Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy

by
PETER P. SWIRE*

This Article puts forward two claims and one proposed new term. The first claim, buttressed by new evidence in this Article, is that we have under-valued the importance of binding legal rules in promoting electronic commerce ("E-Commerce"). The second claim is that, in light of the demonstrated helpfulness of binding legal rules, the case for Internet privacy legislation in the United States is stronger than it was during the start-up period of E-Commerce during the 1990s. The new term, which is central to both of these claims, is the idea of "trustwrap"—the ways that merchants can wrap their transactions in visible, trust-inspiring ways when conducting E-Commerce.

The idea of trustwrap arose for me in thinking about the Tylenol scare in the early 1980s.[1] A malicious person injected cyanide poison into bottles of Tylenol pills, resulting in several deaths and enormous negative publicity. The Johnson and Johnson Company, led by James Burke, reacted with perhaps the most-admired crisis response in corporate history.[2]

The first part of the response was an immediate announcement that all Tylenol on the shelves nationwide would be removed immediately. The company would take whatever short-term loss was necessary to assure customers that no tainted Tylenol would remain available for sale. This strong statement that the company would "do the right thing" created immediate and widespread sympathy for Johnson and Johnson.

* Professor of Law, Moritz College of Law of the Ohio State University; Chief Counselor for Privacy in the U.S. Office of Management and Budget, White House Electronic Commerce Working Group, 1999–2001. My thanks for able research assistance from Cary Bishop, Larry Glasser, and Aimee Kaplan. My thanks also for comments from participants at the Enforcing Privacy Rights Conference and the Conference on International Governance of New Technologies hosted by the School of Advanced International Studies and George Mason University.

1. Indeed, the working title for early versions of this article was *Why E-Commerce is Like a Bottle of Tylenol*.

2. *See* N.R. Kleinfeld, *Tylenol's Rapid Comeback*, N.Y. TIMES, Sept. 17, 1983, (Business), at 33. Tylenol, is of course, a registered trademark of McNeil Labs for its brand of acetaminophen.

The second part of the response, and the more relevant part to the topic here, was the decision by Johnson and Johnson to re-engineer every sale of Tylenol. Today, every bottle of pills has a plastic wrap around the outside of the bottle. Customers can examine this unbroken plastic before they buy the bottle. In addition, every bottle has a foil seal inside the cap. This foil proves that nothing (such as the syringe that earlier had contaminated the capsules) has penetrated the protected area where the medicine actually resides. Inside the bottle, the medicine exists in tamper-proof caplets or tablets, rather than the earlier capsules into which the malicious person had injected the poison.

In short, Johnson and Johnson built trust into every transaction. Customers use their own senses to reaffirm that the Tylenol is safe. They touch the plastic wrap, they open the foil seal, and they take a tamper-proof pill. My informal polling shows that many people will choose a safety-wrapped bottle instead of a traditional bottle of pills that lacks the safety wrap. Tylenol regained its market share within six months of the crisis, and it remains a trusted brand today.[3] One of the biggest crises in consumer confidence became one of the greatest successes.

I propose the term "trustwrap" to bring together the physical transactions of Tylenol and the virtual transactions of E-Commerce. The idea for "trustwrap" originates with the plastic wrap and related techniques that Tylenol uses to demonstrate trustworthiness. We cannot literally follow the Tylenol example on the Internet and use plastic wrap to prove that transactions are safe.[4] We can, however, study which techniques build equivalent forms of trust for virtual transactions. Moreover, the term "trustwrap" invokes the "shrinkwrap" plastic that goes around a box of software, the "shrinkwrap licenses" that often come inside a box of software,[5] and the "clickwrap licenses" that have spread across the Internet.[6] For my proposed use of "trustwrap", the seller demonstrates in the course of the transaction that there are legal, technical, or other protections for the purchaser.

3. Jason Richardson & Eric Bolesh, *Toward the See-Through Corporation*, PHARMACEUTICAL EXECUTIVE, Nov. 1, 2002, *available at* 2002 WL 13373849.

4. The closest analogy would be to use encryption to "wrap" around online communications. Although encryption is enormously useful for certain tasks, there are many issues that it cannot solve. For instance, encryption can help prove that the words a person sends are the words that eventually arrive. But encryption is no help at all in determining whether the sender is a trustworthy person in the first instance. For an analysis of the uses and limits of encryption in E-Commerce, *see* Peter P. Swire, *The Uses and Limits of Financial Cryptography—A Law Professor's Perspective*, *available at* http://www.peterswire.net.

5. *See, e.g.*, Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429 (2002); Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239 (1995).

6. *See, e.g.,* Hillman & Rachlinski, *supra* note 5, at 431; Roger E. Schechter, *The Unfairness of Click-On Software Licenses*, 46 WAYNE L. REV. 1735 (2000).

Part I of this Article looks at three of the striking success stories of E-Commerce—the online credit card, the growth of "clicks-and-bricks" E-Commerce (companies that sell both on the web and in physical stores), and eBay. Each of these three success stories contrasts markedly with the predictions of the Internet pioneers of the mid-1990s. I argue that each success story has created effective trustwrap for online transactions. Notably, the trustwrap in each instance depends substantially on enforceable legal guarantees. This evidence from the success stories on the Internet shows at least a strong correlation with, and quite likely causation from, the sorts of legal enforcement that many observers thought would be irrelevant for Internet commerce.

Part II of the Article explores the implications of Part I on the debate about Internet privacy legislation. Based on my own experience as the Chief Counselor for Privacy for the Clinton Administration, the debates on Internet privacy have often asked whether a legislative or self-regulatory approach will be more effective at fostering trust and encouraging E-Commerce.[7] The success stories in Part I undermine the common view that binding legal rules will interfere with E-Commerce. In addition, a careful examination of our experiences with Internet privacy suggests that legal protections for privacy are more likely to be beneficial now than they would have been during the start-up period of E-Commerce in the mid-1990s. In short, binding legal rules for Internet privacy may well spur E-Commerce and provide more effective "trustwrap" than self-regulatory alternatives.

I. Trustwrap and the Role of Legal Rules in Encouraging E-Commerce

This part of the Article will first try to re-capture the vision of E-Commerce from the initial period in the mid-1990s. It will then examine how the three success stories of credit cards, clicks-and-bricks retailers, and eBay have developed contrary to many of the assumptions of the initial period. In particular, each of the three success stories has included binding legal guarantees as central elements of the ways that they build trust into online transactions.

7. For my own analysis see Peter P. Swire, *Markets, Self-Regulation and Government Enforcement in the Protection of Personal Information*, in PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE 3 (U.S. Department of Commerce ed., 1997), *available at* http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1A, also *available at* http://papers.ssrn.com/SOL3/papers.cfm?abstract_id=11472.

A. The Early E-Commerce Vision of E-Cash, Pure Internet Plays, and No Intermediaries

The early prophets of E-Commerce were infused with a sense of the different-ness of the Net.[8] Transactions would be done with revolutionary e-payments. Numerous new payment systems were discussed and proposed, including at financial cryptography conferences in which I participated. Mathematicians and business visionaries such as David Chaum[9] and Robert Hettinga[10] were convinced that electronic cash would soon be part of everyone's daily experience. The patents at the core of these new payments systems got start-ups off the ground, and major banks invested a great deal of time and effort exploring how to take advantage of the new e-payment systems.

Not only would the payments systems be new, but the merchants would be new, too. The late 1990s was the era of the pure Internet play.[11] The growth of Amazon and Yahoo! made other companies hope that they, too, could parlay a hot domain name into worldwide consumer sales. In the headlong rush to grow, business had to move at Internet speed. A month (or perhaps a quarter) was an entire new Internet generation. In this new environment, new Internet companies would be at a great advantage over the sluggish merchants of the traditional economy. Generation X would be ascendant, and their web sites would spell the end of retailers who were managed by people with gray hair and saddled with expensive real estate.

Next, search engines and other new technology would spell the end of intermediaries. At the most basic level, the Internet makes information flows essentially free, instantaneous, and global. Old markets had been characterized by physical and other costly barriers to matching buyers and sellers. The Internet removed these barriers. In the new, frictionless market, a specialized seller anywhere in the world could peddle wares to a buyer anywhere in the world.

