

---

# PART 1:

---

## **Building Trust in Online Negotiations: A Cross-Cultural Approach to International Business in the Twenty-First Century**



---

# CHAPTER I

## Trust and the Internet

*Tamar Frankel*

BOSTON UNIVERSITY SCHOOL OF LAW  
BOSTON, MASSACHUSETTS

### 1. Introduction<sup>1</sup>

While the Internet is a wonderful innovation that encourages trade, many buyers hesitate to use it because they lack trust in the offers on the Internet. “Trust has become a serious stumbling block to developing e-commerce (electronic commerce).”<sup>2</sup>

This discussion is framed in terms of the benefits, costs, and risks of trusting relationships, and the mechanisms that reduce the costs and risks of trusting. What is trusting? Trusting is a relationship<sup>3</sup> among individuals, entities, and institutions, involving (i) a reasonable belief, supported by an acceptable level of verification,<sup>4</sup> that (ii) another party is telling the truth and will abide by its promises.<sup>5</sup> Trust in persons, institutions, and society is not blind; it emerges from

---

<sup>1</sup> This chapter reprints and adapts significant portions of the following article: Tamar Frankel, *Trusting and Non-Trusting on the Internet*, 81 B.U. L. REV. 457. Some copied materials are not in quotes. The author thanks Boston University Law Review for permission to use the article. Many thanks to William Hecker, Esq. for his review, and David Z. Roiter for his extensive and meticulous research contribution to this chapter.

<sup>2</sup> Ye Diana Wang & Henry H. Emurian, *An Overview of Online Trust: Concepts, Elements, and Implications*, 21 COMPUTERS HUM. BEHAV. 105, 121 (2005). See also Sonja Grabner-Kraeuter, *The Role of Consumers’ Trust in Online-Shopping*, 39 J. BUS. ETHICS 43 (2002).

<sup>3</sup> Trust is defined as expected behavior of the other party and readiness to risk disappointment. The issue of trusting can be raised only in the context of interaction with others. See Rajeev Bhattacharya, Timothy M. Devinney & Madan M. Pillutla, *A Formal Model of Trust Based on Outcomes*, 23 ACAD. MGMT. REV. 459, 460 (1998).

<sup>4</sup> Some authors add an emotional bond or internal moral drive as a bridge from evidence to belief. These elements have merit, but relate less directly to e-commerce than they do to social interaction. Scholars have defined risk of trusting as “asymmetrical information among the parties,” in that the risk of trusting relates to the cost of obtaining the relevant information and the degree of assurance that the information is true. See TRUDY GOVIER, *SOCIAL TRUST AND HUMAN COMMUNITIES* 24 (1997).

<sup>5</sup> There are numerous definitions of trust. Bhattacharya, et al. (*supra* note 3, at 460) survey various definitions, including dictionary definitions of trust and distinguishing between cognitive, emotional, and behavioral components of trust.

and is strengthened by proof.<sup>6</sup> Gullibility, hope, and faith are relatives of trusting,<sup>7</sup> but reflect different degrees of the parties' requirements for verification.<sup>8</sup> Reasonable belief should depend on the context of the relationship. Reliability in love does not necessarily mean reliability in business relationships, and vice versa. The scope of deeper trust, such as trust in a doctor, lawyer, or priest, is usually limited to particular areas of knowledge or brands of honesty. Reasonable belief can be established by verifying the trustworthiness of the other party or, as an alternative to trust, by resorting to other sources of information, usually depending on the relative costs.

Cultural norms shape the parameters of reasonableness of the belief. Reasonableness may differ depending on whether the social norm is lying, frankness, or vagueness of the other parties' statements and promises as well as the acceptable social norms.<sup>9</sup> The law both affects and is affected by these norms. Moreover, trusting is a reflexive and reciprocal relationship.<sup>10</sup> Trusting often creates pressure on trusted persons to meet the expectations of the trusting parties. Signals of mistrust may breed mistrust.<sup>11</sup> Dirty tricks invite reciprocal dirty tricks. As compared to verification cost in real space, verification cost on the Internet is higher.<sup>12</sup>

<sup>6</sup> See GOVIER, *supra* note 4, at 153. See also Ann Marie Zak et al., *Assessments of Trust in Intimate Relationships and Self-Perception Process*, 138 J. SOC. PSYCHOL. 217, 225 (1998) (finding that the trusting behavior of the participants in the experiments is often self-fulfilling and explaining that blind trust is usually a product of one's self-perception). Trustworthy people are more likely to blindly trust others. See *id.*

<sup>7</sup> Trusting does not mean believing all unverified representations; rather, it means believing unverified representations when it is not unreasonable to do so. "[B]elieving when most people of the same social group would consider belief naive and foolish" qualifies as gullibility. See Julian B. Rotter, *Interpersonal Trust, Trustworthiness, and Gullibility*, 35 AM. PSYCHOLOGIST 1, 4 (1980).

<sup>8</sup> Gullibility is an unreasonable belief, while hope involves a strong component of wishing for a future event. See GOVIER, *supra* note 4, at 14, for an elaboration on the distinctions and similarities between faith and trust.

<sup>9</sup> "Do it yourself" verification is not always less costly and more reliable than verification by others. Cost depends on the time spent and lost opportunities, as compared to the compensation of experts and agency costs of delegation. Thus, one's own judgment may be decisive because one bears the consequences of the decision, but one's level of wisdom, knowledge, and expertise may be lower, drawing a distinction between "verification" and "judgment." See GOVIER, *supra* note 4, at 230, citing SISSELA BOK, *A STRATEGY FOR PEACE* (1989).

<sup>10</sup> See GOVIER, *supra* note 4, at 27.

<sup>11</sup> An attempt by teachers in a Canadian law school to control students through minutely detailed rules of examinations led to a culture of mistrust; the attitude of mistrust bred more mistrust. See *id.* at 87–88.

<sup>12</sup> See generally D. Scott Anderson, Comment, *What Trust Is in These Times? Examining the Foundation of Online Trust*, 54 EMORY L.J. 1441 (2006).

However, there are persons and organizations that feed on such traits. Discovering their tendencies and signs of behavior is often difficult, especially when verification is costly. Thus, “[b]usinesses [should] learn how to establish trust in the new [environment and] communication medium.”<sup>13</sup>

Some believe that the Internet is a free space that should not, and cannot, be regulated, and that markets can resolve the trusting problem. I argue that trusting on the Internet will not develop without law. Law punishes breach of trust and compensates those who reasonably trust. It also provides trusted persons with a good reputation, which is very valuable for them.<sup>14</sup>

## 2. Trusting and Non-Trusting

### 2.1 Relative Costs, Benefits, and Risks

“Trusting involves costs, benefits, and risks to both the trusted and the trusting parties.”<sup>15</sup> When trust is absent, parties must resort to verification. If the cost of verification is too high, people will not interact. On the Internet, verification can be very costly. Unless there is a way to reduce the verification costs or raise the level of trust, the Internet will not reach its potential.

There are indications that social trusting is crucial to economic prosperity, and perhaps the very existence of individuals and society.<sup>16</sup> Specialization is a necessary component of a prosperous economy. Specialization requires interdependence, which cannot exist without a measure of trusting.<sup>17</sup> In an entirely non-trusting relationship, interaction

<sup>13</sup> See JOHN O. WHITNEY, *THE ECONOMICS OF TRUST LIBERATING PROFITS AND RESTORING CORPORATE VITALITY* (1996). See also RODERICK M. KRAMER & TOM R. TYLER, *TRUST IN ORGANIZATIONS: FRONTIERS OF THEORY AND RESEARCH* 232 (1996).

