CONSUMERISM AND INFORMATION PRIVACY: HOW UPTON SINCLAIR CAN AGAIN SAVE US FROM OURSELVES

Benjamin R. Sachs[*]

THIS Note will address the salience of a simple analogy: will privacy law be for the information age what consumer protection law was for the industrial age? At the height of industrialization, the United States market for consumer products faced instability caused by a lack of consumer competence, lack of disclosure about product defects, and advancements in technology that exacerbated the market's flaws. As this Note will show, these same causes of market failure are stirring in today's economy as well. The modern economy is not one of goods but of information, and although consumers have long been aware that their personal information may have marketing value, the Internet has fundamentally changed the scope and depth of information collection, exposing more consumers than ever to injuries requiring not just a comprehensive remedy but a wholesale change in the level of care of the information industry. Just as the mass-production economy precipitated a wave of reforms in consumer protection (in part thanks to a kick-start by author Upton Sinclair), so too must the mass-information economy adapt. After demonstrating the parallels between the problems of today with those of yesterday, this Note will propose parallel solutions, particularly a consolidation of regulatory power and a new tort for breach of information privacy, which draws its inspiration from general products liability. These proposals show that rather than reinvent the wheel, modern lawmakers can (and should) answer today's problems with lessons from the last century.

[*] J.D. Expected May 2009, University of Virginia School of Law. In preparing this Note, I cannot say enough about the assistance of Professor James Gibson, whose ability to weave together arguments and examples across disciplines left me truly inspired, and without whose careful critique I could not have produced this final work. I also owe a great debt to Professor Karan Moran, whose mentorship and feedback on this Note went far above the call of her duties. Finally, I owe special thanks to Professors Elizabeth Magill and Christopher Sprigman, as well as the extraordinary editors of the *Virginia Law Review*, all of whom provided new perspectives and critical guidance through the process. Any errors in this Note are entirely my own.

INTRODUCTION

At the turn of the twentieth century, Americans had no idea what they were eating. Before then—that is, before mass production—consumers bought food products from local markets, where they knew and could rely on the reputation of sellers, who both created and sold the food themselves.[1] Local merchants were seen as trustworthy, and, for the most part, there was little to hide. But at the turn of the century, factories and warehouses became home to all sorts of businesses, and the distance between the birth of the product and the store shelf stretched further and further.[2] Behind the curtain, producers were eliminating quality control, cutting wages, ignoring worker safety, and generally engaging in a race to the bottom.[3] But in the store, consumers only saw well-packaged, well-marketed food seemingly fit for a king, products whose careful presentation betrayed nothing of their humble origins.[4]

The curtain came down in 1906, however, when Upton Sinclair published *The Jungle*, a vivid and startling account of the conditions inside Chicago's slaughterhouses.[5] Sinclair had set out to highlight the plight of the slaughterhouse worker, but, as it turned out, Americans were much more interested in the plight of the meat.[6] Sinclair described in detail the stacks of meat left to rot in open rooms where rats, alive and dead, found their way into just about everything, and subsequently the just-about-everything found its way into the can and onto the store shelf. The public lost its appetite, and Congress hurried to the rescue with the Federal

[1] William A. Lovett, State Deceptive Trade Practice Legislation, 46 Tul. L. Rev. 724, 727 (1972).

[2] Id. at 728.

[3] See Jeremy S. Sosin, Note, The Price of Killing a Child: Is the Fair Labor Standards Act Strong Enough to Protect Children in Today's Workplace?, 31 Val. U. L. Rev. 1181, 1187–88 (1997).

[4] See Escola v. Coca Cola Bottling Co., 150 P.2d 436, 443 (Cal. 1944) (Traynor, J., concurring) ("The consumer no longer has means or skill enough to investigate for himself the soundness of a product, even when it is not contained in a sealed package, and his erstwhile vigilance has been lulled by the steady efforts of manufacturers to build up confidence by advertising and marketing devices such as trade-marks.").

[5] See Upton Sinclair, The Jungle 21 (1906).

[6] Sinclair lamented the fact that his work did little to change the conditions for factory workers, his true goal in publishing *The Jungle*. "I aimed at the public's heart," he would later write, "and by accident I hit it in the stomach." Upton Sinclair, What Life Means to Me, Cosmopolitan Mag., Oct. 1906, at 591, 594.

Meat Inspection Act of 1906.[7] Seemingly by accident, Sinclair had triggered the birth of consumer protection, an extensive body of law and policy that would shape the nation's industrial growth.

The last one hundred years have shown a stunning expansion in the area of consumer protection law. What began with meat continued with regulation of all sorts of industries, from food to pharmaceuticals[8] and from toys[9] to cars.[10] Regulatory agencies—most notably the Federal Trade Commission—formed to handle the complex world of product control, and at its height, the law even recognized strict liability for product defects, though in time the law would shift to a more nuanced standard.[11] These developments—targeted regulation, agency oversight, and generalized products liability—did not happen overnight. Instead, the law evolved, benefitting from one hundred years of tension and debate that would shape the law into the body of precedents and theory we enjoy today.

The time has come for Upton Sinclair to rise again. Today, the new jungle is not an economy of industry but one of information, a place where telecommunications have changed the way services reach today's consumers in much the same way that the railroad changed the way goods reached consumers of the 1900s. Information is in many ways both the product and the currency of this new economy. Websites offer sophisticated services to consumers at no charge in exchange for a little, or sometimes a lot of, information. Consumer advocates have expressed concern about what happens with their information behind the curtain,[12] but, until recently, the

[7] Ch. 3913, 34 Stat. 674, amended by Pub. L. No. 90-201, 34 Stat. 1260 (1967) (codified at 21 U.S.C. §§ 601 et seq. (2000)).

[8] See, e.g., Federal Food and Drugs Act of 1906, Pub. L. No. 59-384, 24 Stat. 768 (codified at 21 U.S.C. §§ 1–15 (1934)) (repealed 1938).

[9] See, e.g., Child Protection and Toy Safety Act of 1969, Pub. L. No. 91-113, 83 Stat. 187 (codified at 30 U.S.C. §§ 1274 et seq. (2000)) (amending the Federal Hazardous Substances Act to protect children from hazardous toys).

[10] See generally Jerry L. Mashaw & David L. Harfst, Regulation and Legal Culture: The Case of Motor Vehicle Safety, 4 Yale J. on Reg. 257 (1987) (providing a history of the National Highway Traffic Safety Administration).

[11] See infra Section III.B.

[12] A number of organizations closely track online privacy issues, providing up-to-date information on developments in the media, market, and law. Some of the more prominent of these organizations include the Electronic Frontier Foundation (http://www.eff.org/issues/privacy), the Electronic Privacy Information Center

market seemed to support a comfort zone where consumers were willing to give up a bit of privacy for services or savings.[13] But this comfort zone, like that of the twentieth-century consumers who temporarily traded off quality control for low prices, is slowly evaporating.[14]

This Note will explore the coming crisis in the information economy. Part I will describe the basis for this crisis, including the growth of the "honest web," where consumers hand over their personal information to third parties to store, aggregate, analyze, and present back to the consumer in an interesting or useful way without protection against release of their information into the ether. Part II will explore the negative consequences of this trend, such as the growth of identity theft. As these problems fester, the law will need to step in to correct what the market cannot, or else the resulting friction may slow development of this billion-dollar industry.[15] Part III will compare the growing pains of the information economy to those of the industrial economy, showing how consumers in both eras faced analogous circumstances and, thus far, have reacted in analogous ways. By taking a step back to analyze both economies in the abstract, it becomes apparent that the true success of consumer protection law came in exploiting synergies in the law rather than through a disconnected patchwork of legal tools. Specifically, consumer protection used regulatory and tort law in complementary ways, such as by promulgating best practices and using tort law to incentivize their adoption. These same strategies have a place in the information economy as well, and while some progress has been made, much ground remains uncovered. Therefore, in addition to offering suggestions on how the regulatory regime should change, Part IV will devote special attention to

(http://epic.org/), the Privacy Rights Clearinghouse (http://www.privacyrights.org/), and the Privacy Coalition (http://privacycoalition.org/).

[13] See infra Part II.

[14] See infra Part III.

[15] See Simson Garfinkel, Database Nation: The Death of Privacy in the 21st Century 164–68 (2000) (describing data-collection giant Experian, a $1.5 billion company, as just one example of the growth of the information business). In 2007, funding for collaborative web-based applications grew to $1.34 billion. U.S. Web 2.0 Investment Jumps 88% in 2007 to $1.34 Billion But Sector May Be Maturing, Dow Jones VentureSource, Mar. 18, 2008, http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/03-18-2008/0004775881.

a proposal for generalized liability in tort for breach of information privacy. This proposal draws on a century of experience by analogizing liability for breach of information privacy to that for design defects. Such a law will require careful balancing of interests, but more importantly it will require complimentary features in the regulatory scheme to achieve its full potential.

By recognizing the parallels between the development of today's economy with that of the industrial age, the law can be proactive, identifying and avoiding the problems that will only grow worse with time. Otherwise, Congress may be left to react only after another trip inside the slaughterhouse.

I. UNDERSTANDING THE INFORMATION ECONOMY

A. Framework of Information Collection

In the modern economy, information is a product, a component, and a currency. Collectors of information come in different shapes and sizes, and the risks to the consumer vary greatly depending on the motives for collection. Although there are several ways to frame the mechanics of information collection, this Note proposes a benefits-oriented framework, where what matters is not who does the collecting, but who has the most to gain when the information is honest. While no transaction of information would exist if it were not, on some level, favorable to both sides, the suppliers of information—the people we think of as traditional "consumers"—are more willing to hand over sensitive information when they feel their benefits are tied to their honesty. From this premise, one can generate three basic categories of transactions: information collection for the benefit of the collector (for example, collection for marketing purposes), information collection for the benefit of the giver (for example, using an online calendar to enhance one's productivity), and information collection for the benefit of "many" (for example, posting a file online to share with friends or coworkers).

By examining consumers' incentives to be forthcoming in each of these models, one can better understand the varying features and dangers associated with the information economy.

1. Information Collection for the Benefit of the Collector

Savvy consumers are aware that when they use a frequent-shopper card in a grocery store, the store silently tracks their purchases and uses the information for a variety of purposes, from targeting advertisements to general market research.[16] In exchange for allowing Big Brother to know how many green peppers we purchased today, we enjoy the benefits of slight discounts on our selections.[17] And the advertisements we deal with every day—whether on our receipts, in our mail, on websites, or among the hundreds of other commercial exposures we receive—increasingly share some connection to our interests. This form of information collection certainly creates benefits for the consumer, but honesty better serves the collector that aggregates and analyzes the information in hopes of drawing useful conclusions about its target audience.

On the Internet, advertisers can take these techniques to a new level. For example, if a visitor searches Google for the term "cell phone," the page with search results will include advertisements for cell phones. However, the marketing continues even after the user leaves the search page. Because search companies like Google also operate extensive advertising businesses, they control advertisements on millions of other webpages.[18] When the same user navigates to one of these webpages—say, a website for a discount electronics store—the page accesses a cookie[19] on the user's com-

[16] See Elizabeth D. De Armond, Frothy Chaos: Modern Data Warehousing and Old-Fashioned Defamation, 41 Val. U. L. Rev. 1061, 1073–74 (2007).

[17] Even this seemingly innocuous data can reveal intimate details. In 2005, a security hole on a website for CVS Corporation employees allowed easy access to the purchases of millions of customers at CVS drugstores, including potentially embarrassing items such as condoms and home pregnancy kits. Take Extra Care in Sharing this Card, St. Petersburg Times, June 22, 2005, at 3D. It should be noted that the collector of information may also gain by selling the information to another party who can make use of the data. When this happens, a user's privacy may be put at greater risk by exposing user information even further. Additionally, when more entities have access to sensitive information, the risk becomes higher that one of those entities may have a breach of security that will leak the information into the public domain.