Search engines became an almost-magical way to end friction and match buyers and sellers. As an example, suppose you wanted to buy a specialty item, such as a left-handed corkscrew. Where would you find one near your home? How well would the Yellow Pages solve your problem? What if you lived out on a farm—would you know how to find the right mail-order catalogue? Well, fortunately, we live in the world of the New Economy. A search today on www.google.com found 1,180 sites that

8. Lawrence Lessig has called the views of this initial period "Net95." LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 27–28, 33, 53 (1999).

9. *See* http://www.chaum.com (website of David Chaum).

10. *See* http://www.shipwright.com (website of Robert Hettinga).

11. *See A Challenge for Pure-Play Internet Companies*, INTERNETNEWS.COM, Nov. 5, 1999 (contrasting early success of "pure-play" Internet companies with growing success of multi-channel E-Commerce strategies), *available at* http://www.internetnews.com/ec-news/article.php/4_232871.

matched a search for left-handed corkscrews![12] The search took all of 0.12 seconds.

Traditional retailers and other intermediaries would also be challenged by new technologies for comparison shopping. "Shopping bots" would put the consumer in charge, allowing the buyer to compare prices across an enormous range of web sites. The comparison shopping pages would compete among themselves as well, offering so many different ways to give consumers just what they wanted. My www.google.com search for "shopping bot" found 143,000 sites.[13] In this vision of the New Economy, we are no longer stuck with the retail stores that happen to be close to our homes. Instead, we can shop 'til our fingers drop, instantly honing our searches to find the best product at the best price.

Taken together, this vision of the New Economy foretold a future of E-cash, of nimble Internet companies destroying physical retailers, and an end to intermediaries between sellers and buyers. It was an exciting vision, promising enormous change, but it has turned out to be wrong.

B. Credit/Debit Cards vs. E-Cash

Today, after the bursting of the dot-com bubble, it is easier to see that the prophets over-stated the uniqueness of E-Commerce. The mathematician might note that "commerce" and "E-Commerce" share eight out of nine letters. As a straight orthographic matter, they are thus about ninety percent the same. As a business matter, too, we all see that E-Commerce is subject to some ancient truths—companies must make a profit to survive, they can't lose on every sale and make it up on volume, and an intriguing commercial during the Super Bowl can't substitute for actually delivering a good product to the consumer.

As merchants have rediscovered these ancient truths, they have also invented ways to build trust into each transaction. For instance, the victory of credit cards over new e-payment systems is essentially complete.[14] Most consumer purchases over the Internet are made with credit cards or debit cards participating in the Visa or similar networks. By contrast, the leading

12. The search was conducted on March 17, 2003. Some of the 1,180 hits are duplicates, and some do not actually sell the corkscrews, but the buyer clearly has a large selection of sites that do. Perusal of these sites reveal that an entire industry has developed on the Internet for supplying hardware and other tools designed for left-handed people, a market that apparently was previously underserved. When I presented this paper, one person observed an unsuspected link between left-handed corkscrews and the title of this paper—having corkscrews that turn the correct way for left-handed people (clockwise) could actually reduce the sales of pain medicine such as Tylenol.

13. Search performed on March 17, 2003.

14. By far the most successful non-traditional payments system is PayPal. As discussed below, however, PayPal actually relies on the existing credit and debit card systems to offer binding consumer protections. *See infra* text accompanying notes 17–20.

e-payment prospects are either bankrupt or have refocused on different markets.[15]

In retrospect, the triumph of credit cards is easy to understand. Consider the benefits that a consumer gets from using a new form of e-cash. Essentially, the consumer gets the ability to transfer funds to the merchant and have the merchant instantly recognize that the payment is good.

The same benefit occurs when the consumer uses a credit card—merchants can instantly confirm that the credit card payment is good. In addition, however, a credit card purchase in the United States offers two key advantages. First, consumers are protected against the unauthorized use of the credit card number. By law, the credit card issuer covers any unauthorized use over $50.[16] In practice, most banks do not even charge the customer for the first $50. Second, the credit card brings with it an already-functioning dispute resolution system. If a merchant claims that a customer has spent $200 on software, and the customer disagrees, then the customer is not charged for the $200 while the dispute is in process.

What new e-payment system can match those two advantages? A new system has all the usual challenges of getting a global business up and running, such as figuring out the technology, enlisting partners to deploy the technology, and getting customers to learn how to use the new system. In order to match the $50 rule for unauthorized use, the new system would presumably need to find some private-sector guarantor against unauthorized use, and would then have to educate consumers about the guarantee. To match the credit card dispute resolution process, the new system would similarly have to create a system and then advertise it. These are difficult tasks, indeed.

Credit cards also have another advantage—established brand names and the accompanying sense of solidity. Consumers (and merchants) believe that Visa, MasterCard, and American Express are likely to remain in business for a long time to come. Standard game theory, and the common sense of most consumers, suggests that these sorts of long-term players are more likely to follow the rules of the game than are short-term players. A company that has an established relationship with a customer and a well-known brand has far more to lose by cheating than does a new company that might be trying to score quickly and get out. Established credit card companies thus had an enormous advantage over start-up e-payments approaches, much as the U.S. dollar gets trusted more than the currency of a newly established country.

15. Chaum's Digi-cash is bankrupt. Cyber-cash became a service company to online merchants, and did not even offer a consumer payment system anymore before its Internet payments business was acquired by Verisign. *See* http://www.cybercash.com.

16. *See* Clayton P. Gillette, *Rules, Standards, and Precautions in Payment Systems*, 82 VA. L. REV. 181 (1996) (analyzing consumer protection rules applying to unauthorized use of credit cards, debit cards, and checks).

The success of the online payment system PayPal might, at first glance, seem to contradict these conclusions about the advantages of established payment systems that offer binding legal guarantees. After all, you can use PayPal to transfer money to someone even if you only know that person's e-mail address. Perhaps, with over twenty million customers, PayPal has created a truly successful E-Cash system.[17]

A closer look at PayPal, however, instead reinforces the importance of both established payment systems and binding legal guarantees. In every instance, the recipient is part of the established, bank-based payments system. Originally, PayPal relied on customer checking accounts. New customers would inform PayPal of the routing and account numbers for their checking accounts. PayPal would verify the account,[18] and a customer could then receive money payments in the checking account. Today, customers are far more likely to use credit cards to open their PayPal accounts.[19] Instead of being a direct form of E-Cash, PayPal instead piggybacks on the reputations of customers' banks and the legal guarantees that accompany participation in the established payments system.[20]

C. Clicks-and-bricks vs. Pure Internet Retailers

Established bricks-and-mortar retailers have turned out to have similar advantages over pure Internet retailers. A large and growing percentage of consumer Internet purchases occurs with "clicks-and-bricks" sites, where the Web site has the same name as an established physical-world retailer.[21] The offline retailer comes equipped with a brand name and a sense of solidity. It has "real" stores in addition to the web site. I suspect that the physical experience of visiting a Staples, Wal-Mart, or Barnes & Noble helps an individual trust that the Web site will perform successfully.[22] A

17. *See* http://www.paypal.com/cgi-bin/webscr?cmd=_ir-release&rid=339819.

18. For instance, when my research assistant opened a PayPal account, PayPal made deposits of $.36 and $.11 into the checking account. My assistant then contacted PayPal to confirm the amounts and prove his access to the account.

19. According to its initial public offering: "For the nine months ended September 30, 2001, customers funded 22.2% of payment volumes through their existing PayPal balances, 26.7% via bank account transfers and 51.1% by credit cards." *See, e.g.,* S.E.C. Filing No. 02530308, at 51 (02/07/2002) *available at* http://ccbn.tenkwizard.com/contents.php?ipage=1612158&repo=tenk&TK=PYPL&CK=0001103415&BK=FFFFFF&SC=ON&TCI=FFFFFF&TC2=FFFFFF.

20. In addition, a majority of PayPal transactions are covered by the legal guarantees offered by eBay, discussed *infra* text accompanying notes 25–28. Even before eBay agreed to acquire PayPal in 2002, about 60% of PayPal transactions were related to online auctions. *See* http://www.paypal.com/cgi-bin/webscr?cmd=_ir-release&rid=317994.