<sup>14</sup> Frankel, *supra* note 1, at 459.

<sup>15</sup> *Id.* at 460.

<sup>16</sup> Social capital is defined as a moral resource and a public good that is self-perpetuating and lubricates the growth of trust in society: See GOVIER, *supra* note 4, at 153 (“For politics, economics, and personal well-being, social trust is a valuable resource.”). Lack of trust is costly in psychological terms. The unknown is risky; it breeds fear and anxiety, which can be debilitating. See NIKLAS LUHMANN, *TRUST AND POWER* (1980), *quoted in* BERNARD BARBER, *THE LOGIC AND LIMITS OF TRUST* 10 (1983): “But a complete absence of trust would prevent him even from getting up in the morning. He would be prey to a vague sense of dread, to paralyzing fears. He would not even be capable of formulating distrust and making that a basis for precautionary measures, since this would presuppose trust in other directions. Anything and everything would be possible. Such abrupt confrontation with the complexity of the world at its most extreme is beyond human endurance.” See also Lawrence E. Mitchell, *Fairness and Trust in Corporate Law*, 43 *DUKE L.J.* 425 (1993).

<sup>17</sup> In complex societies we need to trust many people, including experts on information that we would not understand even if it were disclosed to us. See GOVIER, *supra* note 4, at 26. See also Tamar Frankel, *Fiduciary Law*, 71 *CAL. L. REV.* 795 (1983).

would be too expensive and too risky to maintain. There is a correlation between the level of trusting relationships on which members of a society operate and the level of that society's trade and economic prosperity.<sup>18</sup>

Benefits on the Internet are no different. The cost to businesses and people who seek to be trusted is also higher on the Internet because many of the signs that signal trustworthiness do not appear on the Internet.

One effective mechanism that reduces the cost and risks of personal trusting is the utilization of trusted legitimate institutions and intermediaries, both private and public. Institutions reduce trusting costs regardless of consumers' culture and regardless of whether personal trust is mixed with skepticism.

"The benefits of institutional or impersonal trusting are very great. People can trade with strangers through trusted intermediaries and institutions based on impersonal trust.<sup>19</sup> ...[T]he number of institutions is smaller than the number of people with whom business can be conducted, a factor that reduces the investment in verifying the trustworthiness of the institutions. In addition, buyers, investors, borrowers, and depositors can move from one institution to another with little cost. [Further,] institutions have relative longevity, and can build impressive reputations. . . .

[In addition,] institutions reduce lost opportunities of interacting with strangers,<sup>20</sup> allowing people to deal with strangers and benefit from services of capable strangers who function under the umbrella of the institutions.<sup>21</sup> . . .

[Finally,] and most importantly, risks from trusting commercial and financial institutions are reduced by law."<sup>22</sup>

<sup>18</sup> See FRANCIS FUKUYAMA, *TRUST: THE SOCIAL VIRTUES AND THE CREATION OF PROSPERITY* 7 (1995); FRANCIS FUKUYAMA, *GREAT DISRUPTION: HUMAN NATURE AND THE RECONSTRUCTION OF SOCIAL ORDER* 256 (1999); WHITNEY, *supra* note 13; and Bruce Chapman, *Trust, Economic Rationality, and the Corporate Fiduciary Obligation*, 43 U. TORONTO L.J. 547 (1993).

<sup>19</sup> In comparing American impersonal trusting with Japanese personal trusting, one can see the weakness of the Japanese system. The focal point of this weakness is with regard to financial institutions, which Japan is now remodeling. In an international economy, impersonal trusting has become crucial to national economic prosperity.

<sup>20</sup> Modern "urban" trust is strikingly different from trust in, for example, Swedish village life where consumers only transact with known merchants. "Modern trust" is more tied "to people's sense of how institutions operate than to their attitudes towards unknown individuals." See GOVIER, *supra* note 4, at 24-25.

<sup>21</sup> See *id.* at 29: "To live in a complex society without going mad, we must have trust in systems too."; and Grabner-Kraeuter, *supra* note 2, at 45. Institutional trust is especially important on the Internet because it does not depend on past interactions or personal characteristics.

<sup>22</sup> Frankel, *supra* note 1, at 466-67 (footnote omitted). Regarding the ability of parties to move among institutions, many state laws prohibit banks from penalizing borrowers who wish to refinance mortgages (that is, pay off their mortgage loans and take loans at lower interest).

As mentioned, situations that do not require trusting and involve low or no verification costs involve higher costs on the Internet. In real space, the purchaser of a newspaper bears little or no cost in verifying the newspaper and its price, and no promise is involved because the exchange is simultaneous. Transactions on the Internet are usually not simultaneous.

However, in 2008 consumers can buy software that is downloaded immediately upon purchase or subscriptions to Web sites that are activated immediately. A good example of an instantaneous transaction on the Internet would be the purchase of music from Apple's iTunes service.

Risks from third parties [that acquire the consumers' personal identities and credit card numbers] undermine consumers' trust in the Internet. . . . Under United States law, if stolen credit cards are used for unauthorized purchases, banks or sellers must indemnify consumers for losses above \$50. But on the Internet, consumers may not know that their card numbers have been stolen because they still hold their cards. . . . Third parties harm consumers by malicious hyperlinks, spyware, and "spamming"—an avalanche of advertising causing bottlenecks on consumers' computers.<sup>23</sup>

The problem of spyware is not limited to malicious and obscure third parties. Sony BMG Music Entertainment was subject to a lawsuit under California's antispyware legislation for the use of embedded "rootkit" software on their music CDs that monitored users' computer usage, and made itself difficult to find and remove.<sup>24</sup> In its monthly "State of Spam" report for July 2008, Symantec Messaging and Web Security reported that spam levels had climbed from 56 percent in 2006 to over 80 percent of all e-mails today.<sup>25</sup> Malicious third parties can also injure online reputations of businesses. These include, for example, third parties known as "phishers." Phishers send e-mails and create Web sites disguised as legitimate businesses in order to trick victims into sending personal or financial information. The practice of phishing is a significant obstacle for businesses seeking to gain trust on the Internet because the practice uses the good reputation of legitimate businesses as a ploy to trick consumers. Recipients of fake e-mails and victims of phishing have been reported to become less trusting of e-mails and less likely to transact business online.<sup>26</sup> Technology

<sup>23</sup> See Laura L. Edwards, *Oh What a Tangled World Wide Web We Weave: An Analysis of Washington's Computer Spyware Act in a National Context*, 31 SEATTLE U. L. REV. 645 (2008).

<sup>24</sup> *Id.*

<sup>25</sup> See SYMANTEC, THE STATE OF SPAM, [http://www.symantec.com/business/theme.jsp?themeid=state\\_of\\_spam](http://www.symantec.com/business/theme.jsp?themeid=state_of_spam) (last visited Sept. 6, 2008).

<sup>26</sup> See Jasmine E. McNealy, *Angling for Phishers: Legislative Responses to Deceptive E-Mail*, 13 COMM. L. & POL'Y 275 (2008).

provides some redress from these harms, at a cost, and only temporarily, until spammers design software to circumvent the protections.

