CONSUMER INFORMATION USE AND MISUSE IN ELECTRONIC BUSINESS: AN ALTERNATIVE TO PRIVACY REGULATION

Christopher M. Cassidy and Bongsug Chae

The U.S. government and commercial sector have opted to use privacy regulations to control the problem of consumer information misuse in the E-business environment. The authors argue that this is undesirable because it does not correct the market failure that causes this “information externality.” Using the Coase theorem, the authors propose that the market failure can be corrected using either property rules or liability rules and that liability rules at a federal level are likely to be most socially efficient. Recommendations for voluntary actions by industries and companies are also provided.

The future of electronic business heavily relies on consumers’ perception and trust regarding the handling of consumer information by online companies. Within the United States, privacy regulations are currently used to control the problem of consumer information misuse in an electronic business environment. This article argues that this is not desirable for either consumers or online companies. We present an approach to address this increasingly important issue for society, online companies, and individual consumers.


Yet, at the retail level, there appears to be a serious barrier for electronic business to attain its full potential. This barrier is consumers’ concern about personal information handling by firms in the electronic marketplace (Hemphill, 2002). Whereas the potential for harm is also a concern in the offline world, the importance of information handling is exaggerated in the online world. New E-business technologies have substantially increased the ability of online merchants to collect, monitor, target, profile, and even sell personal information about customers.

Christopher M. Cassidy is an assistant professor at Marshall University. His research interests are strategic management, corporate governance, and business ethics. His research has appeared in Advances in Strategic Management, Journal of Business Case Studies, and Information Ethics. He can be reached at cassidy@marshall.edu.

Bongsug Chae is an assistant professor at Kansas State University. His research interests are enterprise systems, knowledge management systems, and supply chain management. His research has appeared in Information Resource Management Journal and Journal of KMCI. He can be reached at bchae@ksu.edu.
These statistics indicate that consumers are attracted to the benefits of the online environment, but they worry about the potential for harm.

to third parties. The online environment also undermines a precondition necessary for commerce: trust. The pseudo-anonymity of the Internet, where people generally do not see, hear, or know the person with whom they transact, reduces the likelihood of successful legal remedies in the event of fraud or deception. Combining these factors with the number and prominence of media stories depicting online firms that have violated and worked against consumers’ interests and preferences — including Amazon, DoubleClick, RealNetworks, Toys R Us, America Online, etc. — people have the perception, if not the reality, that consumers need strong protection in the online environment.

A number of reports have documented that consumers are concerned about the security of their personal data in the electronic marketplace. The Global Online Retailing report by Ernst & Young (2001) indicates that for Web site visitors, personal information handling by Web sites is the major concern: “They want their history, behavior, and data protected.” According to Poulsen (2000), a survey by the American Express Company shows that nearly four out of five current and potential Internet users around the globe have security and privacy concerns. A 2005 survey by RSA Security found that 82.7 percent of respondents felt threatened by identity theft and 83.2 percent felt threatened by online fraud (PR Newswire, 2005). This type of concern makes consumers hesitant to give out credit card information online, or create a personal portal on a Web site. In addition, consumers increasingly distrust businesses’ ability to handle their personal information and are less confident about compliance with existing laws and professed organizational practices. A study by the Annenberg Public Policy Center of the University of Pennsylvania indicates that 95 percent of people using the Internet at home agreed “they should have the legal right to know everything” about the information Web sites collect from them (Annenberg, 2003).

One immediate, negative consequence of this mistrust is that consumers either decline to provide personal information or provide inaccurate information. One survey concluded that almost 95 percent of online users had declined to provide personal information to online sites (Hoffman & Novak, 1999). A survey report of AT&T Labs found that online users indicated they would be more likely to provide personal information if there were laws and policies in force (AT&T, 1999). This kind of mistrust represents a serious threat and business risk to the prosperity and financial success of any firm offering its products and/or services through e-business technologies. Customers suffer from unwanted and even wasteful advertising materials and potential harm caused by misuse and use of their information by companies. Concerns over personal information online appear to be a major barrier to the Internet economy. Despite these concerns, 80 percent of consumers desire personalized Internet content, according to a Choicestream survey (Kerner, 2005). These statistics indicate that consumers are attracted to the benefits of the online environment, but they worry about the potential for harm. The crucial question is how to balance the two.