21. A search of the "allnews" database on Westlaw found a reference to "clicks and bricks" as early as a May 24, 1999 article in Ad Week. Use of the phrase ballooned after that, with 182 uses between August 1 and the end of 1999.

22. I will leave it to the evolutionary psychologists to study the extent to which the ability to physically sense an item contributes to an individual's trust in the quality of that item. *See*, *e.g.*,

consumer's transaction with Staples, for example, is wrapped in the protection offered by the local store and its national reputation.

But what about the old conventional wisdom, that offline retailers are too slow to respond to the Internet marketplace? In part, that conventional wisdom was inevitably going to become less true over time. We now can see the late 1990s as a start-up phase for the entire industry of E-Commerce. During the start-up phase, as with the start-up of an individual company, there are the late nights, long weekends, and frantic efforts to grow the company before the cash runs out or the window of opportunity closes. After a time, the successful start-up company becomes more mature. There is more emphasis on execution and professionalism, and less need for the hectic virtues of doing something brilliantly for the first time.

In comparing the pure Internet plays to clicks-and-bricks, then, many people confused the need for speed *during the start-up phase* with the need for speed on an ongoing basis. It is assuredly true that E-Commerce companies from now on will have to move rapidly to adjust to changing markets. But so will offline retailers and other participants in the universally fast-paced world of modern business. Over time, less of the success of an E-Commerce site will be based on doing the transaction a different way today than it did it a month ago. More of the success will be based on traditional virtues such as managing inventory, controlling costs, buying in volume, and the rest.

In this more mature E-Commerce market, the traditional retailers' supposed weaknesses become their strengths. Some of the retailers have taken time to learn to do it right. The office-supply giant Staples, for instance, saw its Internet sales and profits flourish in 2001, during the collapse of many pure online retailers.[23] It turns out that rushing to market during the dot-com boom was not essential, at least if a brand name and physical stores back up the Web effort. Along with this possibility of going slow-and-steady, the offline retailer already has the existing inventory systems, buying relationships, and cost-cutting measures that provide the competitive edge in a more mature market.

Clicks-and-bricks retailers also have more in their favor than a trusted brand name and physical solidity. They, like the credit card companies,

ROBERT WRIGHT, THE MORAL ANIMAL: EVOLUTIONARY PSYCOLOGY AND EVERYDAY LIFE (1994). To follow the sort of reasoning used by Robert Wright in *The Moral Animal*, it is intuitively plausible to me that the ancestors of homo sapiens developed elaborate ways on the ancient savannah to tell whom to trust or not trust. *Id*. From my own interactions online with other people, I have gotten to know many people online first, and then met them face-to-face. My own experience is that I often trust someone more after we have met face-to-face, having a "real" connection to supplement the virtual connection.

23. *See* Reuters, *Staples Earnings Sink, Online Unit Shows First Profit* (Aug. 21, 2001), *available at* http://www.idg.net/english/crd_staples_772063.html; Reuters, *Office Product Retailers Welcome Online Success* (Aug. 23, 2001), *available at* http://www.idg.net/english/crd_online_744440.html.

provide value added for E-Commerce transactions. Physical retailers conveniently provide key services that are difficult or impossible for pure Internet retailers to match. Physical retailers are set up to accept returns on damaged or unwanted merchandise. They can often exchange the item or fix the problem on the spot. If the consumer is confused, they can explain how to use the product so that it will work properly. If the product is the wrong size or color, the disgruntled consumer can see the replacement immediately. The return or exchange can happen the same day, which is something even overnight shipping can't achieve. The physical store employs a live person to complain to or talk with, a touch that some consumers will value. When warranty work is needed, the physical retailer can handle it in town, without the need for the consumer to find the right box and ship it to a distant location.

In addition, consumers who buy from a clicks-and-bricks retailer increase the likelihood that their local consumer protection laws will apply. The issues of jurisdiction and choice of law for Internet sales have been very controversial.[24] Internet merchants have usually sought "country of origin" treatment, in which the laws of a jurisdiction chosen by the seller would govern. Consumer advocates have usually sought "country of destination" treatment, in which the laws of the consumer's jurisdiction would apply. The point here is that the presence of a physical store is likely to tip the question in the direction of the consumer's jurisdiction. It will be difficult for a clicks-and-bricks company to say that the laws of a distant place should apply when sales by its local retailer would clearly be governed by the local jurisdiction. The consumer, in essence, gets insurance against unfamiliar consumer protection rules.

In short, clicks-and-bricks retailers can provide a panoply of services better than a pure Internet company. (I am not claiming that all of them offer outstanding customer service, just that the physical retailers have important advantages.) The consumer gets all of the advantages of the pure Internet play, because a clicks-and-bricks retailer typically offers the same mail-in service that a pure Internet retailer offers. But the consumer can trust that there is the back-up of help from real people in a real store. And the consumer can know that local laws will almost surely apply, increasing the trustworthiness of the entire transaction.

D. eBay vs. The End of Intermediaries

Credit cards and clicks-and-bricks retailers solve some of the problems of Internet commerce. eBay goes much further. A visit to eBay's *Rules and Safety Overview* shows an entire shadow legal system at work.[25] In my opinion, the phenomenal success of eBay shows both the

24. For my own views, see Peter P. Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INTERNATIONAL LAWYER 991 (1998).

25. *See* http://pages.ebay.com/help/community/index.html .

efficacy of this shadow legal system and the need for much larger amounts of trustwrap than the early prophets of E-Commerce ever dreamed.[26]

eBay did not start out with a shadow legal system. The early dream of eBay was premised on a non-legal "feedback" system. The idea was that sellers and buyers who successfully completed transactions would accumulate positive feedback, and sellers and buyers who performed badly would accumulate negative feedback. This feedback system proved to be a substantial, if incomplete, success. Today on eBay, many sellers have ratings in the dozens, hundreds, and beyond, indicating that they are repeat players who have successfully completed many previous transactions. In this way, buyers can have substantial trust in their first transaction with a seller they have never encountered before, vindicating one of the dreams of the New Economy.

In the pure form of the feedback system there would be no need for backup legal enforcement to ensure trust. A high rating would ensure trust, and a low rating would put the buyer on notice to take extra precautions. In real life, however, eBay has wrapped its transactions in more and more layers of reassuring legal and practical protections. Some of these protections address specific imperfections in the feedback mechanism. For instance, there is now a detailed legal document explaining the circumstances where feedback will be removed from the eBay site. There are also now rules to prevent "shills" from bidding up an auction item artificially.

More generally, eBay has moved far away from the original New Economy dream that distant buyers and sellers could conduct transactions over the Internet without any need for the Old Economy concepts of law and sanctions. To be sure, the *Rules and Safety Overview* continues to voice the community-building spirit that was so important to the initial growth of eBay.[27] The *Overview* also, however, contains buyer and seller protections including the following:

1. Fraud insurance for the buyer, up to $200 per purchase, with a $25 deductible.
2. An escrow service so that buyers can examine the item before payment is made to the seller.

26. Some imperfections in the eBay system are discussed in Clayton P. Gillette, *Reputation and Intermediaries in Electronic Commerce*, 62 LA. L. REV. 1165, 1177–92 (2002). My claim here is that eBay's trustwrap has reduced a large number of risks for remote sellers and buyers, not that it has reached some optimal stasis.

27. eBay's Community Values state:

> (1) We believe people are basically good. (2) We believe everyone has something to contribute. (3) We believe that an honest, open environment can bring out the best in people. (4) We recognize and respect everyone as a unique individual. (5) We encourage you to treat others the way that you want to be treated.

eBay, *Community Values*, *at* http://pages.ebay.com/community/people/values.html.

3. An identification logo that participating sellers can display to show that they have a verified identity.
4. Independent services to appraise or otherwise verify the quality of items.
5. A "verified rights owner" program so that owners of copyright and other intellectual property can work with eBay to remove unlawful items. This program reduces the risk that buyers will be unwittingly buying illegal works.
6. A detailed "systems outage" policy explaining what happens if eBay's service goes down, including credits from eBay to sellers in certain circumstances.
7. A "non-paying bidder" policy, including fees from eBay to sellers who are not paid by buyers.
8. An independent dispute-resolution and mediation service, available at no or modest cost.
9. A program that insures sellers against "charge-backs" from a credit-card company if a credit card is used without authorization.