There has been legislation over the last decade in response to the ever-increasing flood of spam and spyware. Congress attempted to address the spam issue in 2003, by enacting the CAN-SPAM Act.<sup>27</sup> The CAN-SPAM Act does not grant a private remedy for victims of spam but rather authorizes the FTC to bring actions against individuals who violate the provisions of the CAN-SPAM Act. A single violation can result in a fine of \$10,000 and spammers could face prison sentences of up to five years. However, few individuals have been prosecuted under the CAN-SPAM Act to date. The Act was widely criticized as ineffective.<sup>28</sup> The CAN-SPAM Act does not aim at outlawing spam altogether as much as regulating it.<sup>29</sup> More importantly, though, spam is a global problem and spam e-mails can come from anywhere in the world. A law enacted in the United States that subjects citizens to fines for failing to include an opt-out clause in their e-mails will not realistically stop a spammer in eastern Europe from sending spam to American inboxes. Because of the global nature of spam, no single nation or state can draft laws that would eliminate or drastically lower spam.<sup>30</sup> The best that can be hoped for in unilateral antispam legislation would be to lower the creation and dissemination of spam within the borders of the countries or states that enact it.

Various forms of spyware legislation have been proposed in Congress, but none have yet been enacted.<sup>31</sup> While no spyware laws have been passed on the national level, the FTC has targeted and punished multiple spyware distributors under existing laws regulating deceptive business practices.<sup>32</sup> Also, some states, such as Washington and California, have tried to tackle the spyware problem with various forms of antispyware legislation.<sup>33</sup> However, because the distribution

<sup>27</sup> See Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified at 15 U.S.C. §§ 7701–7713, 18 U.S.C. § 1037 (Supp. IV 2004)).

<sup>28</sup> See Edwards, *supra* note 23, at 657–58.

<sup>29</sup> See Samuel Boone-Lutz, *Just Say Yes: Drug Trafficking Treaties as a Model for an Anti-Spam Convention*, 39 GEO. WASH. INT'L L. REV. 367 (2007).

<sup>30</sup> See *id.*

<sup>31</sup> For example, in 2005, four pieces of federal spyware legislation were introduced into the House and Senate, none of which have yet been made into law: Securely Protect Yourself Against Cyber Trespass Act (SPYACT), H.R. 29, 109th Cong. (2005); Internet Spyware (I-SPY) Prevention Act, H.R. 744, 109th Cong. (2005); Software Principles Yielding Better Levels of Consumer Knowledge (SPYBLOCK) Act, S. 687, 109th Cong. (2005); and Enhanced Consumer Protection Against Spyware Act, S. 1004, 109th Cong. (2005).

<sup>32</sup> See Megan M. Engle, *Anti-Spyware Enforcement: Recent Developments*, 3 ISJLP 581 (2008).

<sup>33</sup> For a discussion on Washington's antispyware legislation, see Edwards, *supra* note 23.

of spyware invariably crosses state and national lines, state legislation can do little to solve the spyware problem.<sup>34</sup> Spyware is arguably more damaging to consumer trust online than spam and viruses because whereas spam and viruses are created by hackers for their own benefit or for the benefit of criminal organizations, spyware is more commonly created by large corporations that bundle spyware with legitimate software.<sup>35</sup> Furthermore, while spyware is by definition a subversive program, the existence of spyware in software is frequently included in the end-user license agreements of the software. It is bundled in to protect the distributors from legal action based on a contract theory of liability or based on trespass to chattels.<sup>36</sup> To make matters worse for consumers, spyware manufacturers utilize the current state of the law not just to protect themselves but also to attack the manufacturers of antispyware programs for creating the programs that remove their malicious software from consumers' computers.<sup>37</sup> The proliferation and acceptance of spyware in the e-commerce marketplace led one commentator to remark that "the spyware wars are over—and spyware has won."<sup>38</sup>

The rise of online social networking sites adds a new aspect into the discussion of online trust. With millions of users sharing their personal information on sites such as MySpace<sup>39</sup> and Facebook,<sup>40</sup> opportunities for online fraud, deception, and exploitation have increased dramatically. The two most troubling uses of online social networking sites have been as "one-stop shopping catalogues" for child predators who look for victims<sup>41</sup> and as "virtual bathroom walls" for "cyberbullies" to harass peers.<sup>42</sup> Recognizing the problems that have accompanied

<sup>34</sup> See Erica Pines, Note, *Spyware Regulation: National Regulation Should Prompt Industry Self-Policing*, 38 LOY. L.A. L. REV. 2219, 2239 (2005) ("A state law only affects one state, while spyware is truly a global problem").

<sup>35</sup> See Jacob Kreutzer, *Somebody Has to Pay: Products Liability for Spyware*, 45 AM. BUS. L.J. 61 (2008). For examples of successful spyware manufacturers, see Stefanie Olsen, *Gator Sinks Teeth into New Image*, CNET NEWS, Oct. 30, 2003, [http://news.cnet.com/Gator-sinks-teeth-into-new-image/2100-1024\\_3-5099601.html](http://news.cnet.com/Gator-sinks-teeth-into-new-image/2100-1024_3-5099601.html), and Annalee Newitz, *Don't Call It Spyware*, WIRED MAGAZINE, Dec. 2005, available at <http://www.wired.com/wired/archive/13.12/spyware.html>.

<sup>36</sup> See Kreutzer, *supra* note 35, at 62–63.

<sup>37</sup> See Paul Festa, *See You Later, Anti-Gators?* CNET NEWS, Oct. 22, 2003, [http://news.cnet.com/See-you-later-%2C-anti-Gators/2100-1032\\_3-5095051.html](http://news.cnet.com/See-you-later-%2C-anti-Gators/2100-1032_3-5095051.html).

<sup>38</sup> See Newitz, *supra* note 35.

<sup>39</sup> <http://www.myspace.com>.

<sup>40</sup> <http://www.facebook.com>.

<sup>41</sup> See Jessica S. Groppe, *A Child's Playground or a Predator's Hunting Ground? How to Protect Children on Internet Social Networking Sites*, 16 COMM.LAW CONSPECTUS 215 (2007).

<sup>42</sup> Cyberbullies, also known as "trolls," typically post degrading and cruel messages and pictures on social networking sites' "walls." Cyberbullying (or "trolling") causes more than hurt feelings and has led to death threats, suicide, and murder. See *id.* at 227–28.

online social networking sites, various safeguards have been suggested and put into action. There has been a significant push in the legislature to address the issue,<sup>43</sup> most notably in the Keeping the Internet Devoid of Predators Act of 2008,<sup>44</sup> and the Internet Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act of 2007.<sup>45</sup> Those who oppose regulation of online social networking sites argue that permissible speech will be "chilled" and would possibly force sites overseas in order to escape regulations.<sup>46</sup> In addition to state and national legislation, various self-help and educational programs have been put into action. Three educational campaigns that have been launched are (1) Help Delete Online Predators (HDOP), which is designed to educate parents about online child predators, (2) Don't Believe the Type, which is designed to educate teens about predators, and (3) Think Before You Post, which is designed to educate teens about posting personal information online.<sup>47</sup>

The rising pressure has caused some social networking sites to change their user policies to protect children. Most notably, MySpace has made serious efforts in order to render its site safer for children and teenagers. (MySpace hired a former Department of Justice prosecutor as its security officer, developed parental notification software, and banned sex offenders from its site using a program called Sentinel Safe.)<sup>48</sup> Self-help and education may be the most effective remedy for the problems on social networking sites because so much of the damage is self-inflicted and easily preventable if better judgment is used. Teaching children and teenagers the consequences of posting harmful personal information and pictures would nip much of the social networking problems in the bud. However, it is unrealistic to believe that children will be able to consistently protect themselves. Therefore, for online social networking sites to be safe and trustworthy environments, there is a need for legislation, regulation, and tougher self-policing by the sites.

