of greater power was only justified after the original surveillance furnished additional indicia of wrongful intention that allowed the police to stop a crime before it happened. To get the desirable social result, the "reasonable suspicion" standard operated as a sensible middle ground between a rule that allowed the police to stop and frisk at will and one that required them to demonstrate probable cause for arrest.

B. PEN REGISTERS

The protected zone of behavior makes a difference in certain types of cases, most notably those involving the use of a pen register. A pen register is a device installed at the central switchboard that tracks the phone calls made from certain phones. In *Smith v. Maryland*, the telephone company, at the request of the police, installed a pen register at the home of the defendant who was under suspicion of committing robbery and harassment.[57] The Supreme Court decided that the use of the pen register did not count as a search by resorting to its extravagant view of the standard assumption of risk doctrine.[58] Kerr summarizes the situation by arguing that the petitioner voluntarily conveyed numerical information to the telephone company and thereby exposed such information to the telephone company's equipment in the ordinary course of business.[59] Doing so implied the assumption of risk that the company might reveal to the police the dialed numbers.[60] Kerr continued that: "The switching equipment that processed those numbers [was] merely the modern counterpart of the operator who, in an earlier day,

---

54. Gouled v. United States, 255 U.S. 298, 306 (1921) (holding there is a Fourth Amendment protection for information gathered through private snooping and later turned over to the United States).

55. *See* 392 U.S. 1, 30 (1968).

56. *Id.*

57. 442 U.S. 735, 736 (1979).

58. *Id.* at 749.

59. Kerr, *supra* note 2, at 570.

60. *Smith*, 442 U.S. at 744.

personally completed calls for the subscriber."[61] The Court held that the third-party doctrine applied even though "the telephone company ha[d] decided to automate."[62]

The same result is achievable without resorting to the assumption of risk doctrine. The key point here is that the telephone company monitored only the connections.[63] It did not actually examine the content of the phone messages, which would have been a form of snooping. In one sense this case is an extension beyond the usual surveillance case because not every individual is in a position to monitor phone calls, while anyone can follow someone down the public street. But the information that can be gained by tracking connections in pen registers can prove of great benefit without revealing the content of the message. The pen register accommodation consequently counts as a clear line in a workable place. The decision to write down the information only improves its reliability after the fact. It does not increase the nature of the intrusion, but only serves as a protection for innocent persons that might otherwise be drawn into the web of surveillance, by reducing the risk of mistaken identification. It is both possible and desirable to defend the result without allowing the police the option to snoop on the calls themselves.

This point has urgent bite in the age of telecommunications. Much of the intelligence activity of the government involves a modern update of watching the connections that are made between various phone lines. There may be some questions of presidential power, that is, whether the Foreign Intelligence Surveillance Act authorizes the president to undertake those actions unilaterally in his role as commander-in-chief, which I do not believe to be the case.[64] But it does not implicate concerns with the Fourth Amendment, even if it were otherwise to apply, say, in the case of full Congressional authorization. The reasonable expectations test, carried over from the privacy setting, works in both directions. *Smith v. Maryland* is not like *Katz*, which it expressly distinguished, since the government in *Katz* had in fact overheard the *contents* of the phone calls. This qualifies *Katz* as a pure snooping case without the trespass.[65] On the strength of the approach taken

---

61. *Id.*

62. *Id.* at 745.

63. *Id.* at 741.

64. *See generally* Richard A. Epstein, *Executive Power, the Commander in Chief, and the Militia Clause*, 34 HOFSTRA L. REV. 317 (2005).

65. *See* Katz v. United States, 389 U.S. 347, 351-59 (1967); *see also Smith*, 442 U.S. at 739.

here, the difference is clear. *Katz* would count as an invasion of privacy if done by a private person. Its tortious nature therefore is what renders the conduct unjustifiable from, as the case put it, "an objective" point of view.[66] The proposition that Katz was entitled to rely on the privacy of the phone booth stems from precisely those calculations that brand private snooping wrong, as the balance of convenience shifts given the reasonable expectation of privacy.[67] So long as private parties are not in a position to snoop, the government needs a warrant. The restrictions of the common law of trespass are no greater obstacle in dealing with constitutional searches than with private actions for the invasion of privacy.

C. FOURTH AMENDMENT PROTECTION FOR ORAL EVIDENCE

As noted earlier, the Fourth Amendment has been held applicable to some oral communications, and it is useful to sort out the various scenarios. These cover information that is revealed in ordinary conversation, information that is obtained by eavesdropping on private conversation, and information collected in public places.

The first scenario involves persons who reveal information to others during the ordinary course of conversation, sometimes in confidence and sometimes not. This issue was set up by the Supreme Court's decision in *Silverman v. United States*,[68] which extended the reach of the Fourth Amendment to any government recording of oral statements that was accomplished without committing a trespass at common law. The actual listening to the remarks is like the eavesdropping that was condemned in Blackstone.[69] The use of the device to make the information more reliable does not, of course, remove the original taint on the source of the collection.

---

66. *Katz*, 389 U.S. at 353, 358.

67. *See id.* at 361 ("The critical fact in this case is that '(o)ne who occupies it, (a telephone booth) shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume' that his conversation is not being intercepted.") (Harlan, J., concurring).

68. 365 U.S. 505 (1961).

69. The Supreme Court remarked,

> Eaves-droppers, or such as listen under walls or windows, or the eaves of a house to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance and presentable at the court-leet: or are indictable as the sessions, and punishable by a fine and finding securities for good behavior.

Berger v. New York, 388 US 41, 45 (1967) (citing 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 169 (1769)).

The decision does not stand in real tension with the text of the Fourth Amendment, as the right of "the people to be secure in their . . . houses" is broad enough to protect the activities undertaken there, as well as the house itself.[70] In addition, the term "search" is broad enough to cover any intrusion into a particular area, even if there is no manipulation of the physical objects that are located there. The government searches an individual's open documents by reading their contents, even if it does not turn the pages (or lets the blowing wind do it). Similarly, a searchlight is used, well, for searching, even if it does not touch any object. Any intrusion into a protected space has a very different resonance than surveillance on the public streets where the reasonable expectations run in the opposite direction, on the strength of the private law analogies.

The situation becomes much more difficult when the information is collected in other circumstances where the usual understanding of privacy is attenuated. This is particularly true for conversations in public places. On this point, Kerr defends the rule that admits the evidence in order to force the criminal to substitute less efficient means of execution to achieve his illegal result.[71] Kerr's point here is that the threat of disclosure will reduce the frequency of crimes by making them more costly, so that most of the benefits will never be observed in handling cases brought within the criminal system.[72]

In making this argument, Kerr taps into a long criminal law tradition that deals with various restraints on cooperation through, for example, the law of conspiracy, complicity, and the like.[73] It is, however, vital to recognize that Kerr's argument is a two-edged sword. The usual approach to contract supports voluntary agreements for two reasons. First, they produce gains between the parties; second, they generate positive third party effects, by creating increased opportunities for trade. However, when the systematic externalities from contracting turn negative and exceed the gains to the contracting parties, it is important to stamp out the voluntary transaction.

---

70. U.S. CONST. amend. IV.

71. Kerr, *supra* note 2, at 564 ("Without the third-party doctrine, savvy wrongdoers could use third-party services in a tactical way to enshroud the entirety of their crimes in zones of Fourth Amendment protection.").

72. *Id.* at 564-65 (noting the weakening of general deterrence effect from abandoning the third party rule, owing in part to the greater clarity of the rule).

73. *See* MODEL PENAL CODE §§ 2.06, 5.02, 5.03. The intuition behind these sections is clear enough. Agreements produce gains between the parties, but when those come at the expense of the life, liberty, and property of third persons, they have to be blocked, because the gains from trade between the parties are negatively correlated with social welfare.

Cooperation thus becomes conspiracy to commit robbery or murder, or, closer to the line, conspiracy to fix prices. The larger the potential private gains, the larger the social losses, leading to the reversal in social response. The same argument holds true with the sale of goods. It is socially beneficial when the sale is of legal goods, and it is a form of trafficking when it is the sale of contraband or stolen goods.

This analysis presupposes that consumers can categorize the nature of each transaction, and thus can give a definitive answer to the sign of its externality. Unfortunately, when dealing with criminal processes, that sign is not as readily apparent because the substance of the underlying transaction is unknown. If people knew in advance that all these conversations were part and parcel of some illegal scheme, then why not admit whatever evidence the prosecutor can assemble? But if there is an invasion of privacy that turns up no evidence of illegal conduct, the social calculus is a lot closer. Coming up with the right answer is now hard because we cannot determine in the abstract whether the substitution away from a particular mode of doing business is a good or a bad thing. Kerr is right to insist that it is socially desirable to force the criminal to adopt less efficient means. But by the same token, the substitution effect will be socially undesirable for all innocent individuals who want to steer clear of the law. The full accounting has to include those social losses as well as the social gains. But how do we get the measure of the trade-off?