Going beyond these risk-reducing provisions, eBay transactions are now subject to an entire anti-fraud investigation and enforcement program. eBay now has an extensive investigations policy, with detailed explanations about the list of offenses that it investigates. Sanctions by eBay range from a formal warning to an indefinite suspension of the user's account. The disappointed person in the transaction can seek civil remedies in court. The get-tough attitude toward fraud was underscored in December, 2001 when two U.S. Attorney's offices announced guilty pleas by eBay sellers and another office announced an indictment.[28]

E. E-Commerce and Legal Trustwrap

The point of the discussion thus far is not to deny the many ways that the Internet has allowed new forms of E-Commerce, much as the original prophets foretold. The example of the left-handed corkscrew shows how search engines allow buyers and sellers to find each other through the Net, even for very specialized goods that could not previously have sustained a market. Some pure Internet companies, such as Amazon and Yahoo!, have achieved brand recognition that most physical-world retailers can only imagine. E-cash may yet emerge from the shadows to become a significant part of online purchases (although I tend to doubt it).

28. *See* Press Release, U.S. Department of Justice, Man Pleads Guilty in eBay Fraud Case (Dec. 13, 2001) (*at* http://www.cybercrime.gov/inciongPlea.htm); Press Release, U.S. Department of Justice, Man Pleads Guilty to eBay Auction Fraud (*at* http://www.cybercrime.gov/wildmanPlea.htm); Press Release, U.S. Department of Justice, San Francisco Man Indicted for Selling Fake Derek Jeter and Nomar Garciaparra Baseball Bats on eBay, Harrassing E-mails (*at* http://www.cybercrime.gov/derungsIndict.htm).

The point instead is that a large and increasing fraction of E-Commerce will take place where there is value added to the transaction by one or more forms of trustwrap. Credit cards, clicks-and-bricks retailers, and eBay are just part of the list. Web sites have come up with other ways to reinforce the trustworthiness of the individual transaction. For instance, web transactions using Secure Socket Layers ("SSL") have the familiar lock icon on the screen, and sites that employ SSL technology generally start with "https:" rather than "http:", demonstrating to the surfer that encryption is being used.[29] Some sites offer a fax number or other alternative for buyers who do not wish to give their credit card number over the Internet. Credit card companies, in a trend I strongly support, have experimented with techniques such as one-time credit card numbers, so that the merchant never sees the buyer's permanent credit card number.[30] Each of these techniques adds value to the transaction by visibly demonstrating to the buyer that there is protection against the risks of buying over the Internet.

Within the area of trustwrap, some efforts have fared far better than others. Some companies have tried to establish themselves as "infomediaries," (information intermediaries) where the consumer would store a great deal of personal data with the company.[31] The company would then manage the customer's data, following the privacy rules chosen by the customer and revealing personal information only where the benefits to the customer exceeded any privacy and security risks. Having talked with many of those involved in infomediary ventures, my impression is that none of them has yet found a breakthrough business model. The attempts to build customer trust have foundered on a contradiction—what is so special about the infomediary compared with all the other online companies? That is, why should consumers trust one company to manage all their personal information when the business model is based on consumer distrust of how companies handle their data?

In looking at the successful trustwrap examples and the thus-far unsuccessful infomediary experience, one can tell the conventional E-Commerce story of the importance of market forces in shaping the growth of online sales. On this view, credit card companies, eBay, and clicks-and-bricks retailers have all increased their market share by offering value-added ways of conducting online transactions. Infomediaries and the many dot-bombs have failed the market test when they did not offer enough value to consumers.

29. *See* http://www.modssl.org/docs/2.8/ssl_glossary.html (defining the HyperText Transport Protocol (Secure)).

30. Steve Bass, *Wily Tricks to Thwart Rascally E-Thieves: Keep Your Money—and Your Identity—Safe While You're on the Web*, PC WORLD, Jan. 1, 2002, *available at* 2002 WL 7717478 (discussing one-time credit card numbers).

31. *See*, *e.g.*, JOHN HAGEL III & MARK SINGER, NET WORTH (1999) (the infomediary idea was notably and persuasively advanced by this book).

What is striking to me, however, is the less conventional side of the story. The early enthusiasts for E-Commerce were disdainful of law, and believed that new technology would free sellers and buyers from the constraints of real-space jurisdictions. In each of the success stories, however, there is a prominent role for law and dispute resolution in explaining the success of the type of transaction. Legally binding consumer protections are built into each of the three successful examples: credit cards offer insurance against unauthorized use; local retailers offer legal advantages if the product needs to be exchanged; and eBay now wraps its sales in a long list of consumer protections. This experience suggests that enforceable legal protections play an important role as consumers choose how to conduct their online transactions. The successes in the marketplace turn out to be highly correlated with legal protections. Law, rather than being an enemy of the market, is a facilitator of it.[32]

III. Trustwrap and Internet Privacy Legislation

We now turn from E-Commerce generally to one of the most hotly-debated policy topics affecting E-Commerce, the issue of Internet privacy legislation. Although there are many contested sub-issues concerning Internet privacy, this Part will try to shed light on some specific items. After giving a brief history of U.S. government policy toward Internet privacy, I will focus on reasons to believe that the case for Internet privacy legislation is stronger today than it was during the start-up period of E-Commerce in the 1990s. Self-regulation was particularly apt during the start-up period, with faster response from industry than Administration support for legislation would have secured. Crucially, the start-up period provided important lessons about how to draft privacy legislation in the U.S. setting. In particular, there are compelling reasons to support the somewhat surprising conclusion that legislation should be limited to online collection of personal information, and not extend to all offline collection. As we consider the possibility of Internet privacy legislation, the lessons about trustwrap in Part I can shift our overall sense about the desirability of binding legal rules. Such rules, after all, have been tightly linked with E-Commerce success, and binding privacy rules may well build additional such success.

A. A Brief History of U.S. Government Policy Toward Internet Privacy

Commercial activities were not even permitted on the Internet until 1992.[33] During the mid-1990s the U.S. Department of Commerce and the

32. PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, E-COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 76–89 (1998) (for an earlier discussion of how law can facilitate E-commerce).

33. The Scientific and Advanced Technology Act of 1992, signed into law on October 23, 1992, "subtly modified [the National Science Foundation's] authority to support computer

Federal Trade Commission gradually increased their attention to privacy issues, especially concerning the use and disclosure of information gathered at web sites. Secretary William Daley and the Department of Commerce hosted a conference on the subject in June, 1998.[34] The Clinton Administration announced its basic positions for electronic commerce and on-line privacy in July, 1997 in *A Framework for Global Electronic Commerce*.[35] The Framework announced its support for industry-led, bottom-up efforts to create good practices on the Internet. Until it left office in early 2001, the Clinton Administration continued to encourage self-regulatory efforts for Internet privacy while stating that other approaches might need to be developed if progress did not continue.[36]

The Federal Trade Commission, an independent regulatory agency, was also active on Internet privacy topics.[37] Commissioner Christine Varney was dubbed "the Commissioner from Cyberspace" for her attention to Internet privacy and related issues in 1996 and 1997.[38] Chairman Robert Pitofsky and other Commissioners devoted considerable attention to privacy issues. In June, 1998 the FTC issued its first survey of Internet privacy practices.[39] That August the FTC settled its first enforcement action in the area, with the action brought for "unfair and deceptive trade practices" under Section 5 of the Federal Trade Commission Act.[40] For the next two years the FTC continued to bring enforcement actions, issue annual reports about Internet privacy, and take other actions in the Internet

networks that are not limited to research and education." NATIONAL SCIENCE FOUNDATION, OFFICE OF INSPECTOR GENERAL, REVIEW OF NSFNET, March 23, 1993 (citing 42 U.S.C. § 1862(g)). This change was one important legal step toward development of commercial activity over what is now called the Internet.