“Privacy” is a hot topic in many countries’ political arenas (Rubin & Lenard, 2001). To date, U.S. society has focused on privacy solutions to problems related to consumer information. More than five years ago, a BusinessWeek/Harris poll found that 57 percent of Americans believe the government should pass privacy laws now restricting how personal information can be collected and used on the Internet (Garfinkel, 2000). Online privacy has been the subject of several major bills introduced in the U.S. Congress since 1999–2000, and the issue has remained important (EPIC, 2005). An emphasis on privacy issues in the online environment can be found in recent academic literature as well (e.g., Moores & Dhillon, 2003; Liu, Marchewka, Lu, & Yu, 2004). Yet despite governmental action and industry attention, the issue has not gone away.

We recognize that privacy is an issue embedded in the larger issue of how consumer information is used, and it is specifically related to the misuse of information. Information is a good with unique characteristics that make it unlike other tangible goods. The use of consumer information sometimes results in benefits that are unjustly transferred to entities other than the consumer, and also in harms that are unjustly transferred to the consumer. Society has chosen to deal with this transfer, described by economists as an externality, using a regulatory solution generally referred to as privacy.

Privacy is a regulatory approach to the use of information that legally restricts the collection, use, and dissemination of particular types of information. This approach prohibits any use or misuse that might result in huge costs for some consumers. In this article we argue that privacy, as with most regulatory approaches,
Privacy advocates argue that a consumer’s personal information can be used to inflict harm on that consumer.

Privacy, as it has been enacted in law, most resembles inalienable rights (Calabresi and Melamed, 1972) that impose protective behaviors on others. Inalienable rights are the strongest form of protection available to safeguard individuals. Unlike property rights, which are quite limited, inalienable rights cannot be exchanged or sold. An individual may choose to leave these rights unexercised; however, if the individual cannot disavow them. Familiar examples include the right to be free from governmental coercion in the realm of speech, assembly, and worship. Excessive police powers are reigned in by the right to due process, proscriptions against self-incrimination, and the right to be free from torture and other cruel or unusual punishments. Equal opportunity is predicated on the right to be free from discrimination based on sex, race, color, national origin, and religion. Calabresi and Melamed’s analysis suggests that inalienable rights are so strong that they should be used only when potential harms to individuals are significant and when alternative methods of protection are inadequate.

As with freedom of conscience and equal opportunity, an inalienable right to privacy would be justified if the following conditions exist: (1) the harms cannot be avoided, (2) the harms are severe, and (3) privacy rights are the only efficient method to reduce the harm.

What is frequently ignored in privacy discussions is that some injury is unavoidable when people interact through commerce (Calabresi and Melamed, 1972). Accidental disclosures of personal information will cause injury to some people. Unscrupulous people will attempt to defraud others by using their personal information. Even with the most intrusive of law enforcement, society cannot eliminate this harm entirely.

It must also be understood that restrictions on the use of consumer information in the form of privacy rights will prevent the beneficial uses as well as the harmful uses. There is an opportunity cost to society if privacy restrictions prevent the use of individual information to create benefits. Utilitarian thinking suggests that it would not be unethical for society to compare the costs and benefits of privacy with other alternatives and choose the option through some calculus that balances the needs of society with the need to protect individuals from harm (Mill, 1987; Velasquez, 1992; Baron, 2000; Steiner and Steiner, 2003).

Given the preceding discussion, it should be noted that harms can be reduced in number and magnitude when individuals exercise due care with respect to their own personal information. People can take preventative steps to minimize the harm from information misuse:

WHY A PRIVACY APPROACH IS INADEQUATE

Little progress can be made in understanding the information externality without first understanding the costs and benefits of privacy. Privacy advocates argue that a consumer’s personal information can be used to inflict harm on that consumer. For example, a consumer’s credit card and identity information can be stolen, inflicting high costs or damaging reputations. E-mail addresses and telephone numbers can be collected and spammed, wasting precious time and resources. Because these harms are undesirable and because people should be protected from harm, society must prevent the misuse of consumer information through privacy.

Among the classic citations in the privacy literature is Brandeis and Warren (1890), who viewed privacy as a negative right “to be let alone.” The concept of privacy has evolved over the last century to the positive right to be kept free from harm. In this vein, Rotenberg (2001) stated that “the protection of privacy in law is central to the American legal tradition.”

Privacy, as it has been enacted in law, most resembles inalienable rights (Calabresi and Melamed, 1972) that impose protective behaviors on others. Inalienable rights are the strongest form of protection available to safeguard individuals. Unlike property rights, which are quite limited, inalienable rights cannot be exchanged or sold. An individual may choose to leave these rights unexercised; however, if the individual cannot disavow them. Familiar examples include the right to be free from governmental coercion in the realm of speech, assembly, and worship. Excessive police powers are reigned in by the right to due process, proscriptions against self-incrimination, and the right to be free from torture and other cruel or unusual punishments. Equal opportunity is predicated on the right to be free from discrimination based on sex, race, color, national origin, and religion. Calabresi and Melamed’s analysis suggests that inalienable rights are so strong that they should be used only when potential harms to individuals are significant and when alternative methods of protection are inadequate.