One approach to this problem begins by dividing the world into two kinds of cases: cases involving casually acquired information and cases involving government agents who are sent to spy. In cases of the first kind, the government is taking advantage of information that it casually acquires from some third party who has happened to have some interaction with the accused. The key point about these situations is that there is *no* prearrangement between the government and the third person whose testimony is sought. At this point, it is not possible to insist that the government make any kind of a showing before a neutral public official that it is appropriate to conduct this investigation through a third person. Either the evidence is admitted or it is excluded.

In general, I would admit virtually all evidence of this sort in a criminal trial, for the simple reason that, empirically, the scenario does not point to any abuse of government power that should be restricted from the ex ante perspective. It should not matter, as was held in *Miller*, that the disclosures to the third person were made in confidence. There are in all private law settings various levels of confidences and secrets. At one level we can declare privately that we think that something is conveyed in confidence or something is held in secret. But does the simple designation of something as

a trade secret make it so, or is there some additional requirement that has to be satisfied in order to obtain that preferred status? This is not an easy question because the standard definitions of trade secrets are stunningly evasive on this point. The early definition from 1939 limits the scope of trade secret protection to:

> [A]ny formula, pattern, device or compilation of information that is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers.[74]

This definition of trade secrets cabins the concept into discrete categories. In contrast, a 1995 definition extends the scope of trade secrets by eliminating the earlier enumeration: "A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others."[75]

Consider the case where a suspect's conversation with a stranger contains incriminating evidence. It is clear that this kind of talk does not fit within the first definition of a trade secret. Probably, but not certainly, it does not fall within the second definition either. At this point, it appears that by most accounts the recipient of that information could reveal it to third parties without suffering legal sanctions, even though that decision would generate a lot of social pushback. No one likes snitches or tattle-tales. Accordingly these cases lie in that gray zone where social obligations have not been promoted to legal ones. There is little doubt that this information would be admitted, if relevant, into a civil trial, at which point the reasonable expectations theory points toward its admissibility in criminal prosecutions. It is one thing to ask for protection against third party snoops. It is another to demand legal protection when you have the power to pick the person with whom you deal.

But what should be done if this information has been given to the third person in confidence? The Supreme Court's formulation of the rule in *Miller* regards this fact as irrelevant to the legal situation, and that conclusion has to be right as well, for otherwise the ability to use oral information from a

---

74. RESTATEMENT OF TORTS §757 cmt. b (1939).
75. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

subject is lost.[76] If information imparted in confidence to a random person is not available to the government, everyone with an illegal purpose will declare that he is supplying information in confidence. That defensive application of the autonomy position marks the end of all criminal investigations, for even if the condition were not stated, under orthodox contract it should be implied on the grounds that it works to the mutual benefit of both parties to the communication in situations where the government cannot credibly claim to be a third-party beneficiary.

In this situation, however, the reasonable expectation test, in contrast to *Katz*, does not expand the sphere of protected activities. Rather, it narrows it on the ground that no one (or no two people) can conceal evidence from criminal prosecution by their joint declaration alone. All this information is admissible in civil cases, and the same rule applies in criminal contexts. Put otherwise, the only confidences that matter are those that are externally validated by law: the lawyer-client relationship, work product and the like. These are regarded as exceptions to the well-established norm that the law is entitled to the evidence of every person, and it is hard to think of a criminal system that could survive a new-found ability of every person to bind the state by contracting out of the third party rules.

The second set of cases does not involve random third persons, but rather government agents who are sent to spy. At this point, the calculus is surely closer because the risk of government abuse is greater. The disclosure of valuable information is likely to have been induced by fraud, sometimes tacit, but often overt. On this issue the private law analogies cut both ways. The private law is filled with cases where a seller conceals a latent defect in the product sold,[77] or the buyer does not reveal to the seller that he is buying a particular plot of land in order to assemble a large factory.[78] The law usually requires the disclosure of the latent defect, but in general is wary of forcing the buyer to reveal his lands, lest the forced disclosure of that information blunt the buyer's willingness to form his plan in the first place.[79] In similar fashion, restaurant reviewers never reveal their identity in order to acquire an accurate assessment of the food and service.

---

76. United States v. Miller, 425 U.S. 435, 443 (1976).

77. RESTATEMENT (SECOND) OF TORTS § 551 (1965) (discussing the basic rule of nondisclosure and its long list of exceptions including that it applies to "facts basic to the transaction").

78. Guar. Safe Deposit & Trust Co. v. Liebold, 56 A. 951 (Pa. 1904).

79. Anthony Kronman, *Mistake, Disclosure, Information, and the Law of Contracts*, 7 J. LEGAL STUD. 1, 13-16 (1978).

As such, these fraud cases land right on the cusp in private law, and so too in criminal law. Entrapment by a secret government agent vitiates the consent, but the defense is generally narrowly construed, so that the agent must induce a crime that would not otherwise be committed. It is not sufficient to offer an opportunity that the suspect seizes on his own initiative.[80] Without that distinction, all undercover work is off-limits. The causal refinements are not elegant, but again, I am hard-pressed to see whether any other legal regime works better on the entrapment cases.

At other extreme, it hardly follows that the government can plant moles, with or without wires, on agents without any showing at all. In these situations there are few pressing emergencies, so it should be possible to have some neutral oversight of the process. Trying to run this case through the standard warrant requirements, however, is a hopeless task because there is no probable cause and no ability of "particularly describing the place to be searched, and the person or things to be seized." Those requirements make sense when the investigation of a particular offense has led to a particular place. But the secret agent is placed on spec, as it were, without any particular person, place or thing in mind. It is the information that is acquired that leads in the desired direction.

In contrast, however, there is no reason why the *Terry* reasonable suspicion standard could not be imported into this situation. To be sure, in *Terry* the reasonable suspicion standard was used to authorize a warrantless search for otherwise the suspect would be gone and so too the opportunity of apprehension prior to the commission of the harm.[81] But which way does that cut? Once there is the opportunity to survey the situation, the reasonable suspicion standard can be used to let a third person examine the evidence, ex parte of course, to see whether there are reasonable grounds to go further. The use of secret agents on an emergency basis could be allowed under reasoning analogous to *Terry*.[82] In the large number of cases, however, the same magistrates that issue warrants on probable cause could exercise oversight of this process, using a somewhat lower standard of proof, given the nature of the inchoate, but important, information to be sorted. Since this proposal builds off present institutional arrangements, it should be capable of orderly implementation. The modest restriction on police ability

---

80. *See, e.g.*, Jacobson v. United States, 503 U.S. 540, 548 (1992) (holding on facts that the government agents induced the commission of this crime).

81. Terry v. Ohio, 392 U.S. 1, 23 (1968).

82. *Id.* at 20-22.

to use secret agents should increase public confidence in the procedures, and offer a better balance in the chronic debate between liberty and security.

D. DOCUMENTS

The next question is what rule should apply to the government's ability to search or seize documents that are stored with third persons. As with oral testimony, the legal system faces the same double-edged sword problem on the substitution effect from the law. By transferring information or files to third persons, the criminal makes these documents available to search while making it harder for the criminal to execute his scheme. But by the same token, ordinary people, anxious to preserve their informational privacy, will be reluctant to put documents into the hands of third persons if they know the government can now sift through them it at will. In this situation, it is thus common that many documents are just transferred for safe-keeping, where the recipient is not supposed to look at their contents.

At this point, we are not faced with the common situation of oral testimony from random third persons. Rather, in this situation, the sensible approach parallels the approach used with secret agents. More specifically, the first concern in all document cases is to make sure that the documents are kept available to public authorities as needed in the course of a criminal prosecution. The proper way to achieve this result is to let the government obtain an ex parte order that these documents should not be returned to their owner or destroyed pending some judicial review of the matter. That stabilization order eliminates the risk of third party misconduct and buys time to see whether the requested disclosure to the government should be authorized.

The next stage in the proceedings goes to the question of whether the government can gain access to the contents of these materials. In dealing with this problem, it seems evident in many contexts that private decisions on where and how to store the information look far less dramatic in execution than those to share information with another person. Thus it seems odd in the extreme that the government could go through these records at will if they were stored on some Google cloud, but could only gain access to them on a showing of probable cause if they were located securely on that person's own hard drive, where they could easily be treated as a techno-version of "papers" that receive the full measure of Fourth Amendment protection. On this issue, moreover, the reasonable expectations test cuts firmly in favor of the ordinary individual who does not regard either a warehouse or an on-line storage facility as a trusted confederate or partner.