In addition, traditional policing and enforcement against illegal actions is weaker on the Internet, although the Internet does offer

<sup>43</sup> For an extensive discussion on the legislative response to the problem of child predators on online social networking sites, see Susan Hanley Duncan, *Myspace Is Also Their Space: Ideas for Keeping Children Safe from Sexual Predators on Social Networking Sites*, 96 Ky. L.J. 527 (2008).

<sup>44</sup> Keeping the Internet Devoid of Sexual Predators Act of 2008, S. 431, 110th Cong. (as passed by Senate, May 20, 2008).

<sup>45</sup> Internet Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act of 2007, H.R. 837, 110th Cong. (2007).

<sup>46</sup> See Michael D. Marin & Christopher V. Popov, *Doe v. MySpace, Inc.: Liability for Third Party Content on Social Networking Sites*, 25 COMM. LAW. Spring 2007, at 3, 8 (2007).

<sup>47</sup> See Duncan, *supra* note 43.

<sup>48</sup> See Groppe, *supra* note 41, at 238–39.

added enforcement tools, including publication and automated monitoring. Thus, both costs and risks for buyers (and some for sellers) on the Internet are higher than in real space. Sooner or later, consumers recognize the danger.<sup>49</sup>

### 3. Risk Reduction

In general, common interests can reduce the risks associated with trusting, as can similarity of character.<sup>50</sup> Similar incentives operate on the Internet. Information about persons on the other side of an e-mail message is costly to verify, making personal trust-building on the Internet better achieved by sharing, as in real space. Proof of one party's trustworthiness, through consistent behavior, can reduce the risks associated with trusting. A similar approach works on the Internet. Self-help can also reduce the risks associated with trusting.

On the Internet, some of the verification costs and burdens have shifted from buyers to sellers. The shift is efficient. First, commercial and financial institutions can reap enormous benefits from Internet communications. Presumably, that gives them incentives to expend more efforts to gain customers' trust. New market entrants, or sellers of new products, recognize the need to capture customers' trust even in real space.

Second, as compared to real space, the level of customers' commitment to cyberspace is not as high. While buyers are exposed to more costs and risks in Internet transactions, buyers also have alternatives to buy in real space, even though these alternatives lack the convenience and choices of Internet shopping. As their risks and costs rise, many customers are inclined to expend little effort in reducing their risks. Thus, in relation to verification, the bargaining power between these two groups has changed and shifted from buyers to sellers.

Third, the cost of proof and risk reduction may be lower for the sellers than for the consumers. Although sellers can shift the added costs to consumers, competition limits such increases. Therefore, even if sellers transfer some of the costs, buyers' increased costs will still be lower than if the buyers had to verify the facts and promises themselves. Fourth, the more sellers succeed in convincing customers of

---

<sup>49</sup> Consumers who are not familiar with communicating on the Internet seem to be more gullible than they would be in real space. They view experts in Internet communications as more trustworthy. Thus there is something like a reverse order: expertise produces dependency and dependency produces trust.

<sup>50</sup> Russell Hardin defines trust mostly in terms of encapsulated interest. See RUSSELL HARDIN, *DISTRUST* (2004). I argue that encapsulated interest is a risk-reducing situation that contributes to trusting but is not trusting per se.

their facts and promises, the lower their burden becomes as they build a trusting relationship with their customers.

Finally, many sellers have begun to recognize that they are better off uniting rather than competing on the issue of trustworthiness. A race to the bottom will bring Internet use to the bottom as well. Therefore, there should be (and hopefully there is) a growing tendency to monitor others, at least within the same industry, to maintain a minimal level of trustworthiness.

Market actors can reduce the risks associated with trusting. Sellers can offer self-binding obligations, such as warranties and “no questions asked” return policies. Lower information and verification costs can reduce the risks associated with trusting. A reputation for being trustworthy is one such mechanism that businesses can also acquire in the market.<sup>51</sup> Reputation serves the dual role of being a source of information for consumers and a source of possible sanctions for businesses.<sup>52</sup> Hence, people rely on reputation, good or bad, as a form of verification, as an added comfort, or as the least expensive alternative when direct sources of information are too costly.

On the Internet, information tools can develop for individuals. For example, direct traders can create a personal business reputation on the Internet, as the eBay<sup>53</sup> experience has shown. Traders on the Internet eBay site are likely to rely on their own experiences, and on those of others regarding other individuals’ behavior, and choose their trading partners according to the reputation they developed for telling the truth and keeping their word.<sup>54</sup> The low publication costs and eBay’s services provide powerful information that helps make or break a reputation fairly quickly. The reputation of traders on eBay’s site affects the prices traders can obtain or are willing to pay. A trader with a good reputation will attract more bidders, who will bid the price

<sup>51</sup> Market reputation has a different weight than personal observation, yet can carry weight of the aggregate opinion of others. It is more like price, a “black box,” unless others have similar concerns. Reputation is a marketing device, distinguishing competitors in the markets. Trustworthy people offer reduced information costs to other parties, and can therefore charge more for their services and products. When transactions are trust-dependent to the extent that most people would not engage in a business relationship without trusting, the assurance of trusting becomes crucial to the transaction. In such a case, the interference of the law as a guarantor of trustworthiness may be cost reducing and even necessary.

<sup>52</sup> See Grabner-Kraeuter, *supra* note 2, at 48.

<sup>53</sup> See eBay, Keeping You Safe on eBay, <http://pages.ebay.com/help/account/safety.html> (last visited Dec. 10, 2008).

<sup>54</sup> “Feedback is the foundation of security and trust in the eBay community. If a user is untrustworthy or unreliable, the user’s feedback score will reflect this reality. This creates a system of normative behavior, which allows users to self-regulate within the eBay community.” See Jeffrey Aresty, *Digital Identity and the Lawyer’s Role in Furthering Trusted Online Communities*, 38 U. Tol. L. Rev. 137, 137, 157 (2006).

up. A trader with a poor reputation will attract fewer bidders, who will not bid as much for the same item.<sup>55</sup>

Recognizing the importance of reputation, some sellers on eBay have created a “market for feedback” where they buy and sell items of nominal value among themselves in order to artificially boost their feedback ratings.<sup>56</sup> This practice degrades the effectiveness of the feedback system and thereby makes eBay reputations suspect and achieving trust on eBay more difficult.

A reputation-forming device, such as membership in professional and other groups, can also reduce the risks associated with trusting. Internet businesses have followed the real space model and formed societies whose main function is to gain the customers’ trust. Internet businesses recognize that their competitors, who may act unwisely, can adversely affect their own reputation. For example, Financial Services Technology Consortium is composed of competitors who combine to create a “public good,” that is, trustworthiness for all, and monitor their members to maintain this public good.<sup>57</sup>

Markets are populated by private sector professionals and organizations with significant reputations that can act as reliable verifiers of others’ assertions of facts and promises. They can verify the information or actually lend their credit and name to back the sellers’ obligations. That involvement offers parties both an additional trusted obligor and an indirect assurance of verified information, which the obligor will gather to protect its interests. Accountants and lawyers act as market verifiers of information. They command trust by membership in self-regulating organizations, and by strict government regulation. They verify information about the trustworthiness of strangers.