As with freedom of conscience and equal opportunity, an inalienable right to privacy would be justified if the following conditions exist: (1) the harms cannot be avoided, (2) the harms are severe, and (3) privacy rights are the only efficient method to reduce the harm.

What is frequently ignored in privacy discussions is that some injury is unavoidable when people interact through commerce (Calabresi and Melamed, 1972). Accidental disclosures of personal information will cause injury to some people. Unscrupulous people will attempt to defraud others by using their personal information. Even with the most intrusive of law enforcement, society cannot eliminate this harm entirely.

It must also be understood that restrictions on the use of consumer information in the form of privacy rights will prevent the beneficial uses as well as the harmful uses. There is an opportunity cost to society if privacy restrictions prevent the use of individual information to create benefits. Utilitarian thinking suggests that it would not be unethical for society to compare the costs and benefits of privacy with other alternatives and choose the option through some calculus that balances the needs of society with the need to protect individuals from harm (Mill, 1987; Velasquez, 1992; Baron, 2000; Steiner and Steiner, 2003).

Given the preceding discussion, it should be noted that harms can be reduced in number and magnitude when individuals exercise due care with respect to their own personal information. People can take preventative steps to minimize the harm from information misuse:
Society should evaluate the alternative solutions for managing personal information before adopting privacy rights.

Information is a beneficial economic good. Businesses’ use of consumer information, such as names, addresses, and phone numbers, is beneficial to consumers because it allows businesses to communicate with or deliver goods to consumers. Consumers recognize that the use of their information for communications related to new product offerings or safety recalls is valuable. Consumers rarely dispute such beneficial uses of their personal information. The privacy issue becomes relevant only when consumer information is misused or consumers suffer harm related to their information.

Like other economic goods, information provides significant benefits and is costly to create. For an extremely tangible example of the high cost of information, consider the cost of consumer product safety information related to automobile crash tests. To determine the safety of the various makes and models of cars, under a variety of conditions, researchers must crash a lot of cars and they must do so in a variety of ways. The information is beneficial to consumers but is also expensive to create.

Information has several characteristics that distinguish it from other economic goods. The previous example illustrates two of these characteristics: non-deletability and non-excludability (Walters, 1993). Once information is created, it can be distributed to any number of additional information consumers at negligible cost. For instance, the information about automobile crash test safety does not require the consumption of additional cars to create duplicate reports. The characteristic of non-deletability means that, unlike other products, information is not used up through use. Additionally, once information is created, it is costly to prevent its distribution to unintended consumers. Consider the business model of a company creating the automobile crash test safety report for sale to car consumers. If the crash test company wanted to sell the report, they could set the price to cover the cost of the printing as well as a percentage of the cost of all the cars consumed in collecting the research data. Once they sold a few copies of the report, a consumer might copy and distribute it to other consumers for only the printing costs. The alternative business model is to sell the report once for the full price of collecting all the data. Regardless of which business model is chosen, the characteristic of non-excludability means that expensive methods must be used to prevent unintended information consumers from getting information for which they have not paid (Priest, 1997). The example of online music swapping illustrates this and reminds us that legal solutions may do little to correct the underlying problem.

The economic implications of non-deletability can be grasped when considering large-scale electronic databases containing consumer information on thousands or millions of people. The marginal cost of another database is the marginal cost of a blank CD or other form of data transfer. Toys R Us, a Fortune 500 firm, sold its customer database to Coremetrics. Toys R Us incurred little or no additional cost while being compensated by Coremetrics (Liu, Marchewka, & Mackie, 2003). Non-excludability implies that Toys R Us must engage in expensive

WWW.ISM-JOURNAL.COM
SUMMER 2006
contracts or software protections, or resort to post hoc legal remedies, to prevent Coremetrics from reselling that database to other companies.

The implication of these characteristics is important to the market for information. In a properly functioning market:

- Consumers pay sellers the full price for goods purchased.
- Sellers deliver to consumers the total value intrinsic to the goods sold.

Information markets do not function properly in that they are inefficient in the distribution of costs and benefits of traded goods. Information suppliers find it difficult to create and sell information to consumers who might benefit from that information because once the information is sold to one consumer, copies will be made, and some consumers will forgo the purchase of the good by obtaining it from another consumer. This distorts the market for information. The distortion results in what is called an externality (Walters, 1993). An externality exists when producers or consumers do not pay the full costs or receive the full benefits from a market transaction.