The hard question that remains is whether there exist situations where the government's ability to search should be governed by a reasonable

suspicion and not a probable cause standard. That point comes up because many investigations, especially in the context of national security, are not intended to solve crimes that were already committed, but to prevent the occurrence of crimes for which there is no judicial remedy. The difference between general surveillance and criminal investigations should not be lost in these cases, and the release of information to the government on the reasonable suspicion standard seems appropriate. At this point, the protection for ordinary individuals whose phone calls or billing information is collected does not lie in the inability of the government to access the information, but in the types of use the government can make of that information once access has been obtained. The easy case covers a flat prohibition against any political or other collateral use of the information. In my view, President George W. Bush was able to survive charges for impeachment because the information collected in his FISA-type searches was not used to advance those particular ends—in sharp contrast to the use of the Nixon Watergate tapes. It does, however, seem more doubtful that a rule could be devised in all cases that kept that information from use in criminal trials. Some such separation regime was contemplated by the original FISA statute,[83] but it might be quite difficult to apply in ordinary criminal contexts where the criminal safeguards come in the articulation of the substantive crimes and in the applicable standards of proof. At that point, however, the results are identical to those in *Terry*, which seems to have worked tolerably well over the past 40 years.

Like all trade-offs between liberty and security, the distinction between national security surveillance and criminal investigations has its inelegances. But, again, in light of the weighty objectives on both sides of the line, it may well be harder to develop a better regime. There is only so much that rules under the Fourth Amendment can do to deal with system-wide government mistakes. For certain types of serious police and investigative misconduct, other institutional arrangements, including police review boards, and, if need be, criminal prosecutions may be required. In other cases, the release of information by third parties, such as phone companies, should be accompanied by various protections that regulate, and probably insulate them

---

83. *See* The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. § 1806(b) (2006). Section 1806(b) states: "No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General." *Id.*

from civil liability from customers who claim that their cooperation with government officials facilitates an invasion of privacy.

IV. CONCLUSION

It is thus apparent that the Fourth Amendment cannot be the only tool that is used to deal with the manifold issues associated with third party searches. But even in the narrow Fourth Amendment context, these issues present challenges that are easy to state but hard to resolve. The simple solutions all fail because an autonomy-based system that deals with consent and assumption of risk misses the key point that public necessity could easily require an abandonment of those rules, just as it does in ordinary cases. At this point it is necessary to think about reasonable expectations as an optimization process that plays such an annoyingly persistent role in this analysis. It is a common characteristic that all optimization games share. It is easy to identify some clean cases where we are confident that the rule is correct. *Katz* looks like such a case. But the greater the refinements, the more likely it is that the next round of cases will come closer to the line, and so too with each successive iteration. In virtually all settings we shall eventually come close to the point of equipoise. That is why, for example, the art of implying a term that leads to business efficiency in the law of contract can take the analysis so far, but no further. And it is why the use of reasonable expectations leads to such close decisions for and against protection of privacy interests against various kinds of intrusion.

Those difficulties in the private law set up a warning system, for there is no magic approach that avoids these problems in public law settings. Public lawyers do not have available a novel set of tools that are unavailable in the simpler contexts of private law. If those tools lead quickly to honest differences of opinion in private law settings, then they will do so in public law settings as well.

In this connection, Orin Kerr has done us a great service in pointing out the substitution effects that come from a rule that exposes to government action documents and words that are entrusted to third persons. But by the same token his insight cuts in both directions, so that the inability to substitute creates social inefficiencies with respect to lawful conduct that people naturally wish to keep from the prying eye of the state. Thus, the problem of the third hand becomes a familiar problem of minimizing the sum of two kinds of error. At that point, we can be quite precise in identifying the relative conflicts, but very cautious in asserting dogmatic conclusions. It is for just that reason that relying on an expanded application of the *Terry* reasonable suspicion standard offers some help, particularly

because in many cases of proactive government action it suggests a set of public procedures that can contain, without destroying, various police and surveillance techniques. Yet at the end of the day, some profound disagreements will still persist. And for those we have to take comfort in the Humean injunction that for some problems "carelessness and inattention alone can afford us any remedy.[84]"

84. DAVID HUME, THE TREATISE OF HUMAN NATURE 218 (L.A. Selby-Bigge ed. & Peter Nidditch, rev., Oxford: Clarendon Press 1978).

DEFENDING THE THIRD-PARTY DOCTRINE: A RESPONSE TO EPSTEIN AND MURPHY

By Orin S. Kerr†

TABLE OF CONTENTS

In a recent article, *The Case for the Third-Party Doctrine*,[1] I challenged the consensus view among academic commentators that the third-party doctrine of Fourth Amendment law is a terrible mistake. I argued that the third-party doctrine serves two important functions. First, it furthers technology neutrality by correcting the substitution effects of third parties; second, it ensures the ex ante clarity of Fourth Amendment rules. I also argued that the primary criticisms of the doctrine are significantly weaker than critics have alleged. In particular, I noted that substitutes for Fourth Amendment protection already exist that address the concern that the doctrine provides too much power to the government. As I noted in my article, my aim was not to defend the third-party doctrine in every possible application. Rather, my goal was "to replace the partial view of the third-party doctrine found in existing scholarship with a richer and more balanced account of its costs and benefits."[2]

---

† Professor, George Washington University Law School. Thanks to Richard Epstein and Erin Murphy for their interesting and thought-provoking essays. Thanks to Paul Schwartz for convening the event that made them possible. And thanks to the editors of the BTLJ for allowing me to publish my response in the Journal.

1. Orin S. Kerr, *The Case for Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).
2. *Id.* at 566.

In contributions published in this issue, my friends Richard Epstein and Erin Murphy have offered us their own thoughts on the third-party doctrine.[3] Epstein brings the perspective of an outsider to Fourth Amendment law, and Murphy brings her perspective as an accomplished defense attorney. Each of their articles is at least in part a response to my article, and in this brief essay I am delighted to offer my thoughts in reply. On the whole, I find myself agreeing with much of Epstein's framework. Our differences are more a result of our different assumptions than of different analysis. On the other hand, I have a fundamental disagreement with Murphy's approach. Despite her welcome efforts to persuade me to change course, I find myself sticking to my position in the face of her critique.

I will start with a reaction to Richard Epstein's article, and then offer a few responses to Erin Murphy's.

I. A RESPONSE TO PROFESSOR EPSTEIN

Richard Epstein and I are not as far apart on the third-party doctrine as he may think. My sense is that we differ mostly on our assumptions. First, Epstein derives from first principles what I take from more traditional legal sources. Second, Epstein assumes that he is not bound by the all-or-nothing framework of existing law, by which government conduct either is not a search or is a search that requires probable cause and a warrant.[4] In contrast, my defense of the third-party doctrine takes this foundational aspect of Fourth Amendment law as a given.

A. HOW MUCH DO EPSTEIN'S FIRST PRINCIPLES ADD?

Epstein uses a remarkable range of different legal sources to derive from first principles a new methodology for the meaning of "reasonable expectations." Relying on insights from libertarian political theory, the common law of torts, and Fifth Amendment takings law, Epstein concludes that the question of "reasonable expectations" requires a cost-benefit analysis.[5] Specifically, the goal should be to "find[] that set of rules, which when laid down generally, produces the best mix of privacy and security that is obtainable in light of the limited knowledge that we have" and the fact that some suspects will be innocent and others guilty.[6]

---

3. Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199 (2009); Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239 (2009).

4. Epstein, *supra* note 3, at 1211.

5. *Id.* at 1202.

6. *Id.*

I wonder, though, what has this first-principles rethinking actually added? It seems to me that Epstein's formula largely replicates existing doctrine. Consider *Hudson v. Palmer*, a case that considered whether a prison inmate has a reasonable expectation of privacy in his prison cell.[7] The Court stated that the expectation of privacy analysis "necessarily entails a balancing of interests," in this case a balance between "the interest of society in the security of its penal institutions and the interest of the prisoner in privacy within his cell."[8] The Court's opinion balanced these two competing interests and concluded that the balance favored security: inmates do not have a reasonable expectation of privacy in their cell because "recognition of privacy rights for prisoners in their individual cells simply cannot be reconciled with the concept of incarceration and the needs and objectives of penal institutions."[9]

Hudson's analytical framework seems to match Epstein's theory without incorporating his first principles rethinking into the meaning of "reasonable expectations." To be sure, the Supreme Court has not always been clear about the normative framework triggered by the reasonable expectations framework; I have argued elsewhere that institutional limitations on lower court decision-making have made the consistent recognition of such a normative framework unworkable.[10] At the same time, it seems to me that the driving force behind the existing doctrine is the same normative inquiry that Epstein identifies.

I have a somewhat similar reaction to the second part of Epstein's Article, in which he applies his general approach to a few specific cases. As a policy matter, Epstein's approach does not seem particularly new. His balancing is the same basic type of ballpark balancing that occurs frequently in Fourth Amendment law and in the rest of the field of criminal procedure.