34. Public Meeting to Explore Privacy Issues Related to Electronic Commerce, 63 Fed. Reg. 33,355 (June 18, 1998). For further information, see Commerce Secretary William Daley, Opening comments at the Electronic Privacy Summit (June 23, 1998) (*available at* http://www.ntia.doc.gov/ntiahome/press/623pri.htm; http://www.ntia.doc.gov/ntiahome/privacy/confino/agenda.htm).

35. The White House, *A Framework for Global Electronic Commerce*, July 1, 1997, *available at* http://www.ta.doc.gov/digeconomy/framewrk.htm.

36. For an overview of the Clinton Administration position *see* U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, TOWARD DIGITAL EQUALITY: SECOND ANNUAL REPORT 36–39 (1999), *available at* http://www.ta.doc.gov/digeconomy/ecomrce.pdf.

37. For an insightful academic account of the FTC's role, see Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041 (2000).

38. Kathleen Murphy, *Newsmaker: Becky Burr*, INTERNET WORLD, (Aug. 24, 1998) ("Burr, who was then working as a Washington, D.C. attorney, told Varney, 'You could be the commissioner from cyberspace,' planting the seed of an idea that later fully flowered'").

39. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS, (1998) *available at* http://www.ftc.gov/reports/privacy3/index.htm.

40. The settlement with the web site Geocities, for alleged violation of its privacy promises with respect to both children's and adults' information, is available at http://www.ftc.gov/opa/1998/9808/geocitie.htm.

privacy area.[41] In the spring of 2000, a 3-2 majority in the Federal Trade Commission announced support for Internet privacy legislation.[42]

During this period, from 1997 to 2000, privacy advocates sharply criticized the Clinton Administration for its support of self-regulation and its failure to seek broad Internet privacy legislation. These criticisms were made on a number of overlapping grounds. Some view privacy as a fundamental human right that must be protected by law, as recognized for instance in Article 8 of the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms.[43] That Convention has been signed by forty-three European states, showing widespread support for a human rights approach to privacy that contrasts sharply with the "self-regulatory" approach existing in the United States.[44]

Some critics of the U.S. position emphasized the strict privacy requirements under the European Union Data Protection Directive. As countries around the world have increasingly harmonized their privacy regimes, the United States has become increasingly anomalous in failing to have Internet privacy protections and promulgate comprehensive privacy laws more generally.[45]

Other critics placed more emphasis on domestic U.S. arguments. For instance, Internet privacy violations implicate First Amendment values if individuals are tracked as they read at different web sites.[46] The collection and sale of data treats individuals as commodities, an approach at odds with individual autonomy.[47] In a more instrumental mode, stronger privacy laws

41. *See generally* http://www.ftc.gov/privacy/index.html (linking to FTC privacy policy and enforcement documents).

42. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A FEDERAL TRADE COMMISSION REPORT TO CONGRESS (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

43. *See* Council of Europe, *Complete List of the Council of Europe's Treaties*, *at* http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm. Article 8 provides:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others.

Id.

44. For an extensive discussion of the case law that has developed under Article 8, *see* Daniel J. Solove & Marc Rotenberg, Information Privacy Law 4–24, Ch. 5 (2003) (prepublication draft).

45. COLIN BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1992); Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315 (2000).

46. Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996).

47. *See, e.g.,* Margaret J. Radin, John A. Rothchild, & Gregory M. Silverman, *Internet Commerce: The Emerging Legal Framework*, 619–23 (2002) (citing sources on commodification and privacy).

might promote confidence in Internet commerce, with benefits both for surfers' privacy and companies' sales.[48]

Critics' concerns about Internet privacy invasions were exacerbated by their distress about the Clinton Administration's opposition to the use of strong encryption.[49] Until September, 1999, when the Administration shifted position,[50] critics were concerned about a privacy double-whammy—no technological measures to protect privacy (because of the encryption limits) and no legal measures to protect privacy (because of the lack of U.S. Internet privacy rules). Since the 1999 announcement of support for strong encryption, there has not been any significant legislation or executive action to reinstate encryption controls.

The next section of this Article will assess the effects of public policy during this start-up period of the Internet. Since the Bush Administration took office in 2001, the governmental leader on the issue of Internet privacy has been the new FTC Chairman, Timothy Muris. Chairman Muris set forth his privacy agenda in a speech in Cleveland in October, 2001.[51] Chairman Muris declined to support Internet privacy legislation. Instead, he supported a national "Do Not Call" list for telemarketing and pledged to increase FTC privacy enforcement efforts.[52] At the time of this writing in early 2003, FTC policy in this area has largely followed the agenda set forth in Chairman Muris' speech.[53]

48. For one examination of the argument that privacy legislation will promote E-commerce, *see* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE, 76–89 (1998).

49. For one set of materials about the encryption controversy, see Center for Democracy & Technology, *at* http://www.cdt.org/crypto.

50. My own statements at the White House event in September, 1999 recognized the importance of encryption to Internet privacy:

> I am here to underscore that today's announcement reflects the Clinton Administration's full support for the use of encryption and other new technologies to provide privacy and security to law-abiding citizens in the digital age. . . . Especially for open networks such as the Internet, encryption is needed to make sure that the intended recipients can read a message, but that hackers and other third parties cannot.

Chief Counselor for Privacy, Peter Swire, Statements at a White House Press Briefing (Sept. 16, 1999) (*available at* http://www.privacy2000.org/presidential.htm).

51. *See* Timothy J. Muris, Protecting Consumers' Privacy: 2002 and Beyond, Address before the Privacy 2001 Conference (Oct. 4, 2001) *(at* http://www.ftc.gov/speeches/muris/privisp1002.htm).

52. *Id*.

53. For the final amended rule on the "Do Not Call" list, see 68 Fed. Reg. 4580 (Jan. 29, 2003). For an updated list of news releases and links on FTC privacy enforcement actions, see http://www.ftc.gov/privacy/index.html.

B. The Case for Internet Privacy Legislation Now That the Start-Up Period is Over

Roughly speaking, the Internet was mostly in a pre-commerce period through about 1996. The period from about 1996 until the end of the Internet bubble in 2001 might be called the "start-up period," both for the many individual start-up companies and for E-Commerce as a whole. The period since 2001 has been one of a more mature market, with the exit of many E-Commerce companies that lacked a successful business model.

The discussion in this Part makes the case for different approaches to Internet privacy protection during the start-up period and afterward. Roughly speaking, the benefits of self-regulation and the costs of legislation were likely to be especially high during the start-up period. The balance shifts more toward the benefits of legislation after the end of the start-up period.

(1) The Relative Success of Self-Regulation During the Start-Up Period.

Suppose you are a policy-maker considering the possibility of Internet privacy legislation early in the start-up period, in 1996 or 1997. Suppose, to make a realistic assumption, your goal is to encourage E-Commerce while promoting consumer confidence and protecting individual privacy. You wish to improve commercial practice quickly while holding down compliance costs. In the eyes of this policy-maker, acting in good faith, how would you weigh the choice between self-regulation and legislation for Internet privacy?

At the risk of sounding naïve, this description of a good-faith policy-maker actually matches well with my own experience of discussions within the Clinton Administration about Internet privacy.[54] The essential policy was to support self-regulation but with an understanding that the Administration would support legislation if industry did not make progress quickly enough.

I believe that this policy in fact succeeded quite well during the start-up period. There was a rapid increase in privacy policies during this period, as shown by the annual FTC studies. The 1998 study found that only fourteen percent of commercial web sites had any privacy statement or notice.[55] That number rose to sixty-six percent in 1999[56] and eighty-eight

54. The substantive discussions about Internet privacy took place in a context where the chief political forces operated largely in the same direction as the good-faith policy discussion. The Clinton Administration clearly favored developing electronic commerce. By the late 1990s it also clearly favored finding ways to protect individual privacy while holding down compliance costs. *See* Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263, 1277–82 (2002) (discussing the politics of privacy legislation in the late 1990s).

55. *Supra* note 42.