[18] Perfect 10 v. Google, Inc., 416 F. Supp. 2d 828, 847 (C.D. Cal. 2006) (noting that one of Google's advertising programs generated $630 million in gross revenue in 2005); Ryan Blitstein, Search Engine Buys the House Where Founders Got Their Start, San Jose Mercury News, Oct. 3, 2006.

[19] In the wired world, cookies are simply small chunks of data placed on a user's computer by a website to assist in tracking the user. For more informa-

puter that allows Google to identify the user as the same one who recently searched for "cell phone" through its search engine. Google can then supply advertisements for the webpage related to cell phones, hoping to tempt the user with targeted ads.[20] But companies like Google can take this advertising even further by updating their records to note that the same user that searched for "cell phone" earlier in the day also showed interest in a discount electronics store, so the next time the advertising engine "sees" the user, it may offer cell phone ads geared toward a low-income audience.[21] Because such a system requires that information about the user be collected, tracked, and stored for a significant period of time, this activity, which began as a seemingly benign data collection process, can trigger legitimate privacy concerns.[22]

Of the three models, this form of information collection generally causes the least harm to the consumer, but the risks can nonetheless become quite substantial. The dangers from this type of information gathering come in three forms. First, a great deal of information is generally gathered without the knowledge of the user. Simply by visiting a webpage, users often expose their internet protocol ("IP") address,[23] their internet service provider,[24] their

tion on cookies, see Adam L. Penenberg, Cookie Monsters, Slate, Nov. 7, 2005, http://www.slate.com/id/2129656/.

[20] For a discussion of how cookies enhance the process of targeted advertising, particularly when combined with knowledge of a user's search terms, see David Greising & John McCormick, Users Can Search, But They Can't Hide, Chi. Trib., Dec. 24, 2006, at 1; see also Andrew Brown, They Know All About You, Guardian, Aug. 28, 2006, at G2.

[21] In 2001, DoubleClick, the then-largest provider of internet advertising services, successfully defended a class action under a variety of statutes alleging that its advertisements improperly collected information about web-surfers by tracking the user's movements on a webpage. In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 500 (S.D.N.Y. 2001). *DoubleClick* demonstrates that information collection alone rarely becomes unlawful, and thus companies continue to find ways to combine and expand their collections. Perhaps no company knows this better than Google, which fought off privacy complaints to acquire DoubleClick in 2007. Louise Story, U.S. Clears DoubleClick-Google Merger, Int'l Herald Trib., Dec. 22, 2007, at 15.

[22] Ellen Nakashima, Some Web Firms Say They Track Behavior Without Explicit Consent, Wash. Post, Aug. 12, 2008, at D1.

[23] An IP address is a unique address that identifies devices on the Internet. The address generally cannot be used to directly identify individuals without help from an internet service provider, but with other information, an IP address can be used to narrow the search dramatically. See William McGeveran, Note, Programmed Privacy Promises: P3P and Web Privacy Law, 76 N.Y.U. L. Rev. 1812, 1819 n.37 (2001); Ctr.

most-recently viewed webpage,[25] their choice of web browser,[26] and many other facts about their computing environment.[27] Second, the sheer volume of "innocuous" information obtained about users by well-integrated advertisers can push the limits of personal comfort.[28] Finally, the current technology allows advertisements to act as miniature applications that not only display a message but can talk back to their home servers about what the user is doing on the particular page.[29] For example, a dynamic advertisement resting on a webpage can watch as a user fills out a form on the page even when the form involves such sensitive data as financial or health information. Effectively, in today's online world, ads have eyes.

Consumers, however, do have some ways of limiting their exposure. The critical theme in applications that fall within this category is that consumers have little incentive to be forthcoming with the information collectors in the first place. In many cases, consumers can disable cookies on their browser, leave blank any optional fields on web forms, and lie when asked for such information as an email or home address—all without significantly diminishing the benefit they receive. These actions by skeptical consumers have the effect of limiting the risk that any breach of privacy will have serious consequences, since less information shared means less information at risk.

Furthermore, both the collectors and suppliers of personal information stand to gain in the information economy, even with these risks. Without marketing value, many services now available for free to consumers would not exist. Google, for example, which provides free email, calendar, document sharing, and other services

for Democracy & Tech., Getting Started: Online Tracking FAQ, CDT's Guide to Online Privacy, http://www.cdt.org/privacy/guide/start/track.html (last visited Sept. 20, 2008).

[24] Ctr. for Democracy & Tech, supra note 23.

[25] Id.

[26] Id.

[27] Id.

[28] See, e.g., In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 503–04 (S.D.N.Y. 2001) ("DoubleClick's cookies collect 'information . . . such as names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the Internet, Web pages or sites visited on the Internet and other communications and information that users would not ordinarily expect advertisers to be able to collect.'").

[29] Id. at 504.

to millions of consumers, generates ninety-nine percent of its revenue from advertising.[30] It is not surprising perhaps that, despite the risks of privacy breach, consumers flock to these services in droves.

Regardless of consumers' apparent comfort with these types of information transactions, the risks of data breach are hardly hypothetical. In August 2006, America Online found itself in the headlines when a file was discovered on its research website that contained the search queries of roughly 600,000 subscribers.[31] Though the file did not link the queries with users' names, it did link them with a unique user identification number, which was enough for reporters from the *New York Times* to track down a few of the subscribers themselves.[32] In addition to providing enough information to identify the subscribers, the file also suggested personal information that one could reasonably connect with the subscriber's life. For instance, one subscriber's search queries included "'texas laws on retirement plans,' 'legal separation,' and 'is a restraining order needed during a divorce,'" which taken together would reasonably suggest that the subscriber was contemplating ending a marriage.[33]

2. Information Collection for the Benefit of the Giver

Unlike the first model of information collection, information collection for the benefit of the giver does not suffer from a lack of incentives to disclose private information. In fact, under this second class of services, consumers have every reason to believe that they will see greater benefits if they put more information on the table. Generally speaking, these services work by collecting information from users, processing it, and presenting it *back* to users in a manner that is more useful. For example, users of an online calendar hand over day-to-day details of their lives, and in return, the web-

[30] Google Announces First Quarter 2008 Results, Google Investor Relations, Apr. 17, 2008, http://investor.google.com/releases/2008Q1.html.

[31] Karim Z. Oussayef, Note, Selective Privacy: Facilitating Market-Based Solutions to Data Breaches by Standardizing Internet Privacy Policies, 14 B.U. J. Sci. & Tech. L. 104, 104–06 (2008) (citing Michael Arrington, AOL Proudly Releases Massive Amount of Private Data, TechCrunch, Aug 6, 2006, http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data).

[32] See Michael Barbaro & Tom Zeller Jr., A Face Is Exposed for AOL Searcher No. 4417749, N.Y. Times, Aug. 9, 2006, at A1.

[33] Oussayef, supra note 31, at 106.

site provides them a pleasant and efficient interface for their schedule.[34] If consumers provide inaccurate or incomplete information, they only hurt themselves. When companies provide such services as email and file storage, they often compete over who can offer users' the most space to store their digital lives.[35]

Even traditional ("offline") services rely on this model of incentives. Doctors and lawyers who request information from their clients do so because the services they provide depend on the accuracy and completeness of that information. The law has long recognized that individuals who speak to these professionals are generally truthful, and public policy protects and fosters those incentives.[36] As these services move online, the information once contained in locked file cabinets suddenly becomes much more vulnerable.

3. Information Collection for the Benefit of "Many"

A third class of information-hungry services exists almost entirely because of recent developments in technology. In the early years of the Internet, websites generally offered content to users in a one-way direction. Users could read the webpages but not manipulate them, absorbing content but not creating it.[37] But after the dot-com bubble burst, businesses began to form that focused on offering consumers more of a collaborative experience. Users could themselves contribute, manipulate, share, and otherwise interact with websites in ways typically thought of as happening offline with computer software. This trend, often referred to as "Web 2.0," rec-

[34] Certainly the service providers have plenty to gain in these transactions as well, particularly by placing advertisements on their websites. These complications can have some effect on users' comfort, such as when consumers discovered that Google was analyzing their email to provide targeted advertisements. See infra note 35 and accompanying text. But, in the end, consumers probably tolerate this sort of action as a price of admission. See id.

[35] For example, Google's email service, Gmail, has a counter that displays the storage capacity for any individual email account, but the counter increases every second of every day. Posting of Rob Siemborski to The Official Gmail Blog, http://gmailblog.blogspot.com/2007/10/more-gmail-storage-coming-for-all.html (Oct. 12, 2007, 1:05 EST).

[36] See, e.g., Fed. R. Evid. 803(4) (excepting from the evidentiary ban on hearsay statements made by a patient to a doctor).

[37] See Tim O'Reilly, What Is Web 2.0, O'Reilly Media, Sept. 30, 2005, http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

ognized websites as "applications."[38] Some of these sites simply offer users new ways to interact with their own data, such as a website offering file storage, but others build on the Internet's inherent connectivity to deliver powerful applications using hundreds or thousands of users.

One extraordinary example of the Web 2.0 framework is Wikipedia, the online encyclopedia where visitors can edit and contribute content to almost any article.[39] The site contains more than ten million pages in 260 languages, with thousands of articles uploaded daily.[40] Since Wikipedia stores little if any private information about its "authors," and its content is intended for an unfiltered audience, the site is generally benign when it comes to data privacy.[41] On the other hand, a host of other collaborative tools take in massive amounts of data intended only for a limited group of trusted individuals. For example, Google's document-sharing system allows users to upload, edit, and share documents online.[42] On today's web, people can and do share private documents, photos, and other files with a few simple clicks of a mouse. So long as the data does not become available to people outside of the user's intended audience, these sites offer a wealth of benefits that would have been much less robust—and much more expensive—a few years earlier.

Social networking sites, such as MySpace and Facebook, further demonstrate the comfort users have in sharing personal information with an online service provider. Users of these sites join networks of friends, coworkers, or other groups, and they use the sites to share millions of stories, messages, photos, and other bits of personal information.[43] But unlike the last generation of social web-

[38] Id.

[39] See Wikipedia: About, http://en.wikipedia.org/wiki/Wikipedia:About (last visited Jan. 22, 2009).

[40] Id.

[41] See Wikimedia Found., Privacy Policy (April 2008), http://wikimediafoundation.org/wiki/Privacy_policy.

[42] See Basic Information: What Can I Do with Google Docs?, Google Docs Help, http://documents.google.com/support/bin/answer.py?answer=49008&topic=8613 (last visited Sept. 20, 2008) (listing features of "Google Docs," Google's free service for creating and sharing documents online).

[43] See, e.g., Facebook, http://www.facebook.com/ (last visited Sept. 14, 2008); see also Usha Munukutla-Parker, Unsolicited Commercial E-mail, Privacy Concerns Related To Social Network Services, Online Protection of Children, and Cyberbullying,

sites, these newcomers thrive on—and indeed, demand[44]—honesty from their patrons, and the public has been more than happy to oblige.[45] One might call this new movement the "honest web," a place where people no longer create pseudonyms or act out fantasies, but instead, where they share their true selves, albeit in small doses, with the world. By choosing who can access this information, consumers generally feel comfortable handing it over, trusting that the website will enforce their privacy interests.