Consider Epstein's analysis of how much privacy should extend to remotely stored data on a computer network.[11] Epstein argues that a reasonable suspicion standard is appropriate here, but that the law might impose some use restrictions on the disclosure of information.[12] Epstein also argues that the law should allow the government to obtain an ex parte order requiring the third party not to destroy or return the remotely stored documents.[13] Congress is way ahead of Epstein here: Epstein's view of how to treat remotely stored files was enacted in a 1986 statute, the Stored Communications

---

7. 468 U.S. 517 (1984).
8. *Id.* at 527.
9. *Id.* at 526.
10. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection,* 60 STAN. L. REV. 503, 542-49 (2007).
11. Epstein, *supra* note 3.
12. *Id.* at 1224-25.
13. *Id.*

Act (SCA).[14] The SCA uses a mixed threshold for compelling content held by ISPs,[15] contains disclosure restrictions,[16] and includes the authority to issue a letter to the ISP to preserve the documents pending a court order.[17] This longstanding framework seems quite similar to what Epstein imagines.

B. ALL-OR-NOTHING VERSUS FLEXIBILITY

The greatest difference between Epstein and myself are our assumptions about the consequences of applying the third-party doctrine. My argument assumes the standard all-or-nothing options of Fourth Amendment law: if government conduct is a search, then it is a search that ordinarily requires a warrant based on probable cause to be constitutional.[18] Epstein eschews these options in favor of a more flexible Fourth Amendment.[19] In his view, courts should have the option of saying that a search is either a full probable cause search or merely a reasonable suspicion search.[20] As a result, he imagines a world in which the issue is not whether to apply the third-party doctrine, but rather what degree of privacy is optimal given the range of tools that can be imagined.

That assumption changes everything, as it means that Epstein ends up answering a very different set of questions. Consider the role of substitution effects. In my article, I argue that the Fourth Amendment corrects for the substitution effects of how individuals use third parties.[21] The use of the third party allows individuals to replace an outside transaction that is unprotected by the Fourth Amendment with an inside transaction that receives a full warrant protection. This argument largely depends on the all-or-nothing framework of existing law: If the choices are between no protection and full protection, a third-party doctrine that results in no protection is better than an alternative world in which crimes can be protected in their entirety by a full warrant requirement. By assuming away the all-or-nothing framework, Epstein dramatically changes the costs and benefits of the third-party doctrine.

Epstein's assumption also eliminates the institutional choice between constitutional regulation and either statutory or administrative regulation. My defense of the third-party doctrine takes as a baseline the inflexibility of Fourth Amendment law and the flexibility of its alternatives. In this environment, the third-party doctrine enables the flexible non-constitutional al-

14. 18 U.S.C. §§ 2701-11 (2006).
15. 18 U.S.C. § 2701(b).
16. 18 U.S.C. § 2702.
17. 18 U.S.C. § 2703(f).
18. *See* Katz v. United States, 389 U.S. 347, 354-56 (1967).
19. Epstein, *supra* note 3, at 1210.
20. *Id.* at 1211.
21. Kerr, *supra* note 1, at 573-81.

ternatives while avoiding the very high social costs of the inflexible protective option of Fourth Amendment law.[22] Epstein's response is to envision a flexible Fourth Amendment that eliminates the institutional choice: it presupposes no difference between what constitutional and non-constitutional rules might create. In my view, the institutional choice is too critical to make that step as lightly as Epstein does.[23]

II. A RESPONSE TO PROFESSOR MURPHY

Erin Murphy offers a spirited frontal assault on my article. She directly attacks my two central arguments in favor of the doctrine—first, that it counters substitution effects, and second, that it provides ex ante clarity.[24] I am delighted by the verve of Murphy's critique. At the same time, I do not find myself persuaded by her arguments.

A. DO THE SUBSTITUTION EFFECTS REALLY EXIST?

Murphy begins by questioning whether a substitute effect actually exists.[25] She doubts that the substitution effect occurs, or at least how important it is when it does.[26] Most criminals do not act rationally, she posits, and few are likely to make a conscious decision to use third parties to avoid detection.[27] Further, many crimes must be committed in person, and substitution effects will not appear if no third party is used. Even if there are some kinds of crimes that allow wrongdoers to use third parties to introduce substitution effects, she argues, they do not seem to be so important as to justify a rule designed to block those effects.[28]

I am not persuaded. First, Murphy mistakenly assumes that the role of substitution effects depends on subjective intent. To be sure, the case for the third-party doctrine is clearest and most dramatic with a defendant who makes a conscious choice to use a third party to evade detection. But the danger of substitution effects does not rely on the point. What matters is how much protection the Fourth Amendment provides given the third par-

22. Kerr, *supra* note 1, at 590-600.

23. I do not mean to wade into the debate of whether in fact the Fourth Amendment would be better if judges had more options than no protection or full protection. Other commentators have analyzed this issue far better than I can here. *See* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349 (1974). For my purposes, it is enough to note that existing doctrine does not allow it, and that my case for the third-party doctrine presupposes the framework of existing law.

24. Murphy, *supra* note 3, at 1241.

25. *Id.*

26. *Id.*

27. *Id.* at 1242.

28. *Id.* at 1243.

ties that criminals actually use, not whether criminals happen to use third parties because they have calculated that it will help them avoid detection, or because it's convenient, or for some other reason. The reality is that criminals do in fact use the telephone, banks, and other third parties to commit crimes. Their motivations as to *why* are irrelevant to the substitution effect. So long as criminals take steps that replace outside acts with third-party transactions in the course of their crimes, the substitution effect will exist.

Murphy also notes that many crimes are committed without third parties.[29] That is true, but I am not sure how it is relevant. The fact that many crimes are not committed using third parties in a world with the third-party doctrine does not show the rule isn't useful, just as the fact that many people commit crimes individually does not show that severe penalties for conspiracy aren't useful. Murphy also notes that it may be difficult or even impossible to commit some crimes using third parties, such as drunk driving.[30] But this only suggests that the third-party doctrine is not necessary to maintain technology neutral Fourth Amendment rules for investigations of those particular offenses. Again, I am not sure how that is relevant. In my view, the key question is not whether the third-party doctrine is necessary for the police to investigate every type of crime. The question is whether, on the whole, the rule enables the proper balance between privacy and security given the need for rules that encompass investigations into all different types of crimes.

B. DO THE INNATE DANGERS OF GROUP CRIMES NEGATE THE NEED FOR THE THIRD PARTY DOCTRINE?

My favorite of Murphy's arguments is her assertion that the third-party doctrine is not needed because relying on a third party to commit a crime is already risky.[31] According to Murphy, "enlisting third-party assistance in crime tends to generate, rather than obfuscate, opportunities to get caught."[32] Third parties can rat you out to the cops, and their use can leave a paper trail.[33] As a result, a rational criminal will not rely on third parties regardless of the Fourth Amendment rule.[34] The criminals that do rely on third parties are therefore not very rational, and their conduct is unlikely to be impacted by the operative Fourth Amendment rule.[35]

I think there are three difficulties with this argument. First, as discussed above, the rational actor assumption is largely beside the point. The key ques-

29. *Id.*
30. *Id.*
31. *Id.* at 1244.
32. *Id.*
33. *Id.*
34. *Id.*
35. *Id.*

tion is how the third-party doctrine (or its absence) distributes privacy, not how often a wrongdoer makes the conscious decision to use a third party (or refrain from it) to avoid being caught. Second, the risks of involving third parties in crime generally presuppose the existence of the third-party doctrine. Although the use of a third party can create a paper trail, that paper trail matters because the third-party doctrine leaves it unprotected. In a world without the third-party doctrine, the risks of group crimes would be much lower. The now-exposed paper trail presumably would be as protected as secret plans stored in the suspect's sock drawer.

Even assuming the cost-benefit framework that Murphy suggests, I think the cost Murphy identifies tends to be small or even negligible in most of the interesting applications of the third-party doctrine. The cost is high when a wrongdoer seeks a co-conspirator or solicits crime. If A hires B to kill C, A must disclose his criminal plans to B, creating a potential witness against A. At the same time, the most controversial applications of the third-party doctrine do not communicate criminality or seek conspirators. The most controversial cases involve provider/customer relationships with third-party service providers such as banks, telephone companies, and ISPs. These companies have no reason to watch their customers' conduct closely. Such businesses often have thousands if not millions of customers, and they are not looking to rat them out. On the contrary, as I explain in my article, they have very good business reasons to protect their customers' privacy.[36] As a result, the cost Murphy identifies may exist in theory, but is likely small in the most controversial applications of the doctrine.

C. MURPHY ON MURKINESS

Murphy also cautiously disagrees with my view that the third-party doctrine furthers the goal of ex ante clarity.[37] She does so by offering her own answers to a hypothetical I offer in my article involving an anonymous blog comment about a bribe of a Senator.[38] In my article, I offered that hypothetical to illustrate that if you assume a probabilistic view of expectations of privacy, in which a reasonable expectation of privacy exists when privacy is likely, then whether the Fourth Amendment applies depends on unknowable information history rather than known information location.