Externalities are morally suspect because they allow some buyers and consumers to gain benefits that should belong to others or avoid costs that they should pay. This violates the ethical perspective of distributive justice (Perlman, 1963, 1967). Mass mailers, telemarketers, and spammers benefit from relatively low-cost methods of contacting consumers, but the costs of that marketing are imposed on consumers. The cost to consumers is the sum of the value of time spent dealing with marketers and the costs of dealing with their communications. The benefits to consumers vary with their desire for those communications. In the example of a marketer that sells a huge database of consumer data to another marketer, each marketer benefits at the expense of the consumer, who must spend additional time and resources dealing with the new marketer. When a business fails to make the necessary investment to safeguard consumer information and is then a victim of a hacker, it is the consumer who must pay the price. Axiom Corp (Clampet, 2000) and RealNames (Stellin, 2000) are two companies that failed in their responsibility to protect consumer information and imposed high costs on consumers.

A final note about information is critical. The value of information is individual and context specific. Several examples will suffice to illustrate this. Different people may experience different costs and benefits concerning their personal information. For instance, health information will have different costs and benefits to (1) healthy patients vs. (2) patients with stigmatized diseases (e.g., AIDs, leprosy, etc.). Individuals may experience different costs and benefits for the same information, depending on how it is used. Personal consumer information may have one value when in the hands of a trusted and responsible merchant and another value when in the hands of an Internet spammer. The point is that the value of information can vary from person to person and can vary to one person depending on the situation.

Because alternatives to privacy exist, we might find other methods that would be more efficient and produce greater benefits. There are a variety of methods for correcting externalities: regulatory restrictions can specify legal and illegal conduct, government can sell the right to create an externality, government can subsidize positive externalities or tax negative externalities, and finally government can assign entitlements that, by themselves, eliminate the externality (Ekelund and Tollison, 1994, p. 447). As an example of a tax solution, a mass marketer might be compelled to pay “Internet postage” equal to the full cost imposed on all recipients of Internet advertising. A more market-based regulatory solution might compel the marketer to pay the recipient of Internet advertising some amount determined by the recipient as a precondition for receiving the advertising. Although both solutions would reduce the amount of unwanted advertising, they each present problems. With the first solution comes the difficulty of calculating the full cost to consumers. With the second solution, consumers might solicit unwanted advertising simply for the compensation.

From the previous discussion it can be inferred that externalities allow businesses to benefit from consumer information that far exceeds the cost of that information while some consumers are harmed. Further, it can be inferred that consumers should benefit from their information to a much greater extent than they do. These cost and benefit transfers between businesses and consumers are lucrative to business and costly to consumers and create strong incentives to violate whatever privacy rules society adopts. Even if society adopts strong privacy rules, financial incentives exist to encourage violations of those rules.

Economists generally agree that, if feasible, the best way to correct externalities is to correct
the market failure that causes them. Correcting the market failure has the advantage that, once it is corrected, all the market participants have the incentive to act in ways that produce the greatest value. Properly functioning markets are economically efficient from the standpoint of utilitarianism and ethically efficient from the standpoint of meritocratic justice. Government regulation of externalities, as in the case of privacy, can reduce some problems but does not correct the underlying market failure, because regulation invariably requires some entities to act against their own interests. In some cases, the market failure cannot be corrected and government regulation is the only way to solve the problem. Legislation designed to protect civil rights and prevent the sale of harmful products are examples. Now we turn to an alternative solution to the problem of information externality.

ALTERNATIVE APPROACHES: APPL YING THE COASE THEOREM

Ronald Coase won the 1991 Nobel Prize in economics for his insights into correcting externalities. Coase (1960) argued that it does not matter to whom entitlements are assigned provided parties are free to bargain. At the time, and in certain circles today, this was a revolutionary concept because existing legal practice emphasized that:

1. Only governments, by means of taxes and subsidies, could internalize externalities in economic exchange or production (Pigou, 1920).
2. Entitlements had to be assigned to the victim.

The Coase theorem is important because it showed that society could correct the externality if it assigned an entitlement to nongovernmental entities, and, counterintuitively, it did not matter to which party the entitlement was assigned. Further, the entitlement could be assigned through the legal institution of liability or the legal institution of property rights. This opened greater latitude in solving externalities. The implication is that the granting of entitlements can correct externalities and society doesn’t have to rely solely on invasive government regulation. The practical implications of the Coase theorem are that by assigning someone ownership of consumer information, that owner would have the economic incentive to use that information efficiently.