But Facebook's power as an aggregator of information can also raise privacy red flags. When Facebook first rolled out the "mini-feed," a feature that shows new or updated content from friends, the company drew fire from thousands of subscribers for lacking a clear opt-out feature.[46] Ironically, Facebook was criticized for making it easier to do exactly what users were already doing on their own: using Facebook to explore the personal lives of friends. For example, on a subscriber's profile, which is generally viewable to "friends" on Facebook, a subscriber can indicate his or her relationship status. Assuming a user does not opt out of the mini-feed feature, Facebook will publish changes in the individual's relationship status on the mini-feed for all of that individual's friends. For instance, if subscriber John Doe's relationship status was set to "in a relationship with Jane Smith," and John changes his status to "single," then his friends will see an alert on their mini-feed informing them that "John Doe is no longer in a relationship with Jane Smith." Of course, a diligent user who had access to John's profile could discover this change as well, but by aggregating and analyzing the information so efficiently, Facebook's mini-feed made users feel vulnerable. Because social networking sites foster discussion of social (and thus sometimes less-than-professional) ac-

2 I/S J. L. Pol'y for Info. Soc'y 627, 634 (2006); Thomas K. Arnold, The MySpace Invaders, USA Today, Aug. 1, 2006, at 4D.

[44] Facebook's terms of service, for example, require registrants to provide "accurate, current and complete information." Facebook, Terms of Use (June 7, 2008), http://www.facebook.com/terms.php.

[45] Facebook now counts over 110 million users. See Statistics, Facebook Press Room, http://www.facebook.com/press/info.php?statistics (last visited Oct. 29, 2008).

[46] Mark Zuckerberg, Facebook's founder, published an open letter apologizing for the mishandling of the "news feed" and "mini-feed" services soon after they were released. Posting of Mark Zuckerberg to The Facebook Blog, http://blog.facebook.com/blog.php?post=2208562130 (Sept. 8, 2006, 2:48 EST).

tivities, the sites create real dangers that the details of an individual's private life will reach an unintended audience.

4. Hybrid Models

Of course, the three classes of information services discussed above do not exist in a vacuum. In reality, many service providers find ways to incorporate as many aspects of these models as possible, allowing them to capitalize on the benefits they can accrue from making the most of the precious information commodity. For example, when Web 2.0 applications resort to advertising to make a profit, they tend to use any and all information at their fingertips. This can be troubling because the users of the website generally volunteered significantly more information to these sorts of websites than they did when they were simply surfing static, content-driven webpages. For example, Google's email service, Gmail, posts advertisements on the side of the application when reading email.[47] Google selects these ads based on the content of the email being viewed, meaning that Google's servers are not merely storing email but are, in a sense, "reading" it.[48] Email a friend a question about tort law, and do not be surprised when Google places advertisements next to that email listing local attorneys for hire. And when services band together, such as when a user hands Google control over email, calendar, documents, and photos, the volume of data available on that single user is simply mind boggling.

B. The Benefits of Open Information

Generally speaking, more information is a good thing. Users of social networks like being able to expect that the information found on the profiles of those in their networks is accurate, not only for general enjoyment, but also because the information tends to have real-world value. For instance, social networking sites generally make it easy to find a friend's phone number in a pinch, remember a birthday, or make business connections. Honesty also

[47] David Greising & John McCormick, Users Can Search, But They Can't Hide, Chi. Trib., Dec. 24, 2006, at 1; see also Tim O'Reilly, The Fuss About Gmail and Privacy: Nine Reasons Why It's Bogus, O'Reilly Media, Apr. 16, 2004, http://www.oreillynet.com/pub/wlg/4707.

[48] O'Reilly, supra note 47.

allows people to engage in "collaborative filtering," which allows a service that aggregates data to recommend choices to a given user based on what other similarly situated users have chosen themselves. For example, Netflix, an online and by-mail movie rental company, allows users to rate movies they have seen and then recommends new movies to users based on the similarities in the ratings.[49] For instance, if I like *Gone with the Wind*, and most people who like *Gone with the Wind* also like *Casablanca*, there is a good chance I will like *Casablanca* as well.[50] This not only benefits users by providing tailored recommendations, but it also means that producers of goods that lack the reputation or marketing prowess of other companies can still reach target users, since they can ride the coattails of more well-known products.[51] The more information that is available for the collaborative filtering system, the more likely it will be that the recommendations steer the user in a positive direction.

An "honest web" also allows for more accurate price discrimination. If a seller could access a consumer's "digital life," the seller might learn enough about the person to tailor a price to the buyer for a particular good. Although some consumers might not appreciate having to pay more than they might have otherwise, price discrimination eliminates economists' dreaded "deadweight loss," allowing the market—albeit the producers—to capture profits that previously vanished into thin air.[52] Additionally, price discrimination allows more buyers to enter the market, since the seller can authorize a special price just for low-demand buyers that may be below market price.[53] While at first glance, this may seem like an unlikely scenario due to the possibility of arbitrage, experience suggests that sellers could find innovative ways to offer different prices to different individuals without collapsing the market onto the lowest price. On social networking sites, sellers could have dif-

[49] Mike Musgrove, Waiting for Netflix's Plot to Advance, Wash. Post, Oct. 28, 2007, at F1.

[50] See id. (describing Netflix's collaborative rating system).

[51] Id.

[52] For an economic analysis of these principles, see William W. Fisher III, Property and Contract on the Internet, 73 Chi. Kent L. Rev. 1203, 1234–40 (1998) (noting that price discrimination can expand output, enhance consumer welfare, and reduce deadweight loss).

[53] Id. at 1239.

ferent banner ads that appear on different profiles, where the content of the ad—in particular, the price of the good or service being offered—would depend on certain factors in the profile. Users would not easily realize that their offer might be better or worse than the offer made to other users, and instead, they may simply accept.

These benefits are generally worth protecting and nurturing in the information economy.[54] Online applications that collect, analyze, and present information in a useful way contribute utility to our lives and create opportunities for transactions that would not occur otherwise.

II. THE LOOMING CRISIS IN PRIVACY

Information services have a dark side, however. As the cloud of private information about consumers continues to build, each breach of security becomes more significant than the last. This Part explores the escalating dangers of information sharing and collection in today's economy, followed by an analysis of why the market cannot and will not be able to heal itself.

A. Escalating Dangers from Breach of Privacy

Unfortunately, the very forces responsible for driving the information economy are also responsible for creating substantial dangers for consumers. As this Section shows, while modern consumers enjoy greater services at lower prices, they do not (and indeed, cannot) observe defects in a company's privacy protections, and those who gain access to a consumer's private information have the potential to wreak havoc. If trends continue, these dangers may overtake consumers much faster than the law can evolve to protect them.

1. Information Leak

Today's generation of internet-savvy consumers is accustomed to hearing the advice that anything posted on the Internet stays

[54] Cf. Michael J. Meurer, Copyright Law and Price Discrimination, 23 Cardozo L. Rev. 55, 96–97 (2001) (arguing that, in the market for copyrighted works, the excessive profits that come with price discrimination may decrease incentives to create).

forever. Nevertheless, many ignore this warning for a variety of reasons, not the least of which may be the shear difficulty of staying on-guard in all online communications when no other medium enjoys such dominance in our lives. Understandably, consumers simply want to share and use the Internet without worrying about the relatively remote risk that their embarrassing information may become public.

But the concerns are all too real, and as the information economy develops new ways to organize itself, security holes become easier to identify, exploit, and publicize. Since 2005, security breaches exposed more than two hundred million records containing personal and identifying information.[55] Breaches that expose such sensitive data as private health records certainly garner headlines,[56] but even exposure of "social" data, such as private pictures, can transform a website from an ordinary recreational tool into a public broadcasting system.[57] In March 2008, a security lapse made it possible for clever users to gain access to pictures of anyone on Facebook, even where the owners of the content had classified the pictures as private.[58] When a Canadian technician exposed the weakness, users were able to see pictures of Facebook's billionaire founder Mark Zuckerberg and pop-culture icon Paris Hilton, all of which were intended to be kept within each user's network of trusted friends.[59] MySpace, an older and larger competitor to Facebook, also suffered a similar security breach less than a year earlier.[60] These types of breaches affect personal privacy in its purest

[55] Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Sept. 14, 2008). The confirmed number of "records containing sensitive personal information involved in security breaches in the U.S." stood at 244,803,916 records as of September 14, 2008. Id. The total number of security breaches is much higher, but this figure only includes "breaches that expose individuals to identity theft as well as breaches that qualify for disclosure under state laws." Id.

[56] See, e.g., Brenda Goodman, Georgia Patients' Records Exposed on Web for Weeks, N.Y. Times, Apr. 11, 2008, at A19.

[57] Note that the Privacy Rights Clearinghouse's 200 million data breaches since 2005, see supra note 55, does not include mere exposure of social data such as photographs. The figure only includes exposures of the kind of data that leaves users vulnerable to identity theft. Id.

[58] Michael Liedtke, Security Lapse Exposes Facebook Photos, Assoc. Press, Mar. 24, 2008, http://www.msnbc.msn.com/id/23785561.

[59] Id.

[60] Id.

form. Simply allowing private information to enter the public domain causes a loss of privacy and autonomy, regardless of whether the information is exploited for criminal purposes.

2. Identify Theft

Of course, when criminals do take hold of personal information, the harm that can result affects not only an individual's stability, but the economy's as well. Identity theft occurs when someone acquires and uses identifying information, such as a person's name, social security number, or credit card number to commit fraud or other crimes.[61] In 2007, losses from internet-based crimes reached an all-time high of nearly $240 million.[62] Just about any exposure of private data can contribute to identify theft, even when no financial data is revealed, because criminals can use seemingly innocuous information to develop more sophisticated and more personalized "phishing" scams, where a consumer is induced to hand over sensitive information such as bank account numbers or passwords by appearing to be a service provider the user trusts, making identity theft possible.[63] As consumers continue to pour out their digital lives online, criminals will have more to work with when attempting to imitate an individual for personal gain.

3. Background Checks and Discrimination

Even non-financial information can be dangerous in the wrong hands. Employers seeking to know as much as possible about job candidates have been using the Internet as a research tool for years. One survey found that seventeen percent of employers use social networking sites as a part of their recruitment effort, and nearly half of those will also use the sites to check candidates' profiles.[64] Another survey found that sixty-three percent of employers

[61] Fed. Trade Comm'n, About Identity Theft, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (last visited Sept. 14, 2008).

[62] Internet Crime Complaint Ctr., Fed. Bureau of Investigation, Reported Dollar Loss from Internet Crime Reaches All Time High, Apr. 3, 2008, http://www.ic3.gov/media/2008/080403.htm.

[63] Simone Baribeau, Your Bank in Your Pocket, Wash. Post, Sep. 14, 2008, at F1.

[64] Social Networking Sites Gaining Popularity Among Employers Seeking Job Candidates, JobWeb, Mar. 7, 2008, http://www.jobweb.com/jobmarketnews.aspx?id=1693

who use such websites to review candidates have made rejections based on the information they found.[65] The information economy thrives on making more information available in less time, meaning that in the future, employers will find it even easier to review the highlights of a candidate's "social" resume for hiring. As this awareness of social networking grows in the future, employers might even require access to an individual's social network; after all, companies have a very real interest in ensuring employees do not post confidential information or embarrass the company's reputation. In an age where some employers require regular drug testing[66] and others openly admit to monitoring all internet communication at work,[67] companies who demand access to employees' "social data" may create the next wave of worker-privacy litigation.

Access to social data could also allow an employer to discriminate based on factors that might otherwise be invisible on a candidate's resume or in an interview. While an employee would never see such questions on a job application, a Facebook profile includes optional entries for gender, religious views, political views, and marital status, while the photo portion of the profile would tend to show a candidate's race. Employers who had access to this type of data could make adverse employment decisions without giving away the basis for their decision, allowing for a backdoor to discrimination.[68]

(describing the Job Outlook 2008 report by the National Association of Colleges and Employers).