Murphy answers the hypothetical with two steps.[39] First, she relies on existing law holding that the Fourth Amendment does not regulate subpoenas

36. *See* Kerr, *supra* note 1, at 598-600.
37. Murphy, *supra* note 3, at 1245.
38. *See* Kerr, *supra* note 1, at 584.
39. Murphy, *supra* note 3, at 1245.

to testify.[40] So long as the person called to testify only testifies to what they know, then the Fourth Amendment isn't implicated. Second, she concludes that she would not personally object to a Fourth Amendment rule that all other cases would be protected by the Fourth Amendment.[41] Thus, we arrive at a form of ex ante clarity: The Fourth Amendment protects everything except the subpoena to testify in person.

Murphy's solution is interesting, but I fear that it does not respond to the hypothetical. The hypothetical presupposes a world without the third-party doctrine, in which the question of whether an expectation of privacy is "reasonable" must be answered by a probabilistic determination in each case of whether there was a person who once had the information who reasonably expected privacy. That is, the question is whether someone along the line actually and reasonably expected privacy that the subpoena violated. What existing doctrine provides, and what legal rules Murphy would find acceptable, cannot answer this.

More broadly, Murphy's difficulty identifying an alternative to the third-party doctrine nicely demonstrates my concerns with ex ante clarity.[42] My argument about ex ante clarity is that replacing the third-party doctrine is surprisingly hard. The police need certain answers about what rules they must follow. The existing third-party doctrine provides legal answers that eliminate the difficult task of devising specific rules for each and every use of third party records. When Professor Murphy turns to replacing the third-party doctrine, she acknowledges with admirable candor that she has "no idea" what should replace the third-party doctrine.[43] She offers a few vague proposals for what the new law might look like, but she does not jump into the nitty-gritty of classifying all of the possible cases.[44] I don't mean that as criticism of her substantive proposals. Murphy's essay is brief, and complete answers would be overly ambitious. However, Murphy's admitted uncertainty about what should replace the third-party doctrine supports my point that the ex ante clarity problem is a serious one.

III. CONCLUSION

In the introduction to *The Case for the Third Party Doctrine*, I stated that my goal was "to replace the partial view of the third-party doctrine found in existing scholarship with a richer and more balanced account of its costs and

40. *Id.* at 1246.
41. *Id.*
42. *See id.* at 1251.
43. *Id.*
44. *Id.*

benefits."[45] My hope was that a fresh perspective on the doctrine could help inspire a deeper understanding of its dynamics. I am delighted that Richard Epstein and Erin Murphy have now taken up the challenge; we are all better off for their efforts. If my article helped triggered their contributions, the article was more successful than I ever expected.

45. Kerr, *supra* note 1, at 566.

THE CASE AGAINST THE CASE FOR THIRD-PARTY DOCTRINE: A RESPONSE TO EPSTEIN AND KERR

By Erin Murphy[†]

TABLE OF CONTENTS

Professor Epstein, Professor Kerr, and I may at times approach legal questions from different perspectives, but there is one thing that we all agree upon: the current configuration of third-party doctrine under the Fourth Amendment is problematic. However, lest you worry that this unanimity makes for uninteresting commentary, fear not: that might be all that we agree upon.

In his wonderful and thought provoking article, *The Case for Third Party Doctrine*, and in his comments today, Professor Kerr asserts that the chief defect of the third-party doctrine is one of form, not substance.[1] He finds the rule itself—that information disclosed to third parties receives no Fourth Amendment protection—to be basically a good one. Professor Kerr defends the third-party doctrine in principle, and argues two additional points: first that we should justify it differently (as founded in consent rather than in rea-

† Assistant Professor of Law, University of California, Berkeley, School of Law. My thanks to Professor Paul Schwartz and the Berkeley Center for Law and Technology for inviting me to participate in the 2009 Privacy Lecture, and to Professors Epstein and Kerr for providing such wonderful ideas for discussion.

1. Orin S. Kerr, *The Case for Third Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

sonable expectations of privacy), and second that we should worry less about it (because other legal regimes exist to protect us).

In contrast, in *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*,[2] Professor Epstein is a bit more skeptical and thus a bit more cautious. A rose by any other name, he observes, smells just as sweet. "Consent" is just another way of saying assumption of risk, which falters in the context of unilaterally imposed, government-generated criminal enforcement. In search of a meaningful restraint on state power, then, eventually we will end up right back where we began: the reasonable expectation of privacy. An imperfect doctrine, Professor Epstein concedes, but one that if by nothing other than by the sheer dint of its popularity must achieve something.[3]

Now, Professor Epstein candidly acknowledges coming at the third-party problem as, if you will, a third party. Specifically, he writes as someone "outside of the field of criminal procedure, but with a strong commitment in favor of the principles of limited government."[4] This perspective probably explains why he describes his goal as to "parse the arguments in order to develop a unified approach . . . that can win adherents both within the field and beyond it,"[5] rather than come down wholly on one side or another. Such wild ideas are clearly those of an outsider, someone unfamiliar with the norms of the discipline. In criminal justice, you are either with us or against us. You are either working to free all the criminals or you are an apologist for the fascist police state! This is not a field known for its conciliatory, nuanced "unified approaches."

Having thus stepped into a play that clearly casts Professor Kerr as the defender of the police state and Professor Epstein as the voice of virtuous moderation, I suppose it only remains for me to dutifully assume the role of the advocate for freeing all the criminals. Which, alas, means that Professor Kerr's lucid and important defense of the much-maligned third-party doctrine, having just been knocked around by the middle, is now to be fully assaulted from the left.

I will start by posing the two major questions at stake: should there be any third-party protection at all, and if so, what should it look like? Since Professor Epstein focused most of his attention on the latter point, I will

2. Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199 (2009).

3. *Id.* at 1208.

4. *Id.* at 1200.

5. *Id.* at 1200-01.

spend my time more on the former.[6] To answer that general question, I intend to proceed in the following four steps. First, having agreed with Professor Epstein's critiques of Professor Kerr's technological neutrality and ex ante clarity rationales for scrapping third party protection, I will add two critiques of my own. Second, in the spirit of reconciliation, I will provide an alternative defense for denying third-party protection; but then, in a revived spirit of partisanship, I will turn to attack my own rationale. Third, with lingering pique, I will critique Professor Epstein's alternative approach. Fourth and lastly, I will present in the hopeful and ingenuous manner of an assistant professor some thoughts on how to conceive of a viable third-party protection doctrine.

I. NEUTRALITY, CLARITY, AND EQUALITY: A RESPONSE TO KERR

A. TECHNOLOGICAL NEUTRALITY

Like Professor Epstein, I find Professor Kerr's insight about technological neutrality and substitution effects quite compelling—namely, that the third-party doctrine ensures that savvy criminals cannot strategically exploit sophisticated technological methods to evade detection. But, like Professor Epstein, I find that this insight is open to the critique that it also cuts the other way. Specifically, because the technologies left exposed by third-party doctrine are not exclusively deployed for illicit purposes, failing to protect them generates negative externalities (by dissuading innocent, desirable conduct); thus the possibility of "substitution effects" alone cannot justify the existence of the doctrine.[7]

To this observation I would also add a more fundamental critique, however. Specifically, I am not convinced that such "substitution effects" really take place, at least not on the scale and to the degree that would justify forfeiting all third-party protection. In essence, Professor Kerr claims that extending third-party protections would simply inspire "a rational actor bent on

6. I will note quickly at the outset, though, that I agree that the "assumption of risk" or autonomy framework is the wrong way to go about thinking about whether disclosures to third-parties deserve protection. I also share Professor Epstein's sense that Professor Kerr's "consent" model seems to just circle back to the reasonable expectation of privacy test. Epstein, *supra* note 2, at 1206. Similarly, I concur with Professor Epstein's observation that a notice principle too readily leads to the evisceration of substantive rights, particularly when the coercive power of the government is at issue. *See infra* Part II. Thus, I join in Professor Epstein's search for alternatives geared toward optimizing social utility (even though I typically tend not to phrase my objectives in such economic terms).

7. Epstein, *supra* note 2, at 1226 (discussing "social inefficiencies with respect to lawful conduct that people naturally wish to keep from the prying eye of the state").

criminal conduct [to] use as many third-party services as he can to avoid detection."[8] It is perhaps not surprising that this claim did not capture the attention of Professor Epstein, but it did capture mine—for two reasons.