There are organizations that check businesses for trustworthiness in terms of expertise and proof.<sup>58</sup> Rating agencies perform a similar function. They evaluate bonds after gathering information about issuers including an evaluation of the creditworthiness (trustworthiness) of the issuers. The rating agency Moody’s Investors Service<sup>59</sup> offers, for a fee, “trust packages” to parties who wish to reduce their risk of business

<sup>55</sup> See Susan Block-Lieb, *E-Reputation: Building Trust in Electronic Commerce*, 62 LA. L. REV. 1199 (2002).

<sup>56</sup> See Jennifer Brown & John Morgan, *Reputation in Online Auctions: The Market for Trust*, 49 CAL. MGMT. REV. 61 (2006).

<sup>57</sup> See Financial Services Technology Consortium, <http://www.fstc.org/about/index.php> (last visited July 15, 2008) (comprising over 100 organizations working in collaboration to “solve shared problems and challenges, as well as pioneer next generation technology that benefits us all”).

<sup>58</sup> It is suggested that the value of board directorship for busy corporate leaders is in “networking” and current information, including information about other actors in their field.

<sup>59</sup> <http://www.moody.com>.

relationships with unknown parties abroad. It ascertains whether the unknown party abroad is trustworthy by verifying information, offering the same kind of fact-finding that people engage in to develop a trusting relationship. Moody's has developed a list of factors that demonstrate trustworthiness, and collects information about the unknown party's consistency in performing its promises, paying its debts, making true statements, and conducting long-term relationships.<sup>60</sup> In fact, Moody's has commodified, and is selling, trustworthiness.<sup>61</sup>

Internet businesses have followed the same model. The Internet markets have additional third-party fact verifiers, especially when information can be manipulated on the Internet. For example, pictures shown on the Internet can be digitally changed. Third parties can provide verification of products, such as the true color of women's clothes. This verification was adopted as a selling point to consumers who otherwise mistrust the online display. Unauthorized persons can alter and sign documents transferred through the Internet. Technology is developing to ensure the integrity of documents and signatures. Third-party intermediaries offer trust services for Internet businesses, such as iEscrow escrow services, to ensure that buyers pay money in advance but the money reaches the sellers only upon delivery.<sup>62</sup>

Like reputation-building in real space, businesses build their reputation through associations. The U.S. government offers verification, in the negative sense, about those who are not trustworthy. The Federal Trade Commission issues "Consumer Alerts!" on its Web site.<sup>63</sup> Other associations issue positive recommendations about businesses that act on the Internet, similar to the Better Business Bureau's, such as the Center for Democracy and Technology.<sup>64</sup>

<sup>60</sup> Banks have offered a similar service in the form of letters of credit since the seventeenth century. The letters of credit, however, provide a guarantee to parties abroad, who do not know the domestic parties and therefore do not trust their promises. The bank undertakes, unconditionally, the obligation to pay upon presentation of the bills of lending, providing evidence that the goods have arrived.

<sup>61</sup> See Bernard S. Black & Ronald J. Gilson, *Venture Capital and the Structure of Capital Markets: Banks Versus Stock Markets*, 47 J. FIN. ECON. 243 (1998); see also Donald C. Langevoort, *Angels on the Internet: The Elusive Promise of "Technological Disintermediation" for Unregistered Offerings of Securities*, 2 J. SMALL & EMERGING BUS. L. 91 (1998); Stephen J. Choi, *Gatekeepers on the Internet: Rethinking the Regulations of Small Business Capital Formation*, 2 J. SMALL & EMERGING BUS. L. 27 (1998).

<sup>62</sup> According to the Craigslist's About Scams page, most online escrow services are fraudulent and should be avoided. See About Scams, <http://www.craigslist.org/about/scams> (last visited Dec. 10, 2008).

<sup>63</sup> e.g., Office of Consumer & Bus. Educ., Fed. Trade Comm'n, *How Not to Get Hooked by a 'Phishing' Scam* (2006), <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.pdf>. "The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them."

<sup>64</sup> <http://www.cdt.org>.

In order to maintain a good reputation, online businesses often pay for inspections and certification of their Web sites by trusted third parties.<sup>65</sup> The display of “seals” by such trusted third parties is a strategy used by Web sites to enhance consumer trust.<sup>66</sup> The use of seals is an especially valuable tool for Web sites without brand recognition, as the seal itself can act as a “surrogate brand name.”<sup>67</sup> The display of trusted third-party seals has become so much a part of the culture of online business that even individual sellers on eBay have begun to utilize them through the warranty service SquareTrade.<sup>68</sup> Studies have shown that while these seals do increase consumer confidence in the Web sites that bear them, they are not always reliable indicators of the privacy policies of the sites, and sites that bear these seals on average actually collect more personal data from the consumers that visit them.<sup>69</sup>

“Both on the Internet and in real space, trustworthiness can evaporate on disappointing evidence. But it seems that on the Internet, it can disappear even faster. One organization, created on the Internet, offered to attach its mark ‘TRUSTe’ to businesses as a sign of trustworthiness.”<sup>70</sup> It is of questionable success because some businesses that carried the sign did not live up to the reasonable expectations of the consumers. Once TRUSTe allows its seal to be displayed by a Web site, it will rarely cancel the relationship to demand that its seal to be taken down. In 2005, TRUSTe ended its relationship with Gratis Internet because of privacy violations and demanded its seals be taken off the company’s Web site. This was the first time in two years that TRUSTe had revoked the use of its seal for privacy violations.<sup>71</sup> Many consumers reached the conclusion that TRUSTe did not sufficiently monitor, enforce, or inform about the promises of its sign.<sup>72</sup> Although many

<sup>65</sup> See Bruce L. Benson, *The Spontaneous Evolution of Cyber Law: Norms, Property Rights, Contracting, Dispute Resolution and Enforcement Without the State*, 1 J.L. ECON. & POL’Y 269 (2005).

<sup>66</sup> See Wang & Emurian, *supra* note 2, at 118.

<sup>67</sup> See Daryl Koehn, *The Nature of and Conditions for Online Trust*, 43 J. BUS. ETHICS 3 (2003).

<sup>68</sup> See Gillian K. Hadfield, *Delivering Legality on the Internet: Developing Principles for the Private Provision of Commercial Law*, 6 AM. L. & ECON. REV. 154 (2004). For details on SquareTrade’s seal program, see SquareTrade, <http://www.squaretrade.com> (last visited Sept. 6, 2008).

<sup>69</sup> See Nora J. Rifon et al., *Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures*, 39 J. CONSUMER AFFS. 339 (2005).

<sup>70</sup> Frankel, *supra* note 1, at 473. <http://www.truste.org>.

<sup>71</sup> See Ted Bridis, *Privacy-Assurance Seal Yanked Off Web Sites*, USA TODAY, Feb. 10, 2005, available at [http://www.usatoday.com/tech/news/internetprivacy/2005-02-10-truste-seal\\_x.htm](http://www.usatoday.com/tech/news/internetprivacy/2005-02-10-truste-seal_x.htm).