[65] See Donald Carrington Davis, MySpace Isn't Your Space: Expanding the Fair Credit Reporting Act to Ensure Accountability and Fairness in Employer Searches of Online Social Networking Services, 16 Kan. J.L. & Pub. Pol'y 237, 239 (2007); see also Alan Finder, When a Risqué Online Persona Undermines a Chance for a Job, N.Y. Times, June 11, 2006, at A1.

[66] See, e.g., Aaron C. Schepler, Note, *Hart v. Seven Resorts, Inc.*: Should the Arizona Constitution Protect Employees from Employer-Mandated Drug Testing?, 30 Ariz. St. L.J. 541, 541 (1998).

[67] See Am. Mgmt. Assoc., 2007 Electronic Monitoring & Surveillance Survey, Feb. 28, 2008, http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey (summarizing results of a survey conducted by the American Management Association and the ePolicy Institute concluding that half of all employers fire workers for email and internet abuses).

[68] See Davis, supra note 65, at 243–45.

4. "Offline" Data Security

While much of this discussion revolves around information traded on the Internet, even data collected and stored "offline" has the potential to fall into the wrong hands. In this age of mobility, companies routinely allow their employees to access and store sensitive data about consumers on laptops, disks, and mobile phones, which can then become lost or stolen.[69] In fact, nearly twenty percent of all reported cases of data breach originated with lost or stolen storage devices, according to a study by Identity Theft Resource Center in San Diego.[70] Given these trends, the law of the information economy must be flexible enough to satisfy the concerns of data that is offline, as well as online.

B. Why the Market Cannot Heal Itself

The problems that have faced the information economy until now have been a burden, but not an unbearable one. However, that tide is set to turn. A combination of factors—namely, limited consumer competence, lack of disclosure, and a new technological trend—may set the stage for a perfect storm, an information market failure that will require a new wave of legal reform. Rather than wait for Upton Sinclair to rise again, today's analysts should take a careful look at these developments now and consider what the economy needs to stay on course.

1. Limits on Consumer Competence

In the information economy, it can be difficult to know whom to trust. The modern information age has seen a transition from service providers that have a physical, real-world presence with those that have only a cyber-storefront. This virtualization of business stripped away information that provided a kind of proxy for evaluating service providers. For example, a service provider owning a large office downtown might be seen as more reputable than one

[69] See, e.g., Valerie Kalfrin, Monitor Your Bank Account, HCC Employees Warned, Tampa Trib., July 25, 2008, at 3; Matthew Taylor, Private Data on Armed Forces Goes Missing, Guardian, Oct. 11, 2008, at 11.

[70] Brian Krebs, Data Breaches Are Up 69% This Year, Nonprofit Says, Wash. Post, July 1, 2008, at D3.

operating out of his basement.[71] The Internet obscures this signaling information in the same way that mass-production wiped away evidence of how a good was produced. As a result, consumers in the information age cannot easily know whether the service being offered online will be of high quality.

Despite the loss of this important signaling information, and despite the privacy implications of granting a company such extraordinary access to our data, individuals have been increasingly comfortable supplying this information to third parties.[72] The problem, however, is that no matter which reason users have for handing over the keys to their digital kingdoms, nearly all users lack the capacity to appreciate the choice being made. Today's consumers, much like the early twentieth-century consumers who placed too much faith in mass-producers,[73] simply do not (and cannot) fully understand their risk exposure.

In general, three reasons may justify a user's decision to hand over otherwise private information. First, today's consumers may believe the information they supply online will not be released to anyone they do not trust. The origins of this belief, if consumers indeed possess it, are not entirely clear. Despite the fact that nearly every significant website posts a privacy policy, the average user never reads it.[74] Instead, consumers frequently rely on the reputation of the company as a signal for the quality of data security, while others may simply use other proxies, such as the "look and feel" of the website to determine if it "seems" trustworthy.[75] Even if these approaches were sound, which they generally are not,[76] us-

[71] See Bruce L. Benson, The Spontaneous Evolution of Cyber Law: Norms, Property Rights, Contracting, Dispute Resolution and Enforcement Without the State, 1 J.L. Econ. & Pol'y 269, 281 (2005) (noting that rational consumers view "[i]nvestments in . . . non-salvageable assets [like] elaborate store fronts" as a sign of credibility).

[72] See Louise Story, To Aim Ads, Web Is Keeping Closer Eye on What You Click, N.Y. Times, Mar. 10, 2008, at A1 (noting that despite the risks, consumers have not yet complained "to any great extent" about data collection online).

[73] See Lovett, supra note 1, at 727–28.

[74] Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age 82 (2004).

[75] Cf. James P. Nehf, Incomparability and the Passive Virtues of Ad Hoc Privacy Policy, 76 U. Colo. L. Rev. 1, 23 (2005) (discussing the weaknesses of current signaling mechanisms in the world of information privacy).

[76] Id.

ers cannot actually see how the website works from a technical perspective to verify that the website is using appropriate standards for data security.

Second, consumers may simply believe that the information they provide does not reveal personal details—when in fact it does. The grand collectors of information in the modern world know exactly how to "mine," or analyze, data to make some extraordinary conclusions about individuals' behavior.[77] Many users do not even realize just how deep their data goes; for example, they likely forget that a thorough analysis of a calendar could reveal a person's recreational activities, hobbies, favorite restaurants, dating history, medical information (by tracking location, doctor's name, and frequency of appointments), and other matters generally thought to be private and personal.[78] If before signing up for an online calendar, a user had to explicitly provide the site with answers to questions about these matters, most users would surely balk at the request. The fact that users are comfortable when a computer algorithm produces roughly the same result cannot be explained without acknowledging at least some degree of misunderstanding by the user about the risks involved.

Finally, and most optimistically, consumers may choose to hand over personal information because, while they recognize the risks of exposure, they believe the risk is worth the value of the service. The problem with this view is that consumers in the mass-information age, like their ancestors in the mass-production age, have no practical means of inspecting or evaluating the quality of the supply chain. Even if they were so aware, average consumers lack the expertise to decide whether the security measures being taken to safeguard their information are sufficient. When consumers decide that the benefits are worth the risks, their conclusions may not be a reflection of the market finding a point of stability at all, particularly when network effects make sites like Google

[77] See John Battelle, The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture 6 (2005).

[78] Since the information collection happens seamlessly—often invisibly—most users do not realize the depth of the data collection. "'When you start to get into the details, it's scarier than you might suspect," suggested Marc Rotenberg, executive director of the Electronic Privacy Information Center. "We're recording preferences, hopes, worries and fears." Story, supra note 21, at A1.

Documents or Facebook so enticing. These externalities—which draw consumers into the market for reasons unrelated to quality of service—put pressure on consumers to join, share, and expose their data, even if an independent analysis of the risks might counsel otherwise.

Some have argued that third parties and watchdog groups could instill more competence in consumers with what essentially amount to seals of approval.[79] For example, nonprofit TRUSTe[80] provides a certification service whereby companies that meet specific standards for security can proudly hang an approved badge of honor, the idea being that consumers will look for such seals and know their data is safe.[81] But because companies adopt these seals voluntarily,[82] it is unclear how the market would suddenly come to expect—or demand—such seals before trusting the company. Indeed, at the start of 2007, the majority of the web's top ten sites did not have such seals,[83] and a year later, TRUSTe still only boasts 3440 participating websites.[84]

In general, the problems in consumer competence come down to information asymmetry. To make matters worse, even when consumers recognize their own limitations, the result will likely be detrimental for the market. That is, if consumers believe they have all the information and they are mistaken, their decisions will be poorly made. If they recognize their own limitations and become more cautious, they may choose not to participate in certain market transactions that were actually quite safe because they feared their own ignorance. In either case, the market suffers.

[79] Avner Ben-Ner & Louis Putterman, Trusting and Trustworthiness, 81 B.U. L. Rev. 523, 543–44 (2001) (discussing the growth of VeriSign as an "Internet trust service"); see also Oussayef, supra note 31, at 129–30 (suggesting that market pressure might one day encourage companies to adopt standardized privacy policies as a prerequisite for obtaining a consumer privacy seal).

[80] TRUSTe is an independent non-profit organization specializing in privacy seals and compliance. For more on standards-oriented privacy watchdogs, see generally Major R. Ken Pippin, Consumer Privacy on the Internet: It's "Surfer Beware," 47 A.F. L. Rev. 125 (1999).

[81] Ben-Ner & Putterman, supra note 79, at 543–44.

[82] Oussayef, supra note 31, at 128.

[83] Id.

[84] TRUSTe Fact Sheet, http://www.truste.org/about/fact_sheet.php (last visited Jan. 22, 2009) (describing fiscal year 2008).

2. Lack of Disclosure

While faults in consumer competence may lead some to be too trusting with their data ex ante, problems in disclosure of data breach can prevent consumers from minimizing losses after a breach occurs. Victims of data breach can mitigate their losses in a variety of ways, such as by taking down information from unsecured websites,[85] monitoring their credit reports for unusual activity, or notifying financial institutions of possible compromise. But the consumer who knows nothing can do nothing. Just as consumer protection law developed to correct these deficiencies, privacy law will need to do the same.

One might wonder whether the modern economy's greatest asset—its knack for rapid information sharing—provides the answer to these challenges. That is, since the information economy is so good at aggregating and analyzing data, privacy breaches themselves could theoretically be tracked, analyzed, and publicized fast enough to aid consumers in making appropriate choices about whom to trust. This idea has some merit, and indeed, the market has made headway in certain contexts, such as the use of feedback ratings for sellers on eBay's well-known auction site.[86] But, two problems inhibit the information economy from sorting out its own defects in this manner.

First, most security breaches go unnoticed and unreported.[87] Businesses are understandably hesitant to voluntarily expose themselves to liability or negative publicity,[88] and the law lacks a comprehensive or uniform standard for when service providers must

[85] This strategy would help minimize the extent to which third parties can obtain an individual's personal information, but it is only viable when the defect is one that exposes, rather than actively transmits, the information.

[86] Luís Cabral & Ali Hortaçsu, The Dynamics of Seller Reputation: Theory and Evidence from eBay 1–2 (Nat'l Bureau of Econ. Research, Working Paper No. 10363, 2004); see also Clayton P. Gillette, Reputation and Intermediaries in Electronic Commerce, 62 La. L. Rev. 1165, 1177–80 (2002) (discussing eBay's rating system for sellers in greater depth).

[87] See Posting of Jeanne Friedman to RSA Conference Blog, https://365.rsaconference.com/blogs/rsa_conference_blog/2008/08/05/rsa-conference-survey-reveals-that-more-than-89-of-security-incidents-went-unreported-in-2007;jsessionid=02FD81E7F4245206B22AE5B3316C4951 (Aug. 5, 2008, 16:38 EST) (describing a survey finding that more than 89% of security incidents went unreported in 2007).

[88] Kathryn E. Picanso, Note, Protecting Information Security Under a Uniform Data Breach Notification Law, 75 Fordham L. Rev. 355, 360–61 (2006).

disclose breaches of privacy.[89] Even when the media does pick up on security breaches, such as in the Facebook-photo snafu described above,[90] there is no guarantee that such news will reach the average consumer.

Second, ratings systems that work for online sellers of products would not easily transfer to service providers. Services, unlike goods, are rarely fungible, making it difficult to conduct a side-by-side comparison of service providers. Because of this difficulty in making direct, quantifiable comparisons, sites like Pricegrabber[91] and Google Product Search,[92] which aggregate information about products being sold on the web to allow quick comparison, cannot easily adjust their algorithms to analyze providers of services the way they analyze sellers of goods.[93] Additionally, while it seems obvious that consumers who participate in rating systems for product sellers would use such metrics as whether the good arrived on time and in good condition, it is not nearly so obvious how a consumer would factor privacy-protection into a rating of a service provider. This problem is only compounded by the fact that most consumers do not even know when their privacy has been breached.[94]

[89] See id. at 368–70 (discussing the development of breach-notification laws at the state and federal level). The general tort for privacy invasion, see Restatement (Second) of Torts §§ 652A–I (1977), also has failed to gain uniform acceptance or interpretation. See generally Frank J. Cavico, Invasion of Privacy in the Private Employment Sector: Tortious and Ethical Aspects, 30 Hous. L. Rev. 1263 (1993) (discussing various features of tort liability for invasion of privacy, including the lack of unified approaches).