First, I am not a big believer in the "rational criminal actor." What we know about the criminal actor is that he is usually poor, uneducated, and high on drugs or alcohol a surprising amount of the time.[9] Thus, in the majority of cases, the criminal actor will not be thinking much of third-party outsourcing as a means of evading detection. Of course, we might speculate that the third-party doctrine arises most frequently in cases in which defendants are better educated and resourced—"white collar" crimes, for instance—and thus more likely to act "rationally." But I would argue that the sheer degree to which third-party interactions permeate contemporary life, across all socio-economic boundaries, calls that assumption into question. The doctrine is as much about the secrets told a cellmate as those shared with an investment banker, or the DNA left on a soda can as that given to the doctor during an exam. Recall, after all, that of the two foundational opinions setting out the third-party doctrine, one—*Smith*—was essentially a glorified stalking case.[10] Even mob or racketeering cases, for which third-party doctrine currently eases the path of investigation, inevitably ensnare the impulsive little fish along with the more calculating big ones. In this day and age, *cives technologicus sumus*.[11]

Even assuming the rationally acting criminal, I am still not convinced that Professor Kerr's substitution effect is real. Take the example he gives of Smith the telephone stalker.[12] In the pre-technology world, says Professor Kerr, Smith has to leave the house, drive around, and ring doorbells in order to stalk his victim: all conduct that requires him to be out and about where he can be publicly observed and therefore apprehended.[13] In the technologi-

---

8. Kerr, *supra* note 1, at 580.

9. *See generally* BUREAU OF JUSTICE STATISTICS, U.S DEPARTMENT OF JUSTICE, CRIMINAL OFFENDER STATISTICS (2007), http://www.ojp.usdoj.gov/bjs/crimoff.htm#inmates (describing summary findings from various government reports on the characteristics of state jail and prison inmates, including that roughly 50% were under the influence of drugs or alcohol at the time of the offense, 75% were using drugs or alcohol during that period, roughly 43% had no high school degree or equivalent, and over half have mental health problems). The numbers for federal inmates are only marginally lower. *Id.*

10. Smith v. Maryland, 442 U.S. 735, 737 (1979) (describing how Smith was identified as a robber after repeatedly driving through the victim's neighborhood and making threatening and obscene phone calls).

11. That is, playing on the famous Roman incantation of "civis romanus sum," we are all citizens of technology—bestowed with both the privileges and burdens of our subjugation.

12. Kerr, *supra* note 1, at 580.

13. *Id.* at 578-79.

cal world, though, Professor Kerr proposes that Smith can stalk his victim by phone or Internet with the curtain drawn at home, thereby eluding easy detection if the law interposes an impediment in the form of third-party protection.[14] Thus, he concludes, what stalker would not go with the technological route? You don't even have to change out of your pajamas! But get rid of those protections, argues Professor Kerr, and Smith the phone-stalker is as amenable to detection as Smith the window-peeper.[15]

But is that the right way to frame the issue? A lot of crime does not come with an obvious technological alternative, or to the extent that outsourcing is possible, it fundamentally alters the nature of the offense. One generally cannot murder, rape, or cause serious bodily injury via technology alone. Even if the proper measurement is not the seriousness of the offense but its rate of occurrence, technological outsourcing still raises no real concern. Technology does not offer much by way of protection from accusations of disorderly conduct, or drinking and driving, or even drug distribution—the kinds of crime that, for better or for worse, make up the vast majority of criminal offenses in our country.[16] To the extent that there might be some subset of crimes—say, child pornography or internet fraud—that are disproportionately amenable to third-party technological outsourcing, then it is still worth asking how much of what is involved is a true *substitution* effect as opposed to simply a sub-species of crimes in which third-party participation is an indispensable component (or even instrument) of the offense. Erecting third-party protections would make investigating such crimes more difficult, to be sure, but less because the offender substitutes the Internet for stepping out to the mailbox to get his illicit images than because there are so many more images, and offenders, to police. If that is the case, then third-party doctrine is not so much creating technological neutrality as it is forging a technological exception.

So if it's not universally the case that technology makes possible or incentivizes substitution effects, then is there anything about the nature of how technology is deployed in crime, either its capacity to be private rather than

---

14. *Id.*

15. *Id.* at 578.

16. In 2007, for example, there were over 14 million arrests reported by law enforcement agencies participating in the Uniform Crime Reporting System. A significant number of those were for crimes that seem resistant to substitution, such as drugs (1.8 million), property crimes like burglary, theft, and arson (1.6 million), DUI (1.4 million), assault (1.3 million), disorderly conduct (709,105), liquor violations (633,654), and drunkenness (589,402). CRIMINAL JUSTICE INFORMATION SERVICES DIVISION, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE, *Table 29: Estimated Number of Arrests, in* CRIME IN THE UNITED STATES, 2007 (2008) http://www.fbi.gov/ucr/cius2007/data/table_29.html.

public or the nature of the offenses that are committed via technology, that requires "equalizing"? Do we have to let the police access Google search records without fear of the Fourth Amendment either because they cannot come to your living room to watch your websurfing, or because the kinds of crimes committed online are particularly heinous? In essence, this is just another way of asking whether private crime, and in particular really heinous private crime, should be rendered as readily policeable as public crime. To this, the Constitution has already given us an answer: no. For better or for worse, we have a trans-substantive Fourth Amendment. We do not obliterate privacy protections for the home, for instance, just because the vast majority of child sexual abuse occurs there. Besides, constitutional criminal procedure has crafted other means of dealing with the problems posed by complex or difficult to investigate crimes—namely, the grand jury, which is virtually immune from Fourth Amendment strictures.[17]

Moreover, even to the extent that there are categories of offenses like theft, fraud, or white collar crimes that are more readily outsourced via technology, it still is not clear that third-party participation makes policing all that harder or easier. In fact, it seems probable that the more that third-parties are involved or technology is deployed, even with a robust conception of third-party protections, the more likely it becomes that the criminal will be apprehended. This is for the simple reason that enlisting third-party assistance in crime tends to generate, rather than obfuscate, opportunities to get caught. Third parties increase the possibility that a trail will be left or witnesses will be created, all of which only helps the state in building its case.

Think again about Smith. Suppose Smith took Professor Kerr's technological route, and instead wrote emails or made phone calls. It is true that in a world of third-party protections, the police would likely need something like a warrant and probable cause to get their hands on them. But that is not a particularly high a standard to meet. Even in *Smith* itself, the police had the description of the robber and the make and model of a car at the scene, which matched the car (by license plate) that drove slowly by the victim's house at the time she received threatening and obscene phone calls from the robber.[18] That alone likely constitutes probable cause for a warrant. And once Smith was arrested, wouldn't it be easier to make out the stalking case with the emails and phone calls than, for instance, with just the testimony of the victim that some guy keeps coming around?

In truth, Smith's best bet for evading detection for his stalking was probably not the highly public act of skulking around, nor the intensely private,

17. United States v. Dionisio, 410 U.S. 1, 11-12 (1973).
18. Smith v. Maryland, 442 U.S. 735, 737 (1979).

technologically-substitutive act of calling or emailing, but rather an intermediate public/private, high-tech/lo-tech hybrid of typing and mailing old-fashioned letters (so long as he did not lick the envelope). Thus, if anything, the hypothetical demonstrates that the most likely "substitution effect" of technology may be the slight creation of a front end problem (getting your hands on evidence) in favor of a nice solution to a back end problem (that evidence being persuasive). If that is the case, then it is even less clear which way substitution actually cuts, and this need for "technology neutrality" to level the playing field does not really exist.

B. EX ANTE CLARITY

So then what about Professor Kerr's argument for third-party doctrine on the grounds of ex ante clarity? Like Professor Epstein, I find this point unpersuasive as a normative justification for the lack of protection. After all, if the primary aim is clarity, then I would instead vote in favor of a very clear rule (and one with ample constitutional support) that simply prohibits all third-party investigation without a warrant or probable cause—the "libertarian baseline," if you will.

But even assuming that the ex ante clarity rationale points toward eliminating rather than bolstering third-party protection, then is devising a legal regime really so unworkable and unclear? Professor Kerr argues that the need for clarity is particularly acute with regard to information in the hands of third parties, because sourcing the origins of information ex ante is virtually impossible.[19] This he calls the "information history" problem, and he sums it up nicely with the example of the anonymous blog commenter who posts about a rumored bribe to a Senator.[20] If the government wants to subpoena the commenter, Professor Kerr asks, how will it know whether doing so would violate the Senator's rights under the Fourth Amendment? Professor Kerr posits five scenarios to tease out the issue, in which the blog commenter is: (1) a bank teller who deposited the bribe for the Senator; (2) a bank customer who overhead the Senator's deposit; (3) a bank robber who stole the records; (4) the briber; or (5) the Senator herself.[21] Although a reconstituted third-party doctrine might protect some of these, the government would not know ex ante, at the time of its subpoena, which was the operable scenario.