<sup>72</sup> For criticism of TRUSTe, see Paul Boutin, *Just How Trusty Is TRUSTe?* WIRED MAGAZINE, Apr. 9, 2002, available at <http://www.wired.com/techbiz/media/news/2002/04/51624>.

consumers have identified TRUSTe as unreliable and untrustworthy, there are many more consumers who are unaware of its shortcomings and continue to trust in its label. Because of this, many big-name Web sites such as Microsoft, Disney, and AOL continue to use the TRUSTe seal.<sup>73</sup>

Internet businesses have piggybacked on trusted real space businesses because customers seem to trust businesses in real space more than they do businesses in cyberspace.<sup>74</sup> For example, community banks with a loyal customer base can establish similar relationships on the Internet, and far larger financial institutions may desire to link their products to such banks. Sometimes brick-and-mortar enterprises that have the loyalty and trust of their customers become aligned with Internet enterprises to bestow on those Internet enterprises the trust of the retailers' customers.

This arrangement is similar to franchising—franchising not of expertise or quality of goods, but of trust. For a similar reason, the value of real space brand names has risen on the Internet.<sup>75</sup> Perhaps this may be one reason why trademark owners are so concerned about their trademarks and well-known brand names have acquired special protection by Congress.

For trust purposes, presentation on the Internet is as important as, if not more important than, presentation in the physical world. Online businesses must display a presentable virtual storefront if they wish to garner the trust of consumers. Attributes that have been found to have a positive impact on trust include ease of navigation, good use of visual design, lack of grammatical errors, and an overall professional look to the site.<sup>76</sup> The inverse is true as well. Studies have found that poor visual designs, mixing advertisements with content, and broken links act as cues that a Web site is untrustworthy.<sup>77</sup>

Collection and dissemination of personally identifying information (PII) such as names, addresses, social security numbers, and credit card numbers by Web sites pose serious privacy risks to Internet users that can often lead to spam and even identity theft. Many Web

<sup>73</sup> Groups with similar interests undertake to enforce the members' obligations to be trustworthy, thereby maintaining the trustworthiness of the group. See Tamar Frankel, *Should Funds and Investment Advisers Establish a Self-Regulatory Organization?* in *THE FINANCIAL SERVICES REVOLUTION: UNDERSTANDING THE CHANGING ROLES OF BANKS, MUTUAL FUNDS, AND INSURANCE COMPANIES* 451 (Clifford E. Kirsch ed., 1997).

<sup>74</sup> See Grabner-Krauter, *supra* note 2, at 48.

<sup>75</sup> Different variables that may enhance an online business's reputation include the presence of a physical store, and the size and age of the business. See Miriam J. Metzger, *Effects of Site, Vendor, and Consumer Characteristics on Web Site Trust and Disclosure*, 33 *COMM. RES.* 155 (2006).

<sup>76</sup> See Cynthia L. Corritore, Beverly Kracher & Susan Wiedenbeck, *Online Trust: Concepts, Evolving Themes, a Model*, 58 *J. HUM.-COMPUTER STUD.* 737 (2003).

<sup>77</sup> See *id.* at 747.

sites collect PII. The most common way this is done is by simple surveys that visitors must fill out in order to utilize the Web site's services or complete orders. While most users do not mind, and are aware to some extent, that sites are collecting their personal information, the danger and loss of trust come from the sharing and sale of this personal information by the reputable sites to unknown and untrustworthy third parties. The sharing of personal information with third parties is not limited to shady and disreputable Web sites. Of the top twenty-five Web sites, only one (Apple Computer) states in its privacy policy that it will not share collected personal information with unrelated third parties.<sup>78</sup>

Once personal information has been disseminated to third parties, it is impossible to know who will eventually get it. Unfortunately, consumers have little choice but to submit their personal information in order to utilize the services of these Web sites. Compounding this problem is the fact that many Internet businesses often make their privacy policies esoteric and hard to find on the Web sites, so that even curious consumers have difficulty finding out if they are at risk. The combination of Web sites that force consumers to submit PII, sharing the consumers' PII with third parties, and making it difficult, if not impossible, for consumers to find out to what extent their PII is being spread around the Internet is a toxic mix of practices that can only hurt and certainly not foster the growth of trust on the Internet.

The United States offers very limited protection against Internet users' PII collection and distribution to third parties. That is not to say that Congress has provided no protections concerning the collection of Internet users' PII. For example, children under the age of 13 are protected under the federal Children's Online Privacy Protection Act (COPPA)<sup>79</sup> and the Gramm-Leach-Bliley Act (GLBA)<sup>80</sup> requires financial institutions to provide comprehensible privacy policies and an opt-out clause before disseminating PII.<sup>81</sup> However, most consumer PII is not adequately protected by the law. Web sites are free to use PII without providing clear privacy policies.<sup>82</sup> Since online businesses are primarily concerned with turning a profit and not with protecting the best interests of consumers, they use visitors' PII in the most profitable ways they can. If businesses are allowed by law to make their privacy policies vague and to sell visitors' PII to third parties, there is no reason to expect that the industry would rein in the practice as long as it proved profitable. Because the practice is so meshed within the fabric

<sup>78</sup> See Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553 (2008).

<sup>79</sup> See Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2000).

<sup>80</sup> See Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6802(a)–(b) (2000).

<sup>81</sup> See Ciocchetti, *supra* note 78, at 609–10.

<sup>82</sup> See *id.* at 609–11.

of e-commerce, it is up to the legislature to put limits on this practice or at least to force online businesses to inform consumers in a clear manner about how their PII will be used. The lack of regulations concerning how our personal information is used by Web sites is a serious barrier to online trust.<sup>83</sup>

The online classified ads company Craigslist<sup>84</sup> demonstrates the best and worst examples of Internet trust. Craigslist was started by Craig Newmark in 1995 as a nonprofit e-mail list designed to notify San Francisco residents of local events.<sup>85</sup> Craigslist evolved into a virtual personal ad service spanning 500 cities in 50 countries, where people can post everything from job openings to tickets for sale to romantic want ads.<sup>86</sup> Craigslist became a for-profit corporation in 1999, and in 2004 eBay acquired 25 percent equity in Craigslist.<sup>87</sup> Craigslist derives its profits by charging fees for job ads in ten cities and for apartment listings in New York City.<sup>88</sup> Craigslist is a powerful and useful tool that relies on the communities that use it. However, even though Craigslist is a very useful tool, some people abuse it, and it has some significant dangers that users have to be aware of. In addition to run-of-the-mill fraud,<sup>89</sup> Craigslist has been used to facilitate many types of illegal and morally reprehensible activities. These activities include the solicitation of underage prostitutes<sup>90</sup> and soliciting the services of a hit man,<sup>91</sup> and in one case a couple may have attempted to use the site to sell their newborn baby.<sup>92</sup> Verification is another major problem on Craigslist.

<sup>83</sup> Studies show that Americans resent the freedom of companies to do whatever they want with their personal information and that people are becoming more unwilling to spend money and submit personal information online due to lack of trust. *See id.* at 557.

<sup>84</sup> <http://www.craigslist.org>.

<sup>85</sup> *See* Craigslist Factsheet, <http://www.craigslist.org/about/factsheet.html> (last visited Sept. 6, 2008).