[90] See supra note 58–59 and accompanying text.

[91] See PriceGrabber.com, http://www.pricegrabber.com (last visited Jan. 25, 2009).

[92] See Google Product Search, http://www.froogle.com (last visited Jan. 25, 2009).

[93] A computer that aggregates information about fungible products sold can easily provide a comparison of these products based on such obvious metrics as price, warranty, size, and a host of other standard specifications. Sellers of identical products can similarly be rated based on a few standard metrics as well, such as the number of days the seller takes to ship goods, the percentage of goods sold that never make it to the consumer, and the number of goods sold that arrive in a defective condition. Although sellers will always try to distinguish themselves with other features, ratings based on these metrics are still highly relevant. But services, unlike products, often cannot be compared directly. Some services are popular because of their user experience, while others rely on a web of useful features. In a field where the goalposts are constantly shifting, algorithms cannot offer the kind of discrimination that they can for sellers of fungible products.

[94] See supra notes 79–85 and accompanying text.

3. The Role of Technology

In addition to problems of consumer capacity and lack of disclosure, the market itself is beginning to show signs of technological developments that, in addition to bringing convenience and additional power to information-driven services, will also make consumers significantly more vulnerable. In particular, the market has recently seen a high demand for technologies that allow unrelated and unaffiliated websites to share data and services. For example, a web-based mapping service and a hotel-reservation website can combine their "knowledge" to produce a visually appealing map of available hotels in a given area.[95] Before Web 2.0,[96] such a partnership would have required negotiation between the two companies, but now, many websites have created application program interfaces ("APIs")[97] that allow anyone to connect and use their services in new and imaginative ways.[98] The results of this melding of services, which are generally known as "mash-ups,"[99] provide additional usefulness for consumers, but they also require opening more channels for information between sites that previously had nothing in common. As a consequence of these back-door channels, users on the front end cannot be sure that the information moving back and forth is not of a sensitive nature.

Facebook's "Beacon" feature may signal the first steps down this dangerous path. The goal of this new technology is to track and publish information about the items Facebook members buy on third-party websites.[100] For example, when a Facebook user buys a book on Overstock.com, the purchase is reported as an "alert" on friends' mini-feeds, the same "feed" that tells users when friends

[95] Google has encouraged "mash-ups," particularly through use of its mapping program. See Jefferson Graham, Google's Worldwide Developer Day Places Emphasis on 'Mash-ups', USA Today, May 30, 2007, at 4B.

[96] See supra notes 37–38 and accompanying text.

[97] "By providing a means for requesting program services, an API is said to grant access to or open an application. Building an application with no APIs . . . is basically like building a house with no doors." David Orenstein, Application Programming Interface, Computerworld, Jan. 10, 2000, at 66 (quotations omitted).

[98] For more on the increasing deployment of APIs, see Damon Darlin, A Journey to a Thousand Maps Begins with an Open Code, N.Y. Times, Oct. 20, 2005, at C9.

[99] Id.

[100] See Maria Aspan, How Sticky Is Membership on Facebook? Just Try Breaking Free, N.Y. Times, Feb. 11, 2008, at C1.

upload new pictures or change their status.[101] From Facebook's perspective, the program allows companies to turn consumers into advertisers. Facebook hoped users would appreciate the chance to see what products their friends were buying, and initially, Facebook did not offer a clear opt-out for its members.[102] The backlash was substantial. More than 50,000 Facebook users signed an online petition demanding a clear opt-out, and Facebook redesigned the system with such features in mind.[103]

Although Beacon has had a rocky start, Facebook probably has the right vision of the future. By coupling social data with online-purchase information, companies gain a powerful tool for reaching consumers and analyzing their behavior. But without regulation requiring disclosure of how unprotected information can be shared when these gateways are opened, users are once again left in the dark about how service providers will use their private information.

As powerful as technologies like APIs are for allowing two companies to share services, the system still requires that an outsider wishing to access another site's data write special software code to bridge the gap. From a practical standpoint, this limits the number of sites that can share data, since both creating an API and accessing one requires an investment of time and energy. But these barriers to information sharing may be coming down even further as the market moves toward industry-wide standards for sharing data where "interoperability" may be the buzzword for the next generation of online services. Indeed, this movement is well underway. Software and internet giants like Yahoo! and Google have joined in the "OpenSocial initiative," which aims to standardize the way computers store "social data," such as contacts, photos, messages, stories, and other personal information.[104] These standards, once adopted, would allow companies to pass information much more

[101] See Vauhini Vara, It's Hard to Hide from Your 'Friends', Wall St. J., Jan. 30, 2008, at D1.

[102] Id.

[103] See Aspan, supra note 100.

[104] Jessica E. Vascellaro, Yahoo Endorses Social Networks, Wall St. J., Mar. 26, 2008, at B7. One new technological standard is Attention Profiling Mark-up Language, or APML, which would allow integration of information from a variety of sources, from email accounts to social networking profiles. See APML: Attention Profiling Mark-up Language, http://www.apml.org (last visited Sept. 20, 2008).

efficiently by relying on a single standard of communication. These technologies, which are still in their infancy, are sometimes pitched as making user data more "portable."[105] These innovations have clear benefits for the market, but as data becomes easier to move, it also becomes harder to protect.

III. LOOKING BACK FOR TOMORROW'S SOLUTIONS

The market ailments of the new economy will not heal themselves. No matter how careful users are, it seems that only internet abstinence can guarantee consumers' privacy. Of course, not only is such advice unlikely to be followed, but the entire point of the information economy is that sharing of information is good for business—meaning good for companies and good for consumers. To ensure a prosperous future, the new economy needs the right balance of incentives for sellers to keep data well protected, something only law and policy can provide. As this Part suggests, the solutions to tomorrow's problems may be best found in the last century.

A. Parallel Problems

Although the twenty-first century enjoys a new, high-tech cast of characters, the themes and plot twists are remarkably similar to those of the twentieth century. The failures of the modern market discussed in-depth earlier—namely consumer incompetence,[106] lack of disclosure,[107] and technological complications[108]—are as much a burden today as they were during industrial expansion.

1. Limits on Consumer Competence

First, consider how the industrial economy suffered from a virtualization of business like that which has occurred in today's world,

[105] See Thomas Claburn, Give Them What They Want, InformationWeek, Feb. 13, 2006, at 55 (discussing data portability as the future of online business). Data portability creates complex questions of data ownership, particularly since most websites requires users to agree that the data belongs not to the user, but to the website owner. For more on data portability, see Josh Quittner, Who Owns Your Address Book?, Fortune, Feb. 18, 2008, at 32.

[106] See supra Subsection II.B.1.

[107] See supra Subsection II.B.2.

[108] See supra Subsection II.B.3.

where businesses have increasingly transitioned from a physical identity to an internet-only presence.[109] In the days of Upton Sinclair, consumers bought goods at the end of a production chain without having the opportunity to inspect or evaluate the process,[110] and under the doctrine of *caveat emptor*, producers lacked incentives to change their ways.[111] Accordingly, sellers learned that the faster and cheaper the goods could get to the market, the better chance the producer had of making a profit.[112] Unlike the pre-urbanization years, when consumers bought products from local farmers and family businesses, industrial consumers dealt with large, faceless companies, and it was typically anyone's guess about whether a new product would turn out to be a lemon.[113] In essence, the mass-market economy stripped away some information—namely a local reputation—that consumers could use to make decisions about producers. The old adage of "buyer beware" left industrial consumers irrevocably uninformed about sellers[114] in much the same way that modern consumers must engage online service providers at their own risk.[115]

2. Lack of Disclosure

Next, consider how sellers in the industrial economy, like those in today's world, lacked the incentives to disclose product defects. Consumer protection law recognized early on that manufacturers,

[109] See supra Subsection II.B.1 (discussing in greater depth the virtualization of business in the modern economy and its effect on consumer competence).

[110] See Escola v. Coca Cola Bottling Co., 150 P.2d 436, 443 (Cal. 1944) (Traynor, J., concurring) ("The consumer no longer has means or skills enough to investigate for himself the soundness of a product . . . .").

[111] See Foley v. Clark Equip. Co., 523 A.2d 379, 386–87 (Pa. Super. Ct. 1987) (discussing developments of the industrial age as they relate to the background of strict products liability).

[112] See id. (noting that as the products of the industrial economy grew in complexity, society turned its attention from fostering manufacturing to protecting consumers).

[113] To combat this trend, some producers worked to cultivate personifications, such as General Mills's invention of Betty Crocker, a fictitious persona intended to convey a "warm and friendly" feeling in the minds of consumers. See Ctr. for History & News Media, George Mason Univ., Who Was Betty Crocker?, http://chnm.gmu.edu/features/sidelights/crocker.html (last visited Sept. 20, 2008).

[114] See *Foley*, 523 A.2d at 386 ("The Nineteenth Century principle of caveat emptor was replaced in the Twentieth Century by the notion that it was the consumer who should be protected.").

[115] See supra Subsection II.B.1.

not consumers, were in the best position to gather and disseminate information about products.[116] This lack of incentives was particularly troubling because consumers had no opportunity to minimize their injury from defective products, something they might easily do if notified of the risks after purchasing the products. For example, the owner of a defective saw might dispose of the good or take precautions to cure the defect. Just as today's consumers who are not aware of a security breach are denied the opportunity to mitigate their losses,[117] industrial consumers who purchased products could not expect a recall if their products turned out to be dangerous.

3. The Role of Technology

Finally, technology had as much impact on consumer burdens in the industrial age as it has today.[118] In the last century, industrialization made products—as well as the manufacturing process itself—more complex, making it more difficult for the consumer to make informed choices in the marketplace.[119] Advancements in assembly lines and mass production certainly stimulated the market, but they also exacerbated its flaws. What was an itch became a rash, and lawmakers responded with a wave of reforms for consumer protection.[120] Today's market may need a similar prescription.

B. Parallel Solutions

Given how similar today's problems are to the problems of the industrial economy, lawmakers should take a step back and—rather than reinvent the wheel for information privacy—recognize

[116] Robert A. Van Kirk, The Evolution of Useful Life Statutes in the Products Liability Reform Effort, 1989 Duke L.J. 1689, 1695, 1737.

[117] See supra Subsection II.B.2.

[118] For the role of technology in the modern economy, see supra Subsection II.B.3.

[119] McCormack v. Hankscraft Co., 154 N.W.2d 488, 500 (Minn. 1967) ("[E]nlarging a manufacturer's liability to those injured by its products more adequately meets public-policy demands to protect consumers from the inevitable risks of bodily harm created by mass production and complex marketing conditions.").

[120] Azzarello v. Black Brothers Co., 391 A.2d 1020, 1023 (Pa. 1978) ("The development of a sophisticated and complex industrial society with its proliferation of new products and vast changes in the private enterprise system has inspired a change in legal philosophy from the principle of caveat emptor . . . .").

that the same solutions that worked for the industrial economy can provide guidance for the information age as well.