I have to admit this one stumped me for a while. But then I realized that, as framed, it is not quite right. The scenario actually implies two levels of possible third-party problems. The first regards the request to the blogger's

19. Kerr, *supra* note 1, at 582.
20. *Id.* at 584.
21. *Id.*

ISP for the name of the commenter. But that should not be a problem, third-party protection or no third-party protection, because the Fourth Amendment does not apply to grand jury subpoenas to appear and testify, and the only limit on subpoena *duces tecum* is that it not be "unreasonable." So, done.

But what if there is no grand jury investigation? What if it is just the police officer, kicking around on the Internet, trying to come up with a to-do list for tomorrow? Well, in that case, I say so be it. If an anonymous tip about a person with a gun is not enough to shake someone down on the street,[22] then I am comfortable saying that an anonymous tip of a Senator with a bribe should not be enough to shake someone down on the Internet. Sure, we want to catch gun-toting bus stop patrons and Senators with fat pockets, but not at the expense of trading individual liberty for blind faith in the statements of any Tom, Dick, or Jane with a DSL connection. If the Internet has taught us anything, it has taught us not to believe everything we read, especially when it comes from someone unwilling to back up their allegations with their true name.

What about the second level, then? Assume now that the government knows the name of the commenter, but has to determine whether questioning the commenter about the bribe will violate the Senator's rights. Here, again, this poses no problem in the context of a grand jury investigation. There may be other protections that come into play—for instance, the Senator, the Robber, and the Briber might all have Fifth Amendment privileges, but other than that no Fourth Amendment concerns arise.

What if the context is not the grand jury, but just ordinary investigatory policing? In that case, I disagree with Professor Kerr that the problem posed by third-party doctrine is how the police will figure out from where the information comes. After all, discerning the nature of the source of information is a critical and common part of determining its reliability. It should be expected that officers would ask the commenter, "who are you and how did you learn about this bribe?" right after flashing their badges. In that case, we can easily imagine a functional third-party rule (hinging on the confidence in which the information is transmitted or obtained) that would immediately clue investigators in to proceed no further if the answer is: "I work at the bank," or "I'm the Senator's best friend" or "I stole it," as opposed to "I overheard it on the street" or "I made it up." Indeed, in all likelihood officers would ascertain that information before knocking on the door. It might even be readily apparent from running a routine background check on the information given to them by the ISP that the person is a lobbyist or a bank employee or a criminal with a history of bank robbery or the Senator herself.

22. Florida v. J.L., 529 U.S. 266, 274 (2000).

C. ALTERNATIVE JUSTIFICATIONS FOR ELIMINATING THIRD-PARTY PROTECTIONS

Having joined forces with Professor Epstein in disputing Professor Kerr's twinned virtues of the third-party doctrine—that it affords technological neutrality and that it provides ex ante clarity—is it thus a foregone conclusion that the doctrine should go? Let me provide one half-hearted attempt to supply an alternative justification, which might be deemed technological neutrality in another sense of the term.

If it is true that third-party protections largely come into play with regard to white-collar or organized crime or other sophisticated policing efforts, then even if third-party doctrine is not exclusively a rich people's problem, it is at the very least a middle and upper class issue. In that case, eliminating third-party protections may have an equalizing effect—not between private and public criminality or technological and non-technological offenses as Professor Kerr maintains, but between street and sophisticated crime, or poor people and not-so-poor people crime. The true substitution effect, in other words, is not the manner in which the same criminal commits his crime, but rather one kind of criminal defendant (rich) for another (poor). In Professor Bill Stuntz's terms, it is a matter of displacement and incentives: the more procedurally difficult it is for investigators to obtain the things they need to net the big fish, like bank or phone or ISP records, the more they might be inclined to focus on netting the small, corner fish instead.[23]

Accordingly, it might be posited that third-party doctrine as it currently stands levels the *investigatory* playing field. This alone might serve as a legitimate justification for third-party doctrine: not that it enforces technological non-substitution, but that it ensures socio-economic non-substitution. Yet for several reasons, I believe this defense cannot stand. Most notably, as I suggested earlier, I dispute the initial premise that third-party doctrine primarily affects or applies to white-collar cases.[24]

But even assuming that eliminating third-party constitutional protections creates socio-economic equality, the problem remains that, for the most part, resourced people will not tolerate that equality. Resourced people do not like having their bank, e-mail, and video records open for the government to see. So they call Congress. And they get things passed. And suddenly there is the Wiretapping Act and the Electronic Communication Privacy Act and HIPPAA and the Video Privacy Act and so on. Meanwhile, no one lobbies for

---

23. *See generally* William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 574-75 (2001); William J. Stuntz, *The Uneasy Relationship Between Criminal Procedure and Criminal Justice*, 107 YALE L.J. 1, 3-4 (1997).

24. *See supra* text accompanying notes 10-11.

the Thin Walls and Crowded Conditions of Public Housing Privacy Act, or the I Never Should Have Said That To My Cellmate Act, or the I Cannot Afford a Private Car or Gulfstream 5 and So I Am Stuck Handing My Bag and My Liberty Over to Greyhound Act.

So to the extent that I might be able to rally some support for eliminating third party protection on the grounds that it would create congruence in Fourth Amendment coverage (or more accurately put, *lack* of coverage) for the rich as well as the poor, then the existence of all those statutory protections that Professor Kerr later cites as bulwarks against abuse somewhat dims my enthusiasm for that approach. Besides, if leveling the gap between the rich and the poor is to occur, I would much prefer the extension of protection to the poor, rather than the reduction of privileges held by the rich. After all, who finds a sinking-tide-sinks-all-boats theory an attractive axiom for doling out rights?

II. PRIVATE LAW AND THIRD-PARTY DOCTRINE: A RESPONSE TO EPSTEIN

Having disputed both of Professor Kerr's rationales for eliminating third-party doctrine, and then having supplied (and disputed) an alternative rationale of my own, it remains now to ask from where third-party protections—if they existed—might draw some principled guidance. It is on this question that Professor Epstein focuses most of his attention. Specifically, having rejected the autonomy rationale for eliminating third-party protection, Professor Epstein undertakes a theory grounded in optimal social utility, thereby giving content to the reasonable expectation of privacy by means of social conventions and drawing particularly on private law analogies.

Professor Epstein frames the background inquiry as "are there things that the police can do without regard or resort to their state power, because ordinary citizens can do them too?" If private law prohibits the private actor, so too might it forbid the public actor. If private law allows it, then so too might the Constitution. Of course, Professor Epstein acknowledges a zone of hard cases, but then the question becomes one of nuanced calibrations in which even the hard cases, like those involving fraud committed in the name of public as opposed to private interest, have delicate contours in private law that might or might not transfer to the public law context.

At base, I agree with his general project of attempting to locate some set of overarching principles to guide the formulation of a reconstituted third-party protection. My concern, however, is that lost in this astute and interesting series of analogies is an acknowledgement of that which differentiates private and public law, or private and public power, and which distinguishes

the ordinary citizen from the officer of the state. The question of who is doing something, and why, is as important to me as the question of under what authority it is being done. Private law develops and operates against a backdrop of assumptions that, to my mind, do not hold when applied to the criminal context. Private law actors are presumed to be equal; they are autonomous; they are rational, capable of contracting, and subject to consequences for their actions and choices. What is different about public actors, and why we need special restraints, is that these assumptions no longer necessarily remain true. Indeed, for effective policing to take place, they necessarily remain *not* true. Professor Epstein agrees with all of this in rejecting Professor Kerr's consent and assumption of risk based model, but I fear he too readily relinquishes the profundity of this observation in formulating his own alternatives.

In simpler terms: It is true that I, Erin Murphy, can knock on your door and ask to come in and that the police can knock on your door and ask to come in. We may both have the same authority (namely, none), but you will not experience those knocks in the same way. I do not mean as a subjective matter, which is obviously the case. I mean it objectively as well. For instance, if I shove my way in, you have a means of getting me out (calling the police). If the police shove their way in, you are pretty much at their mercy. If I start asking you a lot of questions about your finances or habits, you will assume I am a nosy person and tell me to bug off. If the police start asking you a lot of questions about your finances or habits, you will assume that telling them to bug off will get you nowhere, and will likely feel pressured to answer. If I get mad that you are not cooperating, and put you in handcuffs and lock you up for twenty-four hours for no reason, I can get convicted, go to jail and be held civilly liable. If the police get mad and put you in handcuffs and lock you up for twenty-four hours for no reason, you have probably just lost twenty-four hours. If I pull a gun on you, or steal your briefcase, I am definitely committing a crime. If the police pull a gun on you, they might just be making a good faith mistake. Even if they steal your briefcase, the most you might get is a stern reproach from the Supreme Court saying "no one should condone" such "possibly criminal behavior."[25] And good luck collecting damages in civil court.

I could go on, but you get the picture. Citizens and the police are not the same. We should never treat them the same. The police can do things that ordinary citizens cannot, for the most part, do: carry guns, lock people up, and conduct searches. The police benefit from default presumptions that ordinary citizens lack: police desires and actions are presumed to be consonant

25. United States v. Payner, 447 U.S. 727, 733 (1980).

with their public protection mission, whereas the same desires and actions by a private person are presumptively illegal or criminal. The police are protected from consequences in a way that ordinary citizens are not.