56. SELF-REGULATION AND PRIVACY ONLINE: A FEDERAL TRADE COMMISSION REPORT TO CONGRESS 7 (July, 1999), *at* http://www.ftc.gov/os/1999/9907/privacy99.pdf.

percent in 2000.[57] My view of these numbers is that the Administration's credible threat to seek legislation, if industry did not respond, led to a remarkable response by industry. If the Administration had instead ignored the issue of Internet privacy, then there would have been a much slower response from industry. If the Administration had instead pushed for early legislation, then I think many web sites would have delayed implementing a privacy policy until they knew the final form of legislation. And that legislation, in light of the opposition of most corporations and their political influence, would quite possibly never have arrived.[58]

Another advantage of the self-regulation-plus-Administration-pressure approach was the blossoming of policy and technical innovations for Internet privacy. Major companies competed for favorable press attention about their privacy innovations. For instance, IBM announced that it would only buy web advertisements from sites that posted privacy policies[59] and Microsoft used its small-business web sites to help its clients develop their own privacy policies.[60] The Direct Marketing Association, long engaged in battles on privacy legislation, adopted the policy and practice in 1999 that members would be expelled unless they posted privacy policies that included an opt-out for third parties.[61] On the technical side, advocacy groups such as the Center for Democracy and Technology ("CDT") worked with industry to develop the Platform for Privacy Preferences ("P3P"), which its proponents hoped would create an

57. *Supra* note 42.

58. The difficulty of passing privacy legislation during this period was illustrated by Congress' inability to pass medical privacy legislation. *See infra* note 68 (providing details of medical privacy rules). As the Health Insurance Portability and Accountability Act was enacted in 1996 ("HIPAA"), Congress gave itself until August, 1999 to enact legislation, or else the U.S. Department of Health and Human Services ("HHS") would gain the power to draft the regulations. Passing medical privacy legislation might have seemed an easier task than passing Internet privacy legislation, both because there was a greater consensus that legislation was needed for sensitive medical records and because the Republican Congress did not favor granting this sort of discretion to the Clinton Administration. Nonetheless, no medical privacy legislation during this period even passed a Congressional subcommittee. The chances for delay in Internet privacy legislation, even if there had been Administration support, were thus very high. *See* Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, *supra* note 54 (discussing political history of the period).

59. Carol Emert, *IBM Gets Tough About Web Privacy/Post Guidelines or Lose Our Ads, Company Says*, S.F. CHRON., Apr. 1, 1999, at B1.

60. Mark Harrington, *Hard-line on Online Privacy: Microsoft Threatens to Pull Ads from Sites without Disclosures*, NEWSDAY, June 24, 1999, at A51.

61. The Direct Marketing Association's Privacy Policy Compliance Guide can be found at http://www.the-dma.org/privacy/privacypromise.shtml. On membership expulsions, see Amanda Beeler, *DMA: Members Must Keep Privacy Promise: Columbia University's Graduate School of Business Faces Expulsion*, ADVERTISING AGE, Nov. 29, 1999, *available at* 1999 WL 26899912.

automatic software mechanism for matching the privacy preferences of surfers with the policies of web sites.[62]

Perhaps the most important innovation, however, was the creation of the so-called web seal programs such as TRUSTe[63] and BBBOnline.[64] The idea of the web seal was that a web site, which was possibly unknown and untrusted by the user, could sign up with the web seal program as a private-sector enforcement agency. The web seal program would only permit its seal to be displayed on sites that met minimum criteria. Surfers could complain to the web seal program about any privacy problem, and the web seal program would act as enforcer, up to the sanctions of withdrawing the seal and referring the case to public agencies.

The web seal programs are especially important, in my view, because they created a plausible case that privacy enforcement would actually be more effective with that sort of self-regulatory program than under a pure legislative approach. The presence of web seal programs does not deprive government agencies of the power to bring enforcement actions against deceptive trade practices; instead, the web seal programs become a supplement to government agencies. They are a source of information for companies seeking guidance and a first line of enforcement for small problems or for problems that can be readily resolved. Perhaps the greatest advantage of the seal programs is that they are scalable. The staffs of TRUSTe and BBBOnline can grow quickly as the number of participating websites increases. By contrast, my experience in the U.S. Office of Management and Budget teaches that the same sort of staff increase would simply not be politically possible at the Federal Trade Commission or other enforcement agencies.[65]

62. For the home page of P3P, developed under the auspices of the World Wide Web Consortium ("W3C"), see http://www.w3.org/P3P. A CDT view on P3P is available at http://www.cdt.org/privacy/pet/p3pprivacy.shtml. For a critique of the P3P approach, see http://www.junkbusters.com/standards.html (open letter dated Sept. 13, 1999 by Jason Catlett explaining deficiencies of P3P).

63. For a more skeptical view of enforcement by the web seal program, see Marc Rotenberg, Testimony and Statement for the Record, Hearing on S. 809, Online Privacy Protection Act of 1999 Before the Subcommittee on Communications of the Committee of Commerce, Science, and Transportation (July 27, 1999) (*available at* http://www.epic.org/privacy/internet/EPIC_testimony_799.pdf, at 64–65)

64. *See* http://www.bbbonline.org.

65. The difficulties in securing enforcement funding for the Securities and Exchange Commission reinforces this point. SEC enforcement staffing actually fell in the late 1990s, despite efforts by the Clinton Administration to increase the funding. Sandra Sugawara, *With More to Oversee, SEC Seeks Additional Money and Staff*, WASH. POST, Feb. 8, 2000, at E3. Even after the Enron and other scandals of 2001 and 2002, funding for enforcement has hit significant snags. Paul Krugman, *Business as Usual*, N.Y. TIMES, Oct. 22, 2002, at A31 (discussing continuing opposition to SEC enforcement funding).

(2)What We've Learned from the Privacy Legislation of the Late 1990s.

At the level of practice, this history of the late 1990s for Internet privacy provides evidence that support for self-regulation, combined with the credible threat of legislation, resulted in a rapid spread of privacy policies and substantial experimentation on new approaches for diffusing privacy policies and enforcement into the world of E-Commerce. Meanwhile, there was a rapid spread of binding privacy rules in the United States for the most sensitive categories of personal information held in the private sector. My thesis here is that legislating first for this sensitive information was a sound strategy, for both political and substantive reasons.

The most important of the binding rules came in three categories: (1) information collected over the Internet about children under the age of thirteen, under the Children's Online Privacy Protection Act of 1998 ("COPPA");[66] (2) financial information, under the Gramm-Leach-Bliley Act of 1999 ("GLB");[67] and (3) medical records, under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the privacy regulation first issued in final form in 2000.[68] The political rationale for moving first on this sensitive data is easy enough to see—it was easier to get political consensus that there should be binding, legal protections for the most sensitive types of information, and there was general agreement that children's, financial, and medical records qualified as sensitive. By contrast, there was less consensus that information collected by web sites over the Internet was inherently sensitive.

On the substance of good legislation, I highlight four lessons from the experience with enacting and complying with laws protecting the privacy of children's, financial, and medical information: (1) the need for well-crafted exceptions; (2) the importance of good notices that are understandable to recipients; (3) the limits of technological fixes; and (4) the importance of carefully defining the jurisdictional trigger for the regulatory regime.

In drafting exceptions, the challenge is how to permit desirable data flows while effectively limiting flows that risk harm to individual privacy. In a 1998 book, my co-author and I criticized the Data Protection Directive in the European Union for not having a number of significant, necessary

66. 15 U.S.C. §§ 6501–06 (2000).

67. 15 U.S.C. §§ 6801–09 (2000).