Consumer protection law has evolved into a complex web of regulation, but a few trends have emerged. Chronologically speaking, the first developments came in the form of targeted regulation for certain areas of industry. After Sinclair's exposé on the meatpacking industry, Congress reacted with lightning speed by passing the Federal Meat Inspection Act of 1906.[121] Over the next fifty years, Congress would continue to pass laws tailored to specific products, including food, drugs, and motor vehicles.[122] These laws recognized the special dangers involved with certain areas of industry and treated those sectors differently.[123] In time, Congress vested greater power in federal agencies like the Federal Trade Commission, Food and Drug Administration, and Consumer Product Safety Commission.[124] These agencies have developed special expertise in various areas of the industry, and they use their investigatory and regulatory powers to promote best practices.

These laws were not left to operate in a vacuum, however. Complementing this regulatory regime was a marked change in the tort system as well: the development of strict products liability. This change in tort liability helped pick up where agencies left off by filling gaps in producers' incentives. Justice Traynor expressed the argument for strict products liability succinctly in *Greenman v. Yuba Power Products, Inc*.[125] First, Justice Traynor noted that the responsibility for injuries from defective products should fall on the shoulders of whatever entity is in the best position to prevent the

[121] See supra note 7 and accompanying text.

[122] See Pure Food and Drug Act of 1906, ch. 3915, 34 Stat. 768 (1906) (repealed 1938); Federal Food, Drug, and Cosmetic Act, ch. 675, § 1, 52 Stat. 1040 (1938) (codified as amended at 21 U.S.C. §§ 301–399 (1938)); National Traffic and Motor Vehicle Safety Act, Pub. L. No. 89-563, 80 Stat. 718 (1966) (codified as amended at 49 U.S.C. §§ 30101–30170 (1966)).

[123] See also Timothy D. Zick, Note, Reporting Substantial Product Safety Hazards Under the Consumer Product Safety Act: The Products Liability Interface, 80 Geo. L.J. 387, 387 n.3 (1991) (discussing Congress's reactions to specific hazards in the market, such as flammable fabrics and potential poisons).

[124] Ronald Chen & Jon Hanson, The Illusion of Law: The Legitimating Schemas of Modern Policy and Corporate Law, 103 Mich. L. Rev. 1, 54 (2004) (noting the importance of these agencies in protecting consumers by testing products, requiring certain disclosures, mandating recalls, and imposing fines for regulatory violations).

[125] 377 P.2d 898, 901 (Cal. 1962).

defects from reaching the market.[126] Certainly, producers are better equipped to prevent defects in the factories than consumers are to detect them on the shelves. Second, the law should allow for costs arising from such liability to spread across the economy, which producers can accomplish through internalization.[127] By factoring cost of liability for injuries into costs of production, the suppliers pass on the costs to consumers as price increases, which translates into slightly lower demand; instead of a few consumers bearing their own losses, the industry as a whole absorbs the financial hit. Third, consumers are in a weak position to show that a manufacturer failed to exercise due care or to identify the cause of a product's defects.[128] In the end, proponents of strict liability aim to increase the average level of care and decrease the extent to which consumers absorb their own losses for injuries by shifting costs of injuries back to the producers themselves.[129]

Originally, courts held fast to a standard of strict liability, but with time, they began to draw more forgiving lines in certain contexts. In particular, courts interpreting the law of defective design[130] waffled for some time between two different tests, one relying on consumer expectations and the other on balancing of risks and utility, before finally tipping toward the risk-utility balancing test.[131]

---

[126] See Angela C. Rushton, Comment, Design Defects Under the Restatement (Third) of Torts: A Reassessment of Strict Liability and the Goals of a Functional Approach, 45 Emory L.J. 389, 395 (1996).

[127] See id.

[128] See id. "In many cases manufacturing defects are in fact caused by manufacturer negligence but plaintiffs have difficulty proving it. Strict liability therefore performs a function similar to the concept of res ipsa loquitur, allowing deserving plaintiffs to succeed notwithstanding what would otherwise be difficult or insuperable problems of proof." Restatement (Third) of Torts: Products Liability, § 2 cmt. a (1998).

[129] Guido Calabresi & Jon T. Hirschoff, Toward a Test for Strict Liability in Torts, 81 Yale L.J. 1055, 1060–67 (1972); John Riper, Note, Strict Liability in Hybrid Cases, 32 Stan. L. Rev. 391, 393–94 (1980).

[130] For a discussion of the differences between manufacturing defects and defective design, see *Barker v. Lull Eng'g Co.*, 573 P.2d 443, 454 (Cal. 1978) ("[A] defective product is one that differs from the manufacturer's intended result or from other ostensibly identical units of the same product line. . . . A design defect, by contrast, cannot be identified simply by comparing the injury-producing product with the manufacturer's plans or with other units of the same product line, since by definition the plans and all such units will reflect the same design.").

[131] See, e.g., David G. Owen, Risk-Utility Balancing in Design Defect Cases, 30 U. Mich. J.L. Reform 239, 242–43 (1997); see also Kim D. Larsen, Note, Strict Products Liability and the Risk-Utility Test for Design Defect: An Economic Analysis, 84

The risk-utility balancing test, which broadly asks whether, on balance, the benefits of the challenged design outweigh the risk of danger inherent in such design,[132] is in effect an ordinary negligence calculus[133] with greater articulation about what "reasonableness" means in the market for goods.[134] Specifically, the Restatement suggests that a product "is defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design . . . and the omission of the alternative design renders the product not reasonably safe."[135] This standard recognizes that imposition of liability should have a policy purpose; pure strict liability might prevent products from reaching the market that cannot be made perfectly safe and yet nonetheless have important value in the market.[136]

Despite many functional similarities to ordinary negligence, the law regarding design defects does build in a number of consumer-friendly features. Under the Restatement, the factfinder may infer the existence of a defect if the alleged harm is the sort that usually results from a defect and was not "solely the result of causes other than product defect existing at the time of sale or distribution."[137] Additionally, a product's design is automatically defective if it fails to comply with a relevant statute or administrative regulation, though mere regulatory compliance will not necessarily render a

Colum. L. Rev. 2045, 2046 (1984) (recognizing that risk-utility has generally overtaken the consumer-expectations test in design defect cases).

[132] *Barker*, 573 P.2d at 456.

[133] Cf. United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947) (Hand, J.) (offering the well-known $B<PL$ calculation for determining negligence, where the burden on the producer is B, probability of injury is P, and the extent of injury is L).

[134] The risk-utility balancing test generally rests on the following considerations:

> (1) the product's utility to the public as a whole, (2) its utility to the individual user, (3) the likelihood that the product will cause injury, (4) the availability of a safer design, (5) the possibility of designing and manufacturing the product so that it is safer but remains functional and reasonably priced, (6) the degree of awareness of the product's potential danger that can reasonably be attributed to the injured user, and (7) the manufacturer's ability to spread the cost of any safety-related design changes.

Denny v. Ford Motor Co., 662 N.E.2d 730, 735 (N.Y. 1995) (citation omitted).

[135] Restatement (Third) of Torts: Products Liability § 2(b) (1998).

[136] See, e.g., Howard Latin & Bobby Kasolas, Bad Designs, Lethal Profits: The Duty to Protect Other Motorists Against SUV Collision Risks, 82 B.U. L. Rev. 1161, 1168–69 (2002) (discussing this principle in the context of car manufacturers).

[137] Restatement (Third) of Torts: Products Liability § 3 & cmt. b. This presumption can occur in cases of manufacturing defects and design defects alike. Id.

product safe.[138] Lightening the burden of production in this manner can relieve consumers of some of the initial hurdles to bringing litigation.

C. Adapting Lessons of Consumer Protection to the Information Age

The true wisdom of consumer protection law is that it does not rely on a single legal tool to accomplish its goals, nor is it simply a disconnected patchwork of regulation. Instead, the regime enjoys certain synergies, such as allowing agencies to build up expertise and promulgate best practices, which then grow teeth in tort. The law can no doubt be chaotic, as would be expected from a large body of regulation that developed over an extended period of time, but as in any good process of evolution, the best features tend to survive. Generalizations about consumer protection law have value because they can guide lawmakers as the crisis in privacy festers across the information economy. The new economy will certainly undergo growing pains similar to those felt in the industrial economy, but by considering the broader legal picture, one can see how the law will need to evolve to meet the new demands of the wired world.

As a starting point, targeted regulation certainly has a place in the information economy, just as it did in the product market. Congress has already passed laws that protect "special" kinds of data, including information about children,[139] financial data,[140] and health records.[141] Congress is right to develop specialized areas of law for unusually sensitive information, much like products liability recognized products with special dangers, such as food and vehicles. A generally applicable legal standard for data privacy would fail to capture these special interests.

But targeted regulation alone cannot satisfy the needs of the budding information economy, much like product-specific regula-

[138] Id. § 4.

[139] See, e.g., Children's Online Privacy Protection Act of 1998 ("COPPA"), Pub. L. 105-277, 112 Stat. 2681-728 (codified at 15 U.S.C. §§ 6501–6506).

[140] See, e.g., Gramm-Leach-Bliley Act, Pub. L. No. 106-102, §§ 501–510, 113 Stat. 1338, 1436–45 (1999) (codified at 15 U.S.C. §§ 6801–6809).

[141] See, e.g., Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 42 U.S.C.).

tion fell short in the industrial age. The law of information privacy must rely on a thoughtful combination of regulation and tort reform that take advantage of synergies in the law rather than leaving tort reform or regulation to work independently. On the regulatory side, agencies need the opportunity to develop expertise in the oversight of information collection and storage, which can then allow them to promulgate an evolving set of best practices. Tort law should then provide consumers with opportunities to bring suits, likely in class action,[142] by establishing a new tort of data-breach liability that substantially parallels liability for design defects in goods.

Before discussing the details of the specific tort proposal,[143] consider the changes that must be made on the regulatory side. Currently, agency oversight of information privacy is haphazard at best, and much of the agency oversight relevant to transactions of information has been simply inherited from powers not specific to the information economy. For example, the Federal Trade Commission has the power to regulate deceptive trade practices that occur over the Internet,[144] while the Federal Communications Commission can regulate the business of internet service providers,[145] meaning either agency may have a say in regulating the business of information to the extent that their powers happen to touch on such areas. Instead, the regulatory regime should carve out clearer responsibilities for agencies, consolidating regulatory power to avoid this haphazard scattering of authority. Such consolidation would allow primary regulators to develop more comprehensive regulatory schemes. One positive example is the Health Insurance Portability and Accountability Act of 1996, which charges the De-

[142] One might reasonably assume that most data breaches will occur because of a design defect that affects a large group of users, rather than a single user, since computers generally treat all members of a particular class of objects in identical ways. If a computer has an error or defect in the management of a particular entity, it will likely have a similar problem in handling all similar entities.

[143] Because the tort proposal requires greater analysis, its discussion has been reserved for Part IV, infra.

[144] See Mark F. Foley, The FTC's Website Privacy and Security Rules for Every Business, Internet Bus. Law Serv., Nov. 19, 2007, http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1905.

[145] See, e.g., Cecilia Kang, Telecom Warily Waits on 'Wired' President, Wash. Post., Nov. 14, 2008, at D2; Stephen Labaton, F.C.C. Reshapes Rules Limiting Media Industry, N.Y. Times, Dec. 19, 2007, at A1.

partment of Health and Human Services with development of national standards for transacting health information.[146] Despite this hopeful start, in general, the law has yet to consolidate oversight of information collection and storage with specific agencies. Without this assignment, the patchwork of regulation will suffer from a lack of expertise and a host of inefficiencies.