For the most part, these distinctions are as they should be. Every civilized society requires a police force to safeguard the rule of law. A police force should be vested with both social and actual authority to execute its mission appropriately. If a stranger busts into someone's house, we assume that person is acting with ill intent; if the police bust into your house, we assume they are there for good reason. We rely on the police to have that special aura of perceived and actual power. But, accordingly, the background assumption of policing should always be that police are different. Of course, a good libertarian will agree with me, as Professor Epstein does in the context of Professor Kerr's assumption of risk and notice discussion: simple notice arguments do not work in the Fourth Amendment context because power trumps notice every time.

For the same reason, I would proffer that the private analogy path is a dangerous one to go down generally, because public power runs on different cylinders than private ordering. That is not to say that police should not be able to do some of the things that an ordinary citizen does. But that should be the beginning of an analysis, not the end. Sure the operator could see the number that Smith dialed. But you know who couldn't? Every other person in the neighborhood. If we really treated the police like any ordinary citizen, then our result in *Smith* would have to be that the average ordinary citizen cannot see the numbers, therefore they were constitutionally protected. There is a difference between thinking of the police as *any* ordinary Joe versus thinking of the police as *every* ordinary Joe. Confusing these two—and adopting the latter position while stating the former, makes the police not Everyman but *every man*. It makes the police omnipotent and omnipresent. Precisely what, I would argue, the drafters of the Fourth Amendment feared and thus forbid.

III. TOWARD A THEORY OF THIRD-PARTY PROTECTION

Having abused every theory and done my Chicken Little government-power routine, then, do I have anything left to say for myself? Well, to avoid Professor Kerr's apt invocation of the "takes-a-theory-to-beat-a-theory" mantra, let me give it my best shot.

By now, it is probably obvious by implication that I do not view Professor Kerr's proposed four alternative, non-constitutional routes of protection

as anywhere near adequate. To wit: *Massiah*[26] is a frail and ailing patient (rendered all but comatose by *Montejo* and *Cobb*);[27] entrapment is so dead that I do not even bother to teach it; vicarious assertions seem so unlikely that Google—arguably a force more powerful than the government—stood alone against the government's subpoenas for search records from large ISPs including Yahoo and MSN, and its most formidable argument rested on commercial trade secret doctrine;[28] and the statutory privileges are barely worth the paper they are printed on. (I am guessing most people these days would happily exchange their priest-penitent privileges for ISP-websurfer ones—although some reports suggest that the two at times may overlap.)[29]

So if I want some kind of constitutional third-party protection, and I recognize that it cannot simply be contiguous with the defendant's Fourth Amendment rights, then how might I imagine the doctrine? Truthfully, I have no idea.

As I see it, the real obstacle to implementing third-party doctrine is that it creates the potential for conflict between a third party from whom information is sought, and the defendant against whom the action ultimately is taken. This conflict occurs both in terms of each party's desire to assert the protection and its probability of doing so. In a world in which we afford some third-party protection, when the knock on a third party's door arrives, how will they experience their authority to assert what feels like the Senator's rights?

To begin with, how will the third party even know they have rights to assert? Investigatory policing hinges on the fiction of "voluntariness"—police routinely get inside the most sacred of Fourth Amendment spaces, the home, simply by asking permission to come in. But to the extent that we barely accept this fiction of voluntariness in the context of intrusions on suspects themselves—individuals that we expect to have clear instincts against complying—we might be even more uncomfortable in justifying such intrusions

---

26. Massiah v. United States, 377 U.S. 201 (1964).

27. Montejo v. Louisiana, 129 S. Ct. 2079, 2091 (2009) (overruling Michigan v. Jackson, 475 U.S. 625 (1986), and holding that court's appointment of counsel does not preclude further police initiation of questioning); Texas v. Cobb, 532 U.S. 162, 172-73 (2001) (holding that *Massiah*'s Sixth Amendment right to counsel at the time of interrogation applies only to formally charged offenses and their equivalents under the exceedingly narrow *Blockburger* "same offense" test).

28. Katie Hafner & Matt Richtel, *Google Resists U.S. Subpoena of Search Data*, N.Y. TIMES, Jan. 20, 2006, at A1 (noting that three of its competitors complied without resisting).

29. Ashley Fantz, *Forgive Us, Father; We'd Rather Go Online*, CNN, Mar. 13, 2008, http://www.cnn.com/2008/LIVING/wayoflife/03/13/online.confessions/ (discussing rise in both religious and non-religious online confession sites).

as voluntary compliance when it is a third party being asked to sell someone else down the river.

More problematically, what if the third party wants to comply? Even more troubling, what if the Senator wishes they would not? Should a third party's autonomous desire to share the Senator's secret or offer up records given in confidence be restrained in the name of safeguarding the Senator's Fourth Amendment rights? Is there any principled basis for allowing the Senator to voluntarily provide information or give up documents to investigators (perhaps to curry favorable treatment) while forbidding the same voluntary compliance from third parties? Even if such a basis existed, could it be articulated and enforced?

These are real problems, to be sure. But they have available, if imperfect, solutions that fall short of dispensing with third-party protections altogether. For starters, we could simply allow third parties to waive Fourth Amendment rights as easily as we allow the defendant to do the same. Crazy, maybe, but that would make the real risk of disclosure to third parties the possibility of picking someone who doesn't have your back. As it stands, third-party doctrine admits no difference between good choices and bad choices: it draws no meaningful distinction between third parties that want to shield the confidence and those that do not.

But why should this be so? A reconstituted third-party doctrine might recognize that some disclosures are made in confidence, that there is value to such confidence, and that if the parties respect it, then the government should too. In such a regime, disclosures made to informants and undercovers, of course, would remain unregulated (as "bad choices" in which to repose confidence), but at least constitutional protection would extend to information held by protective entities and true confidantes. Pick a good ISP or best friend, willing to resist government inquiries and assert Fourth Amendment protection, and you can rest assured—well, at least until the government returns with a warrant and probable cause.

We might even devise a sliding scale of protections that aims to embody important communal and constitutional values: the role of trust in our society, the notion of agency, the need and desirability of third-party confidences, and some idea of autonomy and consent. We could imagine an imperfect but viable hierarchy of disclosures, and concomitant ranges of protection to lack of protection, for disclosures that are of absolute necessity (e.g., medical) to those of effective necessity (e.g., banks, utilities, e-mail, etc.) to those of comfort and convenience (e.g., friends, entertainment records) to those that are primarily elective (e.g., social networks, blogs, etc.). The question of which third parties receive protection may be tricky, to be sure. But how to enforce those protections seems less problematic.

Moreover, we might even impose a heightened standard for what constitutes "voluntary" disclosure of information held by third parties. We might, for instance, require covered third parties (imagine for instance banks and medical professionals) to be informed of the Fourth Amendment right of the defendant to keep this information from government hands absent a warrant and probable cause, before being asked whether they are willing to waive it. Statutory regimes that impose civil liability for wrongful disclosure represent a variation on this theme: the third parties all know about the individual's rights, because they are legally entrusted with safeguarding them.

Most importantly, note that neither suggestion eviscerates the government's investigative authority. We still preserve the power of the government to seek, through a warrant and probable cause or grand jury subpoena, information held in the hands of third parties. The difference is that we also give those parties a right to resist that is akin to the defendant's own right, and the defendant in turn may assert that information obtained in a non-compliant fashion should be suppressed as a violation of the Fourth Amendment. In essence, this regime represents a form of limited consent.

If this does not sound so radical, it is because it is not. As Professor Kerr himself points out, current statutory doctrines create similar structures.[30] We have a range of statutory protections for health records, financial records, video records, and so on. In his hypothetical, for example, the bank teller could possibly resist the government request under the Right to Financial Privacy Act. Some ISPs have fought government requests for information by claiming their clients' First Amendment rights or, as in the well-publicized Google search engine query case, generalized privacy protections. Yet the existence of such protections has not ground investigations to a halt, or left the government hobbled by a confusing web of indiscernible rules. And of course, worst-case scenario: the evidence is suppressed. A wrong call on third-party protection ("what, that was your sister?!") does no more or less damage than a wrong call on reasonable, articulable suspicion.

In the end, then, it may very well be that Professor Kerr and I differ more as a matter of form or institutional preference than of substance. He says that the legislature should craft such regimes. I worry that the legislature *will* create entitlements for the issues and concerns that are raised by its powerful constituents and lobbyists, but that the poor and disempowered will be left unprotected. And that is a result that, given the values enshrined in the Fourth Amendment, to me seems both unnecessary and indefensible.

---

30. Kerr, *supra* note 1, at 596.