68. The privacy regulation was first issued in final form at 65 Fed. Reg. 82,462 (Dec. 28, 2000). It now appears, as modified, at 45 C.F.R. §§ 160, 164 (2001), with relevant materials provided by HHS at http://www.hhs.gov/ocr/hipaa. Under the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1997), Congress stated that HHS should issue the regulation if Congress did not enact medical privacy legislation by August, 1999. When Congress did not do so, HHS went forward with the regulation. *See* Peter P. Swire & Lauren B. Steinfeld, *Security and Privacy After September 11: The Health Care Example*, 86 MINN. L. REV. 1515, 1524–26 (discussing privacy rule history).

exceptions. For example, it was unclear under the Directive on what basis accountants could audit records of a company containing personal information.[69] Similarly, it was unclear whether lawyers performing due diligence could examine a company's records in preparation for a merger.[70] These sorts of needed exceptions were explicitly included in the GLB and HIPAA privacy rules.[71] Indeed, the Clinton Administration did not call for any change in the GLB exceptions when it proposed additional financial privacy protections in 2000.[72]

Creating exceptions should not be seen, even by privacy advocates, as "caving in" to industry. It is good public policy, in my view, to continue to have effective audits and due diligence before mergers. Safeguards can be and have been included for these exceptions, so that the auditors or lawyers remain under confidentiality requirements that prohibit re-disclosure.[73] In addition, the lack of appropriate exceptions can backfire and create political momentum that can kill a privacy regime. One notable example was a medical privacy law in Maine that had the effect of making it difficult or impossible for florists to deliver flowers to patients in the hospital.[74] The immediate effect was to prompt repeal of the entire privacy law.[75] The hope in future privacy legislation is that we will all learn from this experience which exceptions are needed.

On the importance of good notices, the legalistic notices under GLB were widely criticized as too difficult to understand and not effective at letting customers compare privacy policies.[76] Although I have written elsewhere about some surprising virtues of those notices,[77] we should

69. SWIRE & LITAN, *supra* note 32, at 94–97.

70. *Id*. at 109–12.

71. In the medical privacy rule, both auditing and due diligence are specifically included as permissible "health care operations" in 45 C.F.R. § 164.501 (2002). Under GLB, auditing and due diligence are included as exceptions under 15 U.S.C. § 6802(e) (2000).

72. The Clinton Administration proposal was introduced in Congress as the Consumer Financial Privacy Act, H.R. 4380, 106th Cong. (2000). For a discussion of the bill, see Swire, *supra* note 54, at 1292–93. The bill did contain a new exception for certain customer service activities, but this exception was included only because of the expanded coverage of the proposed bill, and not due to disagreement with the exceptions contained in GLB itself.

73. Under the medical privacy rule, auditors and those performing due diligence will be under the confidentiality requirements that apply to "business associates." 45 C.F.R. § 164.504(e) (2002). Similar limits apply under the re-use provision of GLB. 15 U.S.C. § 6803(c).

74. The problem for florists was that they needed prior patient consent to learn the number of the hospital room, but the patients were usually receiving the flowers as a gift and so had not given prior consent. *See* Amy Goldstein, *Long Reach into Patients' Privacy; New Uses of Data Illustrate Potential Benefits, Hazards*, WASH. POST, Aug. 23, 1999, at A1 (strict Maine medical privacy law repealed two weeks after taking effect after complaints by florists and other groups).

75. *Id*.

76. *See* Swire, *supra* note 54, at 1313–21 (discussing criticisms of GLB notices and possible solutions).

77. *Id*. (GLB notices forced financial institutions to examine their internal practices and provide a detailed roadmap for accountability in data handling practices).

obviously learn how to do better in the future. Fortunately, HHS has encouraged a more user-friendly approach to notices in the medical privacy rule. In response to public comments, HHS has specifically encouraged a "layered notice" approach, with a short plain-language notice on top and a more detailed notice as a second layer.[78] The plain-language notice addresses the goal of communicating clearly with the recipient. The detailed notice addresses the goal of ensuring that the organization has examined its own privacy practices and has created an enforceable set of privacy promises. In future legislation, we should avoid the mistakes of GLB and ensure that layered notices are either encouraged or required.

As for the limits of technological fixes, we now have some experience in assessing the heady hopes of the Internet start-up period. One lesson has been the limited usefulness of the technology of P3P as a substitute for legal and institutional privacy protections. While P3P was under construction in 1999 and 2000, some proponents argued that legislation was unnecessary because the P3P software would give users' their desired level of privacy.[79] At the time of this writing in 2003, P3P seems far less than a "magic bullet." Even many of the leading web sites are not P3P readable, and the standard version of P3P offers much narrower privacy protections than proponents had originally hoped.[80]

There have been similar disappointments with the "digital certificates" that the FTC hoped would be an important part of COPPA.[81] In its 1999 rule for children's web sites, the FTC used a so-called "sliding scale" approach that used insecure e-mails to get permission for certain uses of children's information.[82] The Commission believed that, "with advances in technology, companies will soon be able to use more reliable verifiable

78. For one such public comment, see Peter P. Swire, Letter to U.S. Department of Health and Human Services Office of Civil Rights, Apr. 26, 2002 (describing advantages of layered notices), *at* http://www.peterswire.net/CommentsShortNotices.doc. HHS responded: "Covered entities, while encouraged to use a layered notice, are not required to do so." 67 Fed. Reg. 53,182, 53,243 (Aug. 14, 2002).

79. *See* Dissenting Statement of Commissioner Orson Swindle, FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ONLINE ENVIRONMENT, at 17, 19, 20 (2000) (arguing that the development P3P made Internet privacy legislation less desirable), *available at* http://www.ftc.gov/reports/privacy2000/swindledissent.pdf. The full FTC report is available at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

80. As of August, 2002, one report found that 25% of the top 100 domains and 17% of the top 500 domains were P3P enabled. Ernst & Young, *P3P Dashboard Report (2002)*, *at* http://www.ey.com/global/download.nsf/US/P3P_Dashboard_September_2002/$file/E&YP3PDashboardSeptember2002.pdf.

81. In brief, "digital certificates use mathematics or other means to help prove that a particular person has sent a document electronically and to show that the document has not been changed in transit." SWIRE & LITAN, *supra* note 32, at 205; *see also* A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49 (1996) (analyzing law of certificate authorities and digital certificates).

82. 16 C.F.R. § 312.5(b)(1) (2000).

electronic methods in all of their transactions."[83] The Commission specifically believed that digital certificates would shortly be used widely by parents, and so allowed until April, 2002 for digital certificates to become the standard way for parents to consent to uses of their children's personal information.[84] These predictions of the Internet start-up period, however, did not come to fruition. The FTC has extended the date for stronger forms of electronic verification until April, 2005,[85] and it is open to serious doubt whether most parents will be using digital certificates by that date.[86] In my view, the experience with P3P and digital signatures suggests the risks of relying on technology to provide a strong substitute for legal and institutional protections of personal information.

(3) The Online/Offline Question

A lesson from recent privacy legislation, which deserves increased attention, is the importance of choosing a good jurisdictional trigger. For organizations complying with HIPAA, GLB, or other privacy laws, the initial and most significant question is whether they are covered by the law.[87] Covered organizations are required to comply with a full range of legal requirements, but other organizations are not. My own view, which I have recently explained in some detail,[88] is that any forthcoming U.S. privacy legislation should apply to information collected online, but should not apply to all information collected offline.

This proposed different treatment of offline and online data strikes some as unfair.[89] A vice president of Amazon.com, for instance, writes: "The fact that a consumer last year purchased both a pair of blue jeans and a cordless drill is not affected by whether this fact was learned 'online' (e.g., through a website purchase) or 'offline' (e.g., through an in-store credit card transaction or mail-in warranty registration card)."[90] In response, I believe that there are significant differences in consumer concerns in the two settings. The very act of using the Internet reinforces

83. 64 Fed. Reg. 59,888, 59,902 (Oct. 29, 1999).

84. *Id*.

85. 67 Fed. Reg. 18,818 (Apr. 17, 2002).

86. On the slow adoption of digital certificates, see Jane K. Winn, *The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce*, 37 IDAHO L. REV. 353 (2001).

87. Under HIPAA, the question is whether an organization is a "covered entity", as defined in 45 C.F.R. § 160.103 (2002). "Covered entities" include health care providers, health plans, and health care clearinghouses. *Id.* Under GLB, the question is whether an organization is a financial institution, as defined in 12 U.S.C. §1843(k) (2000).

88. Peter P. Swire, *The Online/Offline Question*, *in* CONSIDERING CONSUMER PRIVACY: A RESOURCE FOR POLICYMAKERS AND PRACTITIONERS 72 (Paula Breuning, ed., 2002), *available at* http://www.cdt.org/privacy/ccp/onlineoffline1.pdf.

89. Paul Misener, *Parity in Consumer Information Collection*, *in* CONSIDERING CONSUMER PRIVACY: A RESOURCE FOR POLICYMAKERS AND PRACTITIONERS 76.