This is not to say that one particular agency should be in charge of regulating all data collection in the new economy. Instead, the regulatory regime should recognize that certain kinds of information collection may require special oversight, just as certain kinds of products require special oversight from, for example, the Food and Drug Administration or National Highway Traffic Safety Administration, while another agency might have general oversight for products not specifically regulated by one of these specializing agencies. This latter type of agency oversight would parallel that of the Consumer Product Safety Commission, which broadly "protect[s] consumers and families from products that pose a fire, electrical, chemical, or mechanical hazard or can injure children."[147] This combination of focused and broad agency oversight works because all the agencies involved have relatively clear powers with regard to regulating products, unlike the current regulatory regime in the information economy.

By consolidating agency oversight, the law can take advantage of the expertise that develops over time, and these agencies can become hubs for disclosures of information about privacy breaches that occur. Most importantly, such agencies could also rely on the new tort law proposed here to give greater punch to their propaganda. Because the new tort law would be a significant undertaking for the new economy, such a proposal merits special attention.

IV. SPECIAL FOCUS: GENERAL TORT LIABILITY FOR BREACH OF INFORMATION PRIVACY

Although changes must occur in the present structure of agency powers and regulation, the lynchpin of the suggested framework is the new tort for general liability for breach of information privacy.

[146] Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033 (1996).

[147] U.S. Consumer Prod. Safety Comm'n, CPSC Overview, http://www.cpsc.gov/about/about.html (last visited Sept. 17, 2008).

Keeping in mind the lessons of general products liability, the drafting of this new tort need not start with a blank page. That said, the proposal must be tailored to the needs of the modern economy. With that in mind, the law should establish the following elements.

A. Tailoring Liability

1. Scope of Liability

Much like products liability, the premise of a tort for breach of information privacy is that the law should apply broadly to any seller in the relevant market. The scope of the tort, therefore, should cover any entity, whether corporate or individual, that provides goods or services and in the process digitally stores personal and identifying information. The breadth of this scope would ensure that all data collectors, regardless of the kind of information they collect, carefully consider the level of care to use when securing the data they store.

That said, applying such a law to traditional "pen-and-paper" companies would make the law over-inclusive. Indeed, three reasons support an exclusion for companies whose business primarily does not rely on digitally storing sensitive data. First, these companies inherently create less risk that any data breaches will cause great harm, since they do not primarily post information on the Internet or other broad media. Second, were the law to attach to traditional "pen-and-paper"-based companies, the law would essentially require Mom and Pop not only to learn how to use a computer but also to adopt rigorous technological standards. Even a site that has some internet presence, however small, has a much lighter burden in this regard, since the mere step of putting a business online generally requires either inherent technical expertise or the outsourcing of technical expertise, either of which would mean that the extra step of making the existing technical infrastructure more secure would be a relatively manageable increase in cost. Third, reference to telecommunication may provide a federal jurisdictional hook were this new tort to originate in Congress. Given these arguments, such an exclusion is probably warranted, though in time the exclusion might render itself functionally obsolete as all companies, regardless of technical expertise, recognize the benefits of an online presence.

It is important to note, however, that an exclusion for "pen-and-paper" companies must not create a loophole wide enough to excuse the "offline" data breach discussed earlier—namely that which occurs when a laptop containing sensitive data is lost or stolen.[148] Companies should not be allowed to escape liability when their lax security standards allow laptops containing vast unencrypted databases to fall into the wrong hands. As long as these companies store such sensitive information digitally, they have a responsibility to defend it.

Accordingly, the scope of liability suggested here covers any entity that digitally stores sensitive information as a regular part of its operation.

2. Standard of Liability

The point behind such a broad scope for the proposed tort is that the law ideally should raise the level of care for the industry, which requires that the entire industry have at least some share of liability under the statute. But this expansive scope must be narrowed to prevent the law from over-burdening the industry. That rationing should come from a carefully written standard of liability.

For the liability standard to raise the level of care, the standard must be low enough to make it relatively easy for consumers to bring claims, thus forcing service providers to internalize more of the costs of consumers' injuries. The law, however, must also not go too far, as a too-harsh standard would prevent service providers from entering the market out of fear of excessive liability.[149] Given the competing interests, the best standard would be one akin to the risk-utility balancing test, which, as discussed earlier,[150] asks whether, on balance, the benefits of the challenged design outweigh the risk of danger inherent in such design.[151] Paralleling the language for design defects,[152] the new tort might be drafted to trig-

[148] See supra Subsection II.A.4.

[149] In particular, the law will have to find a way to allow companies wishing to "beta test" their products—a common strategy for deploying and testing a service with real users—without undue exposure.

[150] See supra Section III.B.

[151] Barker v. Lull Eng'g Co., 573 P.2d 443, 456 (Cal. 1978).

[152] Cf. Restatement (Third) of Torts: Products Liability § 2(b) (1998) ("[A product] is defective in design when the foreseeable risks of harm posed by the product could

ger liability for a data breach "when the foreseeable risks of breach posed by the system's design could have been reduced or avoided by the adoption of a reasonable alternative design, the omission of which renders the design vulnerable to data breach." In the context of offline data, the "system's design" would include the technology used to store the digital information.

The risk-utility balancing test is appropriate for three reasons. First, the risk-utility test came into being in the context of design defects, where a product came off the assembly line exactly as the producer intended, but where that design itself rendered the product dangerous.[153] Likewise, most data breaches probably stem from weaknesses in the design of a security system rather than a fluke defect that occurred with a particular user or a particular data record.[154] Just as the law evolved to recognize that defects in a product's underlying design should be subject to this risk-utility balancing, the next-generation privacy tort should similarly adopt such a standard.

Second, putting aside the historical parallels, the practical purpose of the risk-utility balancing test is to eliminate claims where correction of the defect would have been so costly that the product might never have reached the market, in spite of its social utility.[155] This goal applies equally well to the market for information services. While data collectors should be responsible for securing the data they collect, the law must recognize, as cryptanalysts do, that

have been reduced or avoided by the adoption of a reasonable alternative design . . . and the omission of the alternative design renders the product not reasonably safe.").

[153] Contrast this with a manufacturing defect, where a product was designed safely, but errors in the production process, which may or may not have been preventable, caused defects in a small number of the products. See Restatement (Third) of Torts: Products Liability § 2 cmt. a (1998) (distinguishing design defects from manufacturing defects).

[154] This is a corollary to the fact that computer systems tend to treat a class of objects the same way. Computer programs deal with objects using mechanical functions and subroutines, which is why a "bug" in a computer system usually does not affect one user; it affects all users of the software. See generally Marc McDonald, Robert Musson & Ross Smith, The Practical Guide to Defect Prevention (2007); see also infra note 158 (describing the use of reusable portions of code in software development).

[155] See Restatement (Third) of Torts: Products Liability § 2 cmt. a (1998) ("A reasonably designed product still carries with it elements of risk that must be protected against by the user or consumer since some risks cannot be designed out of the product at reasonable cost.").

at some level any data center is vulnerable.[156] The goal of this new tort must be to increase the level of care, not to make entering the market so costly that the smallest service providers cannot get off the virtual ground. Just as products liability for design defects stops short of imposing liability that would prevent all socially-desirable (but inherently risky) goods, like pharmaceuticals, from reaching the market,[157] so too must the law of information privacy strike a balance between raising the level of care and stifling innovation.

The final reason for adopting the risk-utility-balancing test rests on the character of data-privacy technology. Retooling software does not require the investment costs associated with retooling an entire factory. That is, code is cheap; a service provider seeking to upgrade its security standards can do so at a much lower cost than would be required of a factory owner needing a similar physical upgrade.[158] Because of this fact, the burden on service providers to include security measures will generally be low,[159] which has the potential to generate greater liability under the risk-utility balancing test if such measures are ignored. This increase in liability exposure translates into a greater incentive to make upgrades. The effect on the level of care under the risk-utility test, therefore, may be substantial.

[156] See David Alan Jordan, Decrypting the Fourth Amendment: Warrantless NSA Surveillance and the Enhanced Expectation of Privacy Provided by Encrypted Voice over Internet Protocol, 47 B.C. L. Rev 505, 532 (2006) ("In theory, virtually all ciphers can be broken by 'brute force' or other cryptanalytic means.").

[157] Toner v. Lederle Labs., 732 P.2d 297, 306 (Idaho 1987) (relying on Restatement (Second) of Torts § 402A cmt. k).

[158] Further decreasing the cost to service providers is the fact that software programmers tend to rely on "libraries," or pre-fabricated software components, to build their applications. As industry standards develop for data security, these libraries will incorporate such standards, making it even easier to include—and in fact, difficult to avoid including—such protocols as they evolve. While industry standards would need to constantly shift in response to new threats, the market could also help make this process easier by encouraging software code to be written in such a way that the portions of the code dedicated to handling and storing private data can be isolated from other parts of the code. Upgrading to the newest security standards may then require only a simple download, rather than a retooling of the entire software package. See generally Ian T. Foster, Designing and Building Parallel Programs: Concepts and Tools for Parallel Software Engineering (1995).

[159] The costs to service providers will usually come in the form of a labor cost required for recoding certain portions of software, though hardware upgrades, which might be necessary, would be more expensive.

An example helps illustrate how these incentives play a role in urging websites to beef up security. In a "brute force" attack, a hacker writes a program that randomly tries to guess its way into users' online accounts by throwing passwords at the system until one of the passwords is accepted.[160] Two flaws in online forms often contribute to this vulnerability. First, computers (both the ones belonging to hackers and the ones belonging to the target website) are fast, meaning that in just a few milliseconds, a hacker's computer can submit a random password to the target website and get feedback on whether the password succeeded. As common sense would have it, the faster this exchange, the more chances a hacker has to get the password right. Second, the target computer cannot easily tell whether the "person" trying to sign in on the website is a human being or an enemy computer.[161] If the website could distinguish the two, it could make it more difficult for hackers to make rapid-fire login attempts.

In this war over users' privacy, sophisticated website designers have a number of defenses to these attacks. One option is simply to slow things down: when a user tries to log into a website, instead of returning an answer immediately, the site could wait two or three seconds.[162] This delay means little to a human user, but to a malicious software program, could make the difference between making millions of password attempts per day and only making a few thousand. Another option involves presenting the user a task that is simple for humans but difficult for computers—a good way to distinguish the real from the robotic. For instance, some websites ask users to stare at an image containing a word that has been twisted, stretched, or otherwise distorted and retype the word into the form.[163]

[160] Michael Miller, Is It Safe? Protecting Your Computer, Your Business, and Yourself Online 322 (2008).

[161] Id.

[162] For example, at the time of the writing of this Note, Paypal, an online payment service that processes millions of dollars in transactions every year, takes at least four seconds to process a username and password before letting on as to whether the combination was correct. Although Paypal does not advertise its security features, this unusually long delay suggests the incorporation of precisely this kind of intentional slow-down.

[163] Miller, supra note 160, at 325. This tool is generally known as a "CAPTCHA," an acronym for "Completely Automated Public Turing Test to Tell Computers and Humans Apart." See Sara Robinson, Human or Computer? Take This Test, N.Y. Times,

These defenses are well-known in the industry—so well known, in fact, that free resources exist giving away the code necessary to implement these safeguards.[164] But since most consumers have no idea this battle is even being waged, much less what a website has done to protect itself, the market may not create the incentives on its own to speed along adoption of these security measures. Consider a popular website called Twitter, a social networking and "micro-blogging" site where users share 140-character messages with each other.[165] The site boasts more than one million users, including Barack Obama, who used the site to distribute announcements to his supporters during the 2008 presidential campaign.[166] In January 2009, then-President-Elect Obama's twitter account—along with the accounts of pop star Britney Spears and CNN's Rick Sanchez—came under the control of an eighteen-year-old who exploited the fact that Twitter had allowed him to conduct rapid-fire logins.[167] In other words, even though these vulnerabilities are well known, and even though defenses are easy to implement, Twitter did not feel the need to do so—at least not until an exploitation of the flaw became public. The creators of such an enormously popular site should not wait until they draw negative headlines to plug such a basic security hole. A well-crafted standard of liability can correct this problem by providing the necessary incentives for implementing these safeguards.