Coase did note that impediments to bargaining can reduce the efficiency of markets. Therefore, the granting of entitlements tends to be an efficient mechanism for correcting externalities when impediments are low. These impediments, or transaction costs, increase when the parties are unknown or are large in number (Baron, 2000).

Calabresi and Melamed (1972) expanded on Coase’s insights by suggesting practical issues, related to transaction costs, to examine when considering entitlements. They define an entitlement as an entity’s ability to own a resource or take an action under the state’s protection. They distinguish three types of rules or mechanisms for protecting entitlements — property rules, liability rules, and inalienability rules. Calabresi and Melamed warn that these rules are conceptually powerful for understanding entitlements but tend to converge in some areas and leave gaps in others. The nature of the protection provided by each type of entitlement is important:

- **Property rules**: Property rules prevent a person from infringing on the property right holder without the holder’s permission (Baron, 2000). A property right holder possesses control and transfer rights, which gives the right holder (1) decision control — the right to decide if, when, or how to use the property; and (2) transfer control — the right to decide when, to whom, for what price to sell the property. The holder of a property right cannot legally be forced into giving up either control rights or transfer rights. Those rights can be transferred to a buyer only at a price determined by the right holder (Calabresi and Melamed, 1972).

- **Liability rules**: Liability rules protect entitlement holders differently. Liability rules permit infringement but require the infringing person to compensate the entitlement holder for damages. Fair compensation is determined by the market or society, not by the entitlement holder. For example, the recent U.S. Supreme Court decision in *Kelo et al. v. City of New London et al.* (2004) upheld that private property is protected from local governments only by a liability rule, whereas that same property is protected from nongovernmental agents by a property right. The law of eminent domain allows the government to seize private property for public purposes and compensate the owner for the violation (Calabresi and Melamed, 1972).

- **Inalienability rules**: The First Amendment to the U.S. Constitution provides an example of
an entitlement protected by an inalienability rule: the right to freedom of expression. This right cannot be given up, even voluntarily. Inalienability rules are used when inflexible and powerful protections are needed to prevent harm to people under conditions when alternatives are unlikely to work. Given the tendency of people to surreptitiously discriminate against others, the right to be free from discrimination, as provided under Title VII, is another inalienable right that could not have been provided using alternative methods. Alternatively, if property and liability rules are likely to be effective, inalienability rules should not be used.

The application of the Coase theorem to the topic of consumer information suggests that either property rules or liability rules could be used to solve the information externality. Precedence exists for using property rights to assign entitlements to specific pieces of information that are unique and identifiable, such as in the case of intellectual property. Although the total amount of information that is protected by property rights is relatively small, there is little reason to dismiss its use in protecting consumer information. Precedence also exists for using liability to assign entitlements to consumer information, because those who inflict harm on others can be held liable under the law of torts (Whitman and Gergacz, 1991). The law of torts recognizes that individuals who are harmed in society are entitled to some form of compensatory justice (Velasquez, 1992). For instance, if one person disseminates damaging but untrue information about another person, the second person has the right to compensation. If factual information is used improperly, for purposes of prejudicial discrimination, the victim has the right to compensation.

Calabresi and Melamed's Principles

The previous section discussed how entitlements could be used to solve the information externality through either property rights or liability rules. The natural question is, which is the best way to assign entitlements? To answer this question we need to consider the factors outlined by Calabresi and Melamed (1972). Their five criteria are

1. The assignment of entitlements should balance the social benefits (e.g., economic efficiency) with the social costs (e.g., harm to individuals). If one entitlement assignment results in huge net benefits for society and trivial individual costs it is preferable to another assignment with trivial net benefits for society and huge individual costs.

2. In the absence of certainty as to the costs and benefits to society, the entitlement should be granted to the party best able to make such a cost–benefit analysis.

3. When there are alternative means of achieving beneficial outcomes (balancing costs and benefits), the entitlement should be assigned to the party that can do so at the lowest cost.

4. In the absence of certainty as to which party is more efficient at achieving the lowest social costs, the entitlement should be assigned to the party with the lowest transaction costs.

5. Since markets are inefficient in the presence of high transaction costs, a decision will often have to be made between using market transactions or collective fiat depending on which is most likely to bring us closer to the socially efficient or Pareto optimal result (pp. 1096–1097).

Calabresi and Melamed's principles generally follow the philosophy underlying the Coase theorem. These principles focus on net social benefit, where total benefits exceed total costs, and specifically address externalities.