90. *Id*.

the concern for consumers that their personal data may spread quickly and in unforeseen ways. In addition, websites can and do collect far greater detail about consumer actions than physical retailers—an online bookstore learns not only which book an individual purchases, but also every other book that the individual even looks at in the bookstore site.[91]

More importantly, legislation targeted at commercial information collected online creates a bright line concerning who is covered by the regulatory regime. My views here are shaped by my experience with the European Union Directive on Data Protection, whose text applies to an enormous array of online and offline data.[92] In the course of doing research on the Directive, my co-author and I noticed that its text would quite possibly make it unlawful for many business travelers to carry laptops on a plane from the European Union to the United States. In answer to our questions, E.U. officials were split on whether the Directive would indeed prohibit such transfers of personal data.[93] On a practical level, everyone agreed that enforcement against most business travelers was unthinkable. The problem remained, however, "because of the gap between the apparent prohibition in law and the apparent permissibility in practice."[94]

The E.U. solution has been to leave interpretation, for laptops and other issues, to the discretion of enforcement officials.[95] No matter the quality of the officials, I continue to have serious concerns about an approach that depends on overbroad legislation and merciful enforcement. Overbroad legislation, if actually put into practice, leads to needless costs and burdens by those who should not be included. Overbroad legislation fails to provide clear notice of what is prohibited and creates the risk of arbitrary and discriminatory enforcement. Moreover, if everyone comes to perceive the legislation as overbroad and unenforceable, the entire law can become a dead letter. The achievable good purposes of the legislation can be lost, because the law went too far.

Returning to the issue of offline and online, this experience with the overbroad E.U. Directive makes me highly skeptical of legislation that would apply to all commercial offline and online information collected in the United States. I simply do not think it is plausible that every babysitter and every teenager cutting neighborhood lawns will be required to hand out a privacy notice before doing the babysitting or cutting the grass.[96] The

91. For further discussion, see Swire, *The Online/Offline Question*, *supra* note 88.

92. Article 3 reads in part: "The Directive shall apply to the processing of personal data wholly or party by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system." BENNETT, *supra* note 45, at Art. 3. There is an exception for some non-commercial activities, but only "by a natural person in the course of a purely personal or household activity." *Id*.

93. On the issue of laptops, *see* SWIRE & LITAN, *supra* note 32, at 40–44.

94. *Id*. at 73.

95. For discussion of the problems with this discretionary approach, see *id*. at 45–49.

96. Babysitting or cutting lawns for money would be a commercial activity. If the teenager kept notes about the name of each customer, when to go to the house, and how much had been

vague and limitless application of an "all commercial data" law would create great practical problems in determining who was within the scope of the legislation. The ease of creating horror stories, such as my babysitting or grass-cutting examples, would make any such law a subject of ridicule and likely repeal. More likely, an insistence that a privacy law apply to all offline data will ensure that such a law will never be enacted.

At the same time, an online-only law can address the bulk of the privacy issues. Such a law could apply to "mixed databases"—data that combined information from online and offline sources. The Federal Trade Commission has devoted increasing attention to offline data practices, and it is quite possibly a deceptive practice to use information offline in ways that are contrary to the online privacy policy.[97] In this way, only companies that rigidly separate their online and offline databases and sacrifice the ability to participate effectively in E-Commerce would remain outside the scope of the online privacy protections. This approach would provide a smooth path toward widespread privacy protection in the offline world. It would have the greatest impact on the largest and most important databases, which pose the greatest privacy risks and which would inevitably be used in connection with online commerce. At the same time, those who assemble smaller collections of data in the offline world would not need to worry that they had unexpectedly crossed the line into compliance with a federal regulatory scheme.[98]

III. Conclusion: Trustwrap and the Role of Law in Encouraging E-Commerce and Internet Privacy

Compared to the Internet start-up period of the 1990s, we now have the luxury of time and perspective in assessing the role of law in encouraging E-Commerce and Internet privacy. eBay began as a norms-based system that depended on customer feedback rather than legal guarantees. eBay today, however, offers a long list of legal guarantees,

paid, this sort of personal information would presumably come under a law that applied to commercial offline activity. If the teenager told a friend that the family was looking for more help, then that disclosure would presumably be subject to an opt-out or opt-in requirement.

97. *See* Tony Kontzer, *FTC Spreading Its Privacy Net: The Federal Trade Commission Is Making It Clear that Consumer Data Should be Protected Whether It's Collected Online or Offline*, INFORMATIONWEEK, Dec. 11, 2001 (comment by Federal Trade Commission's Director of the Consumer Protection Bureau that a company's online privacy policies apply equally to its offline collection and use of data, unless the online privacy policy contains language limiting the online privacy policy's application to the online collection of data).

98. The risk of over-breadth is much greater in the offline world than the online. For the online world, part of creating a commercial presence on the Internet would be posting a privacy policy. Such policies are already very common, and legislation would simply ensure that this requirement would become of the standard start-up list, along with items such as handling credit card payments. In addition, the marginal cost online of providing a privacy policy is approximately zero, in contrast to the printing and distribution costs of notices in the offline world.

backed up by criminal enforcement for fraud cases. Credit cards began on the Internet with the disadvantage that they would not work for anonymous transactions—the credit card issuer keeps a list of every customer purchase. Credit cards today dominate E-Cash, however, in large part likely because of the statutory $50 limit on unauthorized purchases and the statutory guarantees of dispute resolution if a merchant charges for non-delivered goods. Clicks-and-bricks retailers gained market share in part because of their brand recognition and the practical advantages of offering returns and other services in local stores. These retailers also, however, are almost certainly subject to the detailed consumer protection laws that exist in most jurisdictions.

In a landscape littered with dot-com failures, three examples stand out as areas of flourishing growth. These three examples, with the visible demonstrations of trust that they build into online transactions, should temper anyone's reflexive opinion that statutory and related legal protections will harm E-Commerce. In saying this, I am of course not saying that all statutes are good and all efforts at self-regulation are bad. Any law professor or any businessperson subjected to a regulatory scheme can think of numerous bad statutes. What I am saying instead is that we should notice that major successes of E-Commerce have been accompanied by binding legal protections. Which legal protections are appropriate, in which settings, is then a matter for careful study.

On the topic of Internet privacy, we now have the opportunity to benefit from careful study of the past decade. What is the most effective form of trustwrap on this contentious issue of handling personal information on the Internet? A principle theme in this Article has been the difference between the start-up period of the Internet, which lasted until the NASDAQ bubble burst in 2001, and the subsequent period. I have explained my reasons for believing that self-regulation, accompanied by a credible threat of legislation, was a sound strategy for improving Internet privacy in the start-up period. The argument for legislation is stronger today. Legislators and regulators have developed considerable expertise from the privacy regimes for children's, financial, and medical privacy. We know much more about which exceptions are needed. We know how to write better consumer notices. We have given room for technological privacy measures to do the job. They have performed far less well than proponents had expected, thus strengthening the case for legal and institutional privacy protections. We have also learned, in my view, that privacy legislation targeted at online practices is likely to be politically and substantively superior to legislation that purports to apply to all commercial offline activity as well.

Based on my own experience in the Internet privacy debates throughout this time, I believe the case for legislation is significantly stronger now than it was in the late 1990s. Compared to the relative inexperience and confusion of the mid-1990s, there is far more consensus

today about what constitutes good practices for commercial sites. The risk of badly-drafted legislation is lower due to our experience with other privacy regimes. Many commercial sites have already implemented good practices, and other sites can readily implement such practices as well.

This one article cannot address every nuance of the Internet privacy debates.[99] It aims, instead, to show reasons based on experience why legislation is more likely to inspire trust, while avoiding excessive costs, than many in the U.S. privacy debates have supposed. Binding legal protections have been associated with the growth areas of E-Commerce. Providing binding legal protections for Internet privacy—creating statutory trustwrap to match the $50 rule for credit cards—may well contribute to growth while also matching the wishes of a vast number of those who use the Internet.

99. For a current compendium of essays on the key issues, see CONSIDERING CONSUMER PRIVACY, *supra* note 88.