3. Waivers of Liability

Finally, the law will need to prevent contract law from rendering the tort impotent by simply allowing consumers to waive such injuries. Consumer protection law incorporates limitations already, as

Dec. 10, 2002, at F1. For more on CAPTCHA, see The Official CAPTCHA Site, http://www.captcha.net/ (last visited Jan. 25, 2009).

[164] The Official CAPTCHA Site, supra note 163. Since hackers continually try to write software that can "read" the CAPTCHA images, thus defeating the tests, these CAPTCHA tests must be updated regularly. To make this process easier, the CAPTCHA founders created an application that website owners can use on their site that automatically updates itself to employ the latest form of CAPTCHA—for free.

[165] See Howard Kurtz, Political Coverage That's All a-Twitter: When Each Character Counts, the News Update Is Short and Tweet, Wash. Post., Aug. 26, 2008, at A19.

[166] Id.

[167] Andrew Ratner, In Social-Networking Pool, We Fall Hack, Line and Sinker for Phishers, Balt. Sun, Jan. 13, 2009, at 1C.

the law generally does not recognize waivers of personal injury from product defects.[168] While contract law should continue to allow parties in the modern economy to decide what information will be subject to protection and what may be subject to release to third parties, service providers must not be allowed to have their cake and eat it too by, on the one hand, telling consumers that they have a rigorous privacy policy but, on the other hand, requiring consumers to waive recovery of any injuries arising from data breach. If service providers want to escape liability entirely, they should (effectively) have to ask their users to agree to release their information to the world without limitation. If service providers promise not to disclose information without users' permission, they should not be able to disclaim damages.

B. Minimizing the Difficulty of Proof

1. Proving Damages

Of course, even if nominal liability did attach, the law might have little effect if consumers faced a steep uphill climb in proving the elements of their claims. As to damages, a victim of data exposure faces any range of harms. Identity theft certainly poses a direct threat on an individual whose personal information becomes publicly available. When identity theft occurs, it may take months to discover the problem, and during that time the individual may not have the credit necessary to get favorable terms on any number of transactions, from buying a home to paying off credit card debt. The resulting injuries not only entail wrangling with financial institutions and credit services, but many victims may feel inclined to pay for credit monitoring for several years on the off chance that a new perpetrator will discover and exploit their compromised data.[169]

But while identity theft often captures headlines, exposure of private information creates other risks and therefore other injuries. For example, consider an athlete whose compensation relies heavily on endorsements by significant sponsors and advertisers. Re-

[168] See, e.g., Note, Enforcing Waivers in Products Liability, 69 Va. L. Rev. 1111, 1114 (1983).

[169] See Kathy Kristof, How to Protect Your Identity, Newsday, Oct. 12, 2008, at F1 (discussing the purpose and value of credit-monitoring).

lease of private emails or photographs of the athlete in unsavory situations can quickly destroy such a celebrity's reputation, and with it, the individual's endorsements, potentially costing millions of dollars. Just as complex litigation might ride on a single embarrassing email, so too can information leaks destroy public careers and reputations when private information becomes exposed. But a person need not be a celebrity to feel the bite of public humiliation; it is not hard to imagine how a photograph or an email depicting an otherwise quiet employee in an unprofessional light can end a career. Similarly, a malicious person with access to another's social networking account could add negative content to that profile, content that might be seen by potential employers, among others. In today's world, such incidents are far from hypothetical.[170]

Some may point out that these injuries differ from injuries in the context of product safety, where lives, rather than careers or reputations, may be on the line. But in cases of data exposure, the actual harm to an individual can range anywhere from slight inconvenience or embarrassment to devastating financial loss. The loss of one's career, home, reputation, or social standing may not directly affect the victim's physical health, but the dollar value of these losses can still reach staggering proportions.[171]

As this discussion demonstrates, a plaintiff's injury in these cases might consist of general embarrassment stemming from the exposure of intimate personal information, lost wages from denial of a job due to disclosure of "social" data, or full-scale identify theft. The law should recognize that in some of these cases, proof of actual damages in these contexts may be quite difficult, which would suggest allowing all compensatory damages, including emotion damages and pain and suffering, be reachable through this tort. Of course, even if consumers' damages from breaches of privacy were low, the law might still be successful if it facilitated the organization of class action lawsuits, which would tend to make sellers in-

[170] For example, during Representative Nydia Velazquez's first campaign for Congress in 1992, her mental health records were leaked to a tabloid, revealing a previous suicide attempt and a battle with depression and drugs. Carol Jouzaitis, Americans Losing Medical Privacy, Chi. Trib., Dec. 31, 1995, at 3. The exposure forced her to defend her past to the media and the voters of New York's Twelfth District. Id.

[171] See supra notes 59–62 and accompanying text.

ternalize the costs of consumers' injuries even where the injuries were very small in individual cases.[172]

2. Proving Defect

In products liability, the law generally recognizes that it can be difficult for a consumer to prove that the harm in question was caused by a product defect.[173] Accordingly, the Restatement suggests that "[i]t may be inferred that the harm sustained by the plaintiff was caused by a product defect . . . when the incident that harmed the plaintiff . . . was of a kind that ordinarily occurs as a result of product defect."[174] In the data breach context, so long as a consumer can establish that a third party obtained the information from the defendant service provider, the burden should then shift to the defendant to show the lack of defect, which will generally require showing that the security methods used to prevent such disclosure were sufficiently reasonable to escape liability. While the user might be required to respond with technical evidence that suggests a reasonable alternative method for storing the data more securely, this system would allow plaintiffs to shift some of the litigation burdens to the service providers themselves, making it easier to make out prima facie claims.

C. Creating the Right Incentives

The true power of this new tort may come in the connections the law can make to the regulatory changes suggested earlier.[175] In particular, lawmakers should build into the law incentives for adopting best practices for data security as well as incentives for discovering and disclosing data breaches after they happen.

[172] While this analysis is useful for guiding development of the new law, an entire article could be devoted to the question of what damages should be allowed to best accomplish the goals of this new tort. This standard must be selected carefully so that it both facilitates plaintiffs seeking to bring claims but does not unduly shower the industry in litigation. For now, inclusion of compensatory damages without requiring proof of economic loss may be the best way to ensure recovery is possible for plaintiffs who suffer from the breach of privacy without turning every individual's suffering into a multi-million dollar lawsuit.

[173] See Restatement (Third) of Torts: Products Liability § 3 cmt. a (1998).

[174] Id. § 3.

[175] See supra Section III.C.

1. Adoption of Best Practices

Consumer protection law generally encourages the adoption of regulatory standards in products liability by rendering liability automatic when such standards have been ignored.[176] Under the Restatement, "noncompliance with an applicable product safety statute or administrative regulation renders the product defective with respect to the risks sought to be reduced by the statute or regulation."[177] A tort for breach of information privacy should similarly include a *per se* trigger for liability where service providers disregard regulations governing data storage. This feature of the law would allow the regulatory agency or agencies most responsible for such standards to help catalyze the adoption of such protocols.

2. Disclosure of Breaches

Legal combinations of tort and regulation can also correct the market's failure to incentivize disclosure of data breaches. The new tort can create these incentives in a number of ways. For example, a statute could set a cap on damages that only applies when the service provider discloses the breach before it is discovered by the consumer. Alternatively, the statute of limitations for the new tort could toll continuously until the consumer is notified of the breach. In either case, the service provider would be able to reduce their legal—and thus financial—exposure by disclosing the breach as quickly as possible. The regulatory regime should in turn complement tort law by using investigatory powers to seek out data breaches and acting as a hub for publicizing information about breaches to consumers. Consumer protection has long benefitted from such complementary legal approaches.[178]

D. Moving Forward

While a new tort for information privacy breach cannot be adopted overnight, the features discussed above are pivotal to en-

[176] See Restatement (Third) of Torts: Products Liability § 4(a) (1998).
[177] Id.
[178] See Restatement (Third) of Torts: Products Liability § 10 (1998) (triggering liability for post-sale failure to warn of a product defect).

suring that such a tort provides the right balance of protection and creates the most productive synergies with the regulatory changes proposed earlier.[179] A subsequent article might consider residual issues, such as affirmative defenses, statutes of limitation, and other questions about the manner of proof, but the framework suggested here for the new tort focuses on issues of central importance. As this discussion shows, the lessons of a century of evolution in products liability can help modern lawmakers extrapolate other areas of the new tort law without starting from scratch. More than a century of legal wisdom led to the innovative features we now enjoy in consumer protection law; it would be a mistake to ignore those advancements in the development of a new parallel tort in the area of information privacy.

CONCLUSION

While lawmakers and scholars have been reticent to venture too far into the area of information privacy, the source of this hesitation is not entirely clear. Perhaps in part the hesitation stems from the general criticism that cyberlaw is as useful as the "law of the horse."[180] Whatever merit this quip may or may not have when applied to amorphous concepts like "internet law," it does not apply to the proposals for regulatory and tort law of information privacy described in this Note. Information privacy is not about making a particular technology safe, like the Internet or computer-driven databases, nor is it about enforcing privacy policies on websites. These goals, while valid, are mere corollaries; the primary goal of developing the law of information privacy is to facilitate transactions of all kinds in the information age. The problem is not the technology itself; it is merely highlighted and exacerbated by technology. Therefore, technology-oriented solutions, while helpful, are transient stop-gaps on the road to true protection. If it is to be successful, the law for the information protection should focus on promoting safe transactions instead of simply regulating their me-

[179] See supra Section III.C.

[180] See Lawrence Lessig, Commentary, The Law of the Horse: What Cyberlaw Might Teach, 113 Harv. L. Rev. 501, 501 (1999) (responding to Judge Easterbrook's suggestion that the "law of cyberspace" is no more useful than the "law of the horse," since according to Easterbrook, cyberspace can be governed equally well by existing legal doctrines like contract or intellectual property).

dium. Viewing the proposals suggested here as "internet regulation" would fail to capture the interests of the market as a whole in resolving these issues, resulting in a legal myopia that will inhibit the development of solutions. The longer consumers have to wait for reform, the greater the losses to consumers, producers, and the economy.

Of course, the information economy does have a life of its own. With or without any help from lawmakers, the economy will continue to grow, offering new ways to collect and use personal information in ways that benefit all. But these benefits come at great cost to the consumer whose data is left unprotected, exposed, or stolen. Rather than leave the consumer in the dark, hoping that the market will eliminate its own sharp edges, the law should step in to provide a modest amount of child-proofing. Fundamental protections like consolidated agency oversight and general tort liability provide a balance of protections that will foster growth without hampering the flow of business. Without these safeguards, the market will continue to expand, but that growth will be stunted and scarred by years of privacy breaches and billions of dollars in identity theft.

In many ways, this new economy is much like the old one, and like its predecessor, it requires consumer protection. But thankfully, lawmakers need not start from square one; by recognizing the parallels in the problems between the information and industrial economies, we can develop more innovative solutions. If Upton Sinclair has taught us anything, it is that in an economy centered on providing more for less, "market pressure" cannot justify the sacrifice of quality control. And if consumer protection has taught us anything, it is that these market failures must be addressed on more than one front. Given enough time, a patchwork of legal responses to high-profile data breaches may well evolve into an effective legal framework that parallels many of the features of consumer protection law, but rather than leave the law to Darwin, the past century can be our guide to the next century, providing a valuable framework for evaluating and drafting laws that catalyze, rather than trivialize, the market for information. This framework can ensure protection comes to the market sooner, rather than later. At the current rate of legal reform, however, society may

simply have to pray that the Upton Sinclair of the next generation comes with a degree in computer science.