<sup>86</sup> *Id.*

<sup>87</sup> *Id.*

<sup>88</sup> Craigslist charges \$25 for job ads in cities including Boston and Chicago, and \$75 for job ads in San Francisco. *See id.*

<sup>89</sup> *See* Craigslist—About Scams, *supra* note 62.

<sup>90</sup> *See* Ethan Baron, *Five Girls in Care Have Been Selling Sex on Craigslist, Police Say*, PROVINCE, May 9, 2008, available at <http://www.canada.com/theprovince/news/story.html?id=c1e6d15c-21d9-4619-ada5-f954a0367129>.

<sup>91</sup> A Michigan woman placed an ad on Craigslist offering \$5,000 for the murder of the wife of a man she met online. *See* Matthew Philips, *I Need a Hit Man. Now.*, NEWSWEEK, Feb. 11, 2008, available at <http://www.newsweek.com/id/107602>.

<sup>92</sup> The couple who put an ad up for the sale of their newborn later claimed it was only a hoax and were arrested on charges of mischief, which were dropped. *See* Bob Heye, *Man in Trouble over Craigslist Ad with Baby for Sale*, KATU.COM, Mar. 27, 2008, <http://www.katu.com/news/local/17036956.html>.

Users can pose as other persons and place malicious ads that can cause embarrassment and worse to others.<sup>93</sup>

#### 4. The Role of Law in Support of Trusting

Under certain circumstances, the reliability of trusted persons, institutions, and other intermediaries cannot be fully supported by the trusted parties themselves. There comes a point when the parties will not interact because their costs of verification and proof of trustworthiness will exceed their joint benefits from the transaction. In these circumstances, legal backing is necessary.<sup>94</sup> Law offers benefits to both parties. It offers trusting people reduced risks by preventive regulation of institutions and intermediaries, before the fact, and compensation as well as punishing violators, after the fact. Law offers trusted persons a “brand name” guarantee of their trustworthiness, which may be too costly for trusted persons to create or buy in the markets. These supports for trusting are financed not by private sector interested persons, but by all taxpayers. Hence, the cost of maintaining a trusting system as a whole, in addition to the users of trust relationships, is subsidized and distributed among a large group through government intermediation. Further, law strengthens norms of behavior, and reduces the cost of enforcement. People become trustworthy through habit, with a lower threat of punishment.

Trust verification, especially verification by third parties, is layered. The first layer is composed of direct trusting relationships. The second layer, in lieu of or in addition to personal trust, consists of market verifiers. The third layer is composed of verifying the verifiers: the law. Law regulates trusted persons and intermediaries as well as market verifiers, who establish the trustworthiness of others.<sup>95</sup>

Ultimately, third-party regulatory institutions, such as BBBOnLine and TRUSTe, require the backing of law in order to effectively serve their purpose.<sup>96</sup>

<sup>93</sup> One couple placed an ad on Craigslist posing as a man they had previously burgled, offering to give away everything in his house, in order to cover the tracks of their burglary. See Teresa Blackman, *Cruel Craigslist Hoax Was Elaborate Burglary Coverup*, *Police Say*, KGW.COM, Apr. 1, 2008, [http://www.kgw.com/news-local/stories/kgw\\_040108\\_news\\_craigslist\\_hoax\\_arrest.1fa31526.html](http://www.kgw.com/news-local/stories/kgw_040108_news_craigslist_hoax_arrest.1fa31526.html).

<sup>94</sup> Market verifiers can offer verification at a reduced rate relative to personal time, and the law, through a requirement for insurance, examinations, and other preventive measures, can ensure either that the money will not be converted or that (for example) a bank manager is competent. Trusted private sector qualifiers, however, must also prove their trustworthiness. The law regulates the most trusted private sector qualifiers, such as lawyers and accountants.

<sup>95</sup> See Hadfield, *supra* note 68, at 175–76.

<sup>96</sup> BBBOnLine and TRUSTe rely on the government and the courts as a last resort if firms do not accept their proposed solutions. See Jay P. Kesan, *Private Internet Governance*, 35 *Loy. U. CHI. L.J.* 87 (2003).

The law can regulate intermediaries more effectively than individuals. Intermediaries are often less mobile than individuals and their number is smaller.<sup>97</sup> As the size of private sector actors and intermediaries increases, they are likely to be the first-tier gatekeepers and enforcers of the law within their operational territories, including international enforcement.<sup>98</sup> Mergers of banks and businesses are usually accompanied by stricter requirements for self-regulation, control of illegal acts within the organizations, and trustworthiness towards customers. Professional private sector gatekeepers, such as accountants, are subject to increasingly strict regulation as they testify to the trustworthiness of businesses in real space and on the Internet. In contrast, individuals' costs of establishing the trustworthiness of institutions and other specialized intermediaries are very high. Even though the number of intermediaries is small, they are composed of many individuals and their internal activities are not open to individual customers. More importantly, individuals cannot adopt preventive measures to ensure the intermediaries' trustworthiness even though the risks that individuals take, in entrusting their property to institutions, may be very high.

As the importance of the role of intermediaries increases on the Internet, the importance of law in reducing the customers' risks and increasing the trustworthiness of the intermediaries increases. In reaction to consumers' concerns and Congressional prodding, industries began to establish best practices with respect to privacy issues. While customers may rely on some industries' best practices, for financial intermediaries best practices were held insufficient. The danger of losing public trust is too great and the consequences too grave. Further, the law is most important when the public voices its concern on particular issues.

After recognizing the importance of intermediary regulation on the Internet, the next question is: what form will this regulation take, and how best should it be implemented? Ronald Mann proposes three different types of potential remedies: a tort remedy, a takedown regime, and a hotlist regime, which could be imposed against online intermediaries under different circumstances.<sup>99</sup> The utilization of traditional tort remedy would give intermediaries the most incentive to act carefully.

The recent case of *Tiffany v. eBay*<sup>100</sup> highlights many of the problems facing e-commerce as well as important issues of online trust and

<sup>97</sup> See Ronald J. Mann, *Emerging Frameworks for Policing Internet Intermediaries*, J. INTERNET L., Dec. 2006, at 1.

<sup>98</sup> See *id.* at 5–6.

<sup>99</sup> See *id.* at 6.

<sup>100</sup> *Tiffany (NJ) Inc. v. eBay, Inc.*, No. 04 Civ. 4607, 2008 WL 2755787 (S.D.N.Y. July 14, 2008).

responsibility. Tiffany was justifiably upset about the large amount of counterfeit Tiffany goods that were being sold on auctions hosted on eBay's Web site, and did not find eBay's reaction to the problem to be sufficiently effective. In response to the problem Tiffany made demands to eBay, which eBay refused to meet.<sup>101</sup> In 2004, Tiffany sued eBay for "direct and contributory infringement of Tiffany's trademarks by virtue of the assistance that it provides to, and the profits it derives from, individuals who sell counterfeit Tiffany goods on eBay."<sup>102</sup> At its core, this case was about who should bear the burden of policing the sale of trademarked goods: the intermediary that hosts the transactions or the holder of the trademark?<sup>103</sup> The court found that the holder of a trademark (Tiffany) should bear the burden of policing the transactions, even if it is more cost effective for the intermediary (eBay) to do so.<sup>104</sup> This is not to say that Internet intermediaries cannot be held responsible for the infringement of trademarks by third parties on their Web sites.<sup>105</sup> eBay could have been held liable for contributory trademark infringement if it continued to supply its services to a seller that it knew or had reason to know was infringing on Tiffany.<sup>106</sup> eBay was not found to be liable for contributory trademark infringement because it neither facilitated nor turned a blind eye to the sale of counterfeit Tiffany goods. eBay used its own antifraud engine and worked with Tiffany through its verified rights owner (VeRO) program<sup>107</sup> to take down postings of sellers believed to be selling counterfeit Tiffany goods.<sup>108</sup>

On the Internet, financial intermediaries need a higher degree of public trust, as they are eager to cut their costs by establishing Internet communications with customers. Hence, Congress directed regulators to impose rules of confidentiality on financial intermediaries.<sup>109</sup> On November 13, 2000, the Securities and Exchange Commission put into effect a rule that restricts broker-dealers', investment companies', and

<sup>101</sup> These demands included the institution of a "five-or-more rule" in which eBay would ban any seller who was selling five or more pieces of Tiffany jewelry, *see id.* at \*14.