Assigning the Entitlement and Choosing an Entitlement Rule

According to the Coase theorem, assignment of an entitlement would resolve the information externality. In the case of consumer information, that entitlement could be assigned to one of three separate entities: (1) the specific consumer described by the information, (2) a business that loaded the consumer's information or caused the information to be loaded into a database, or (3) a third-party business (e.g., DoubleClick) that compiled a particular database from existing sources. Although the Coase theorem indicates that we do not need to worry about who receives the entitlement, transaction cost analysis suggests that the assignment to one entity might be more efficient than assignment to another.

According to the prior discussion and the five principles suggested by Calabresi and Melamed (1972), we know that:

1. Information sharing contains positive net benefits.
2. Consumers suffer from substantial harms when information is misused, and the value of those claimed harms can be inflated by opportunistic consumers or reduced by careful behavior.
3. Business is in the unique position to be able to determine the most efficient method of protecting consumers from information misuse.
4. As the central repository of consumer information, business has the lowest transaction cost and thus should shoulder the costs of protecting consumers from harm.

Because of the high transaction costs (Singleton, 1998; Baron, 2000; Nott, 2003), it would be inefficient to assign property rights to individual consumers. Consider the high cost of online banking if individual consumers had the right to withdraw their information from databases that monitor creditworthiness. To compensate for unforeseeable risks, online banks would have to raise interest rates and lower credit limits on any individual who withdrew from the system.

In points 3 and 4 above, businesses are singled out as efficient because they have fewer transaction costs. It is important to note that database archivists may be more efficient protectors of consumers than businesses in general because they have fewer transaction costs (e.g., Acxiom Corp). On the other hand, unless we hold those archivists accountable for the harms they cause directly and indirectly (e.g., security leaks), they will have little incentive to minimize the harm to consumers.

The choice of entitlement rule, between property rights and liability, is the next major question. If society decides to solve the information problem using a property rule, it will assign control rights, much like ownership rights, to specific pieces or components of information, similar to the way it provides for patent and trademark protections. The “owner” of “consumer information” would hold exclusive rights to the use, handling, and distribution of that information. In each of these three cases, the owner would hold veto authority over the use, handling, and distribution of a consumer’s information. In this vein, commentators (Bibas, 1994; Laudon, 1996) and the private sector generally prefer market-based, contractual solutions to personal information protection over the strict regulatory regime. Here, consumer information is a commodity to be exchanged with monetary rewards. The use of information would be prohibited unless it was properly purchased or leased. Restrictions on leased information, intended to protect consumers, are likely to be difficult to specify in advance, quite complex, and costly. The enforcement mechanisms need to remedy violations of such rules are likely to be even more costly and difficult to manage.

The liability approach would permit the selling or leasing of information, but instead of cumbersome prohibitions on use, the users of information would be held accountable for damages resulting from the misuse of accurate information or the use of inaccurate information. Liability rules allow more flexibility in the use of information but hold the users of information responsible for harms inflicted and require restitution to those harmed. Of the two approaches, the liability approach — which requires a system to monitor both data collectors and database archivists in e-business for both improper use and incorrect information — is likely to be more efficient than a property rights–based system of contracting that needs to anticipate problems and remedy violations of contracts.

Thus, the liability approach appears to be more efficient and can ultimately correct the problem of information externality in an e-business environment. When society agrees to adopt a liability approach, the entitlement is assigned to online companies and they are liable for any damage or harm caused by their actions. E-business studies (Gefen, Karahanna, and Straub, 2003; Pavlou, 2003; Suh and Han, 2003) have suggested that trust is critical for the acceptance of electronic commerce. A liability approach is expected to lead to a dramatic increase in consumer trust, and more online transactions by consumers are likely to occur. Thus, both entities — consumers and online companies — will receive benefits from this liability approach, and at the same time electronic business can reach its full potential.

IMPLICATIONS FOR IMPLEMENTING THE LIABILITY APPROACH FOR E-BUSINESS
Implementing the liability approach requires certain actions from two important entities in society — government and online companies — for the full potential of electronic business.

The Role of Government
From a more practical point of view, the implementation of a liability rule in countries such as the United States might take precedence from
the existing law of torts that assesses responsibility on the basis of proposed, current, or historical standards. Two currently used standards—negligence and strict liability—are important to this discussion. Negligence requires that the culprit both caused damage and intended to act improperly. Behaviors are considered improper if the actor failed to exercise “due care.” Strict liability requires only that the culprit caused damage (Whitman and Gergacz, 1991). Strict liability removes the necessity of proving intent: “The law evolved because it is often not feasible for a consumer to prove negligence” (Birnbaum, 1988, p. 142).

Our social intuition and procedures for dealing with huge amounts of consumer information are relatively new, and little definitive guidance exists on what is proper or improper behavior. This would make it very difficult and costly to determine consistent standards for negligence. Because it is unlikely that most consumers have the resources to obtain enough information to prosecute online companies under a negligence standard, the strict liability standard would seem to be the most viable in this situation. We therefore argue:

The government needs to formalize a law of strict liability which provides organizations with basic but clear guiding principles for collecting, using, and distributing consumer information.

The United States has neither enacted comprehensive data protection legislation nor designated an independent agency to oversee information privacy issues at the federal level. No federal law governs the collection, use, and storage of personal information by the private sector (Banisar, 2000; Baumer, Earp, and Pindexter, 2004). Because federal privacy protection has been enacted at a basic level, the various states have enacted more comprehensive legislation that lacks standardization. The resulting patchwork of laws makes business compliance both complex and expensive (Heller, 2002). It also makes enforcement by state authorities problematic because these laws can be enforced only within one state’s jurisdiction. This has led to calls for more federal standardization (Vijayan, 2003).

Without a standardized system to protect personal information when consumers venture online, electronic commerce will never reach its full potential. For this reason, we argue:

The U.S. government should fulfill its lawmakers role as an economic standard setter by enacting a system that permits useful and efficient uses of information while specifying a liability system to protect both companies and consumers from injury using the standard of strict liability.

The law of strict liability should be flexible and minimal enough so that both companies and consumers, acting in the course of their normal activities, can act in economically efficient ways. It should also be broad enough to recognize injuries and deter misuse. These changes to the legal system would increase consumer confidence and lead to market efficiency and increased transactions, as well as ethical data management.

One example of strict liability would be the default rule–based approach proposed by legal scholars (Kang, 1998; Samuelson, 2000) to govern uses and disclosures of consumer information. A default rule is a rule of law that can be superceded by a contract, trust, will, or other legally effective agreement. Contract law, for example, can be divided into two kinds of rules (Barnett, 1992):

- Default rules, which can be modified by agreement of the parties
- Mandatory rules, which will be enforced even if the parties to a contract attempt to override or modify them

To this end, Kang (1998) argues in favor of a default rule that allows only “functionally necessary” processing of consumer information unless the parties expressly agree otherwise. He proposes a statute that translates academic theory into legislative practice. The liability law can grant consumers a protectable interest in their personal information without grounding that interest in property law. It can do so by setting a default rule or a uniform federal law forbidding certain activities with respect to this information, such as unauthorized collection or use unless the consumer has agreed to these activities (Kang, 1998). Samuelson (2000) proposes trade secrecy law, which remains a tort law that has a number of default rules to guide consumer information handling by companies. Trade secrecy for consumer information would allow three things. First, it protects the interests of consumers to restrict access to and unauthorized uses of private information. Second, it can give companies and consumers control over commercial exploitations of their secret and private information. Finally, it can set and
We argue that a liability law reflecting these default rules needs to be enacted for electronic business.

We argue that a liability law reflecting these default rules needs to be enacted for electronic business.

Voluntary Roles: Industry Groups and Individual Companies

One reason why society adopts liability rules is to increase “precaution” in an actor’s decisions and actions. With liability rules, industry associations and individual companies should be proactive. As society adopts more stringent liability rules, evolving from negligence to strict liability, this encourages greater precaution. The use of less stringent liability rules leads to lower levels of precaution and less proactivity.

The absence of comprehensive strict liability standards related to consumer information has led to the use of negligence standards. A negligence rule holds a business liable for damages only if due care has not been taken in undertaking the collection, use, and distribution of consumer information in both electronic and physical settings. Negligence rules do not encourage efficient “precaution” on the part of business. For example, in one recent case the court assigned liability to Docusearch.com for damages caused by selling personal information, using a negligence standard. In another case, EarthLink won $16 million in a spam case to directly compensate it for malicious attacks from mass marketers (Roberts, 2003). Although this illustrates that a negligence standard can be successfully applied, we have little confidence in either the consistency of this approach or the degree of protection provided.

An example of a proactive approach is the adoption of different seal programs (e.g., Online Privacy Alliance, TRUSTe, and BBBOnline) by industry and trade associations (Moores and Dhillon, 2003). According to a Greenfield Online survey, 84 percent of consumers indicated that third-party recognition of an E-business firm would make them more likely to purchase from that firm (Hemphill, 2002). Another proactive mechanism that could be adopted by industry and trade associations is a reputation system (Resnick, Zeckhauser, Friedman, and Kuwabara, 2000). Currently, reputation systems or similar customer feedback systems/forums are popularly used in Web sites such as eBay. After a transaction, buyers and sellers have the opportunity to rate each other and leave comments. Similarly, industry and trade associations can develop reputation systems in which customers rate online companies based on their past experiences with the companies’ products and services as well as practices of consumer information handling. Through such systems, industry and trade associations can protect their industry, trustful online firms, and consumers. Institution-based trust has been found to be important for building effective online marketplaces (Pavlou and Gefen, 2004).

Resolving conflicts between consumers and companies in court is costly. Avoidance of harm is ideal. The ideal liability approach would encourage all parties to prevent or minimize injuries in the online environment. This suggests that online firms need to be preventative, rather than reactive, and cautious about the potential misuse of consumer information. Several major corporations, including IBM, AT&T, Microsoft, EarthLink, DoubleClick, and 24/7 Media, have attempted to achieve this by creating the position of chief privacy officer (CPO) to oversee company relations with their consumers and other firms (Hemphill, 2002).

Online firms should invest in addressing consumer concerns of security and information handling. Consumers report that security and information handling disclosure on Web sites are characteristics of an effective business-to-consumer Web site (Ranganathan and Ganapathy, 2002). Recent studies also indicate that perceptions of lack of security and information handling disclosure lower consumer trust in the Web site and influence behavioral intentions to purchase online (Liu et al., 2004).

Individual companies need to commit to the fair collection, transfer, and use of consumer information; adhere to some basic principles of fair information practices; and prepare their
own practice guidelines and policies. At least four core aspects should be considered in developing fair information practices: notice, choice, access, and security (Pitofsky, 2000). Applying the Federal Trade Commission’s recommendations, for example, to the financial industry, individual companies should:

- Provide consumers clear and conspicuous notice of their information practices.
- Offer consumers basic choices as to how their personal information is used beyond the original purpose.
- Allow consumers reasonable access to their personal information for review and correction.
- Take serious actions, both organizational and technological, for the security of their customers’ information.

Further, the misuse of consumer information by online firms will not only expose them to more risks (e.g., damages to reputation) and potentially serious financial consequences, but will also increase consumers’ privacy concerns. Intense media attention on consumer injuries, without considering the high costs of privacy or the costs and benefits of alternative solutions, may push the issue of consumer information further from discussions of the information externality toward privacy solutions. This may further drive society to adopt a restrictive approach focusing on restrictive privacy laws, based on strong government regulation. As argued previously in the article, this restrictive approach both ignores market failure and is likely to be harmful to electronic business. Such a restrictive privacy approach to online consumer information can result in the loss of benefits that both consumers and companies can receive through information sharing and reuse. At the same time, the implementation of restrictive privacy laws in electronic business can be very costly to both companies and consumers. According to Staten and Cate (2002), some of the potential adverse impacts of mandatory privacy laws requiring explicit consumer consent for information collection, transfer, or use in the arena of credit card services and products include more offers made to unqualified consumers, missed opportunities for targeted marketing to qualified consumers, and impaired efforts to prevent credit card–related fraud.

**CONCLUSION**

The U.S. government and commercial sector have opted to use privacy regulations to control an information externality problem: the misuse of consumer information. We argue that this is undesirable because it does not correct the market failure that causes the information externality and leaves the market inefficient. Regulatory solutions constrain society for years or even decades past the point where technology could solve the problem efficiently. Correcting the externality creates incentives for all parties to act efficiently. The Coase theorem suggests that this market failure can be corrected using either property rules or liability rules; the externality cannot be solved using inalienability rules such as privacy. We suggest that both property and liability rules have costs and benefits, but that liability rules are likely to be the most socially efficient.

A liability approach should include the legal standards of both strict liability and negligence and should be enacted through both regulation and voluntarily adopted industry standards. First, the government should enact a minimal set of legal rules applicable to all online industries and that embodies liability standards. These rules would be flexible enough to take into account unique requirements and risks and minimal enough so that online firms are not unnecessarily constrained. Such a law can increase consumers’ trust in online firms and encourage secure online transactions. For the liability approach to be successful, industries and individual firms should proactively enact self-regulatory codes and norms (e.g., seal programs) and make public their policies and practices for handling consumer information.

In summary, the full potential of E-business cannot be achieved without a better federal approach to the problem of consumer information misuse. A strict privacy regulation approach should be avoided and a liability approach — with certain roles by government, industries, and individual firms — should be implemented to solve the information externality and increase the market efficiency in the electronic marketplace。

**References**


AT&T. (1999, April 14). Beyond concern: Understanding net users’ attitudes about online privacy (AT&T Labs Report Number TR


Clampet, E. (2000, 11 Feb). RealNames is latest hack victim. internetnews.com