<sup>102</sup> *See id.* at \*2.

<sup>103</sup> *See id.* at \*1.

<sup>104</sup> *See id.* at \*47.

<sup>105</sup> "One who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties." *See Metro-Goldwyn-Mayer Studios Inc. v. Gorkster Ltd.*, 545 U.S. 913, 919 (2005).

<sup>106</sup> *See Tiffany (NJ) Inc. v. eBay, Inc.*, No. 04 Civ. 4607, 2008 WL 2755787 at \*1 (S.D.N.Y. July 14, 2008) (citing *Inwood Labs., Inc. v. Ives Labs., Inc.*, 456 U.S. 844, 854 (1982)).

<sup>107</sup> *See* eBay, How eBay Protects Intellectual Property (VeRO), <http://pages.ebay.com/help/tp/programs-vero-ov.html> (last visited Dec. 10, 2008).

<sup>108</sup> *Tiffany*, 2008 WL 2755787 at \*9.

<sup>109</sup> *See* Gramm-Leach-Bliley Act § 504, 15 U.S.C. § 6804 (2000) (requiring specified federal agencies to adopt rules restricting the ability of certain financial institutions to "disclose nonpublic personal information about consumers").

registered investment advisers' ability to utilize customers' personal nonpublic information.<sup>110</sup> Bank regulators enacted similar rules.<sup>111</sup>

The Internet has both increased and decreased the cost of law enforcement. It is unclear what the net costs are. The increased costs are caused by the global impact of the Internet beyond state boundaries. The decrease is based mainly on ease of communication, such as consumers' complaints, information from other agencies and other countries, and technical innovations, such as surfing the Internet for fraudulent advertising.<sup>112</sup>

The FTC operates a program called "Surf Days" in which employees of various agencies surf the Internet looking for Web sites containing solicitations, which likely violate the law.<sup>113</sup> The FTC also operates the "Consumer Sentinel Network," which allows participating law enforcement access to a database of complaints given to the FTC from consumers and participating organizations including the BBB.<sup>114</sup> These programs utilize the benefits of the Internet, such as ease of searching and instantaneous communication, to help law enforcement.

The Internet and the law affect each other. For example, the contract rule of caveat emptor is sufficient to create trusting among buyers and sellers in face-to-face relationships, but not in e-mail communications. Hence, contract doctrine may change and become more "fiduciary-like" and customer friendly. The requirement to tell the truth and be reliable will not be linked to the parties' explicit agreements, but to the default rules that underlie fiduciary law or to stronger fairness concepts in contract law. These may creep into, and create, the "contract law of the Internet." Not only will these rules reflect best practices of industries doing business on the Internet, but they also will be recognized as crucial to the development of e-business, and as such, acquire the power and weight sufficient to change legal doctrine.

<sup>110</sup> Privacy of Consumer Financial Information (Regulation S-P), Exchange Act Release No. 42,974 (June 22, 2000), 65 Fed. Reg. 40,334 (June 29, 2000) (codified as amended at 17 C.F.R. pt. 248 (2008)).

<sup>111</sup> Surf Days are days when staff members from certain governmental and private agencies band together and surf the Internet for suspicious Web sites. The suspicious sites are downloaded as evidence and an e-mail warning is sent to the Web sites that explains the law and links them to the FTC's Web site. After a short period of time has passed law enforcement teams visit the sites to see if the suspicious behavior has been suspended. Between 20 and 70 percent of sites that receive the e-mails end up complying with the warnings. See Privacy of Consumer Financial Information, 65 Fed. Reg. 35,162 (June 1, 2000) (codified at 12 C.F.R. pt. 332 (2008)).

<sup>112</sup> For a discussion on various cost reduction methods in prosecuting Internet fraud cases, see Patrick E. Corbett, *Prosecuting the Internet Fraud Case Without Going Broke*, 76 Miss. L.J. 841 (2008).

<sup>113</sup> See Eric Carlson, *Phishing for Elderly Victims: As the Elderly Migrate to the Internet Fraudulent Schemes Targeting Them Follow*, 14 ELDER L.J. 423 (2006).

<sup>114</sup> <http://www.ftc.gov/sentinel>.

## 5. The Role of Technology in Support of Trusting

Technology has helped reduce customers' risks by eliminating the need to send card account information over the Internet directly to sellers. While the solution is not yet certain, it seems clear that the issue must be resolved if consumers are to consider the Internet as their main form of communication with businesses.

In some situations, enforcing the law against violations on the Internet may be as easy as, or even easier than, enforcing the law in real space. In recognition that "code is law," as Professor Lawrence Lessig argues, government may regulate certain aspects of Internet operations through code—the means of Internet communication.<sup>115</sup> It is likely that the government will use this method to fight against serious crimes, which the Internet greatly facilitates. This method raises issues of government accountability that are beyond the scope of this paper. But technology and government protection can prompt distrust and eliminate some trusting behavior, as Professors Lessig and Helen Nissenbaum note.<sup>116</sup>

The solutions devised to date are operational, technological, and organizational. On the operational and organizational side, experts suggest that consumers avoid some forms of payment on the Internet, such as debit cards. These cards resemble cash and are too risky. Processes, such as the process by which credit cards are settled, may have to change. Credit card transactions that follow real world processes, from the merchant to a merchant processor and then to a credit card processing association, expose the parties to risks from thieves. Among others, a safer approach is to let the merchant directly query the credit-card-issuing bank for payment authorization. Non-face-to-face merchants are required to take an additional step when they authorize a purchase. Businesses are using different payment systems for online shopping, such as digital certificates. There are digital identity services and technical forms of authentication that help reduce consumers' risk. Non-technical solutions are also recommended, such as the use of employees for internal controls, response to possible threats and risks, and the hiring of experts.

On the technological side, businesses are adopting technical solutions to protect against third-party attacks on the Internet business. These include antispamming software and filters against "denial of service attacks." Most companies have installed secure sockets layer (SSL) mechanisms to protect Web transactions.<sup>117</sup> Unfortunately, phishers

<sup>115</sup> See LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999); Lawrence Lessig, *Preface to a Conference on Trust*, B.U. L. REV. 329 (2001).

<sup>116</sup> See Lessig, *supra* note 115, and Helen Nissenbaum, *Securing Trust Online: Wisdom or Oxymoron?* 81 B.U. L. REV. 635 (2001).

<sup>117</sup> See Peter P. Swire, *Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy*, 54 HASTINGS L.J. 847 (2003).

have discovered ways to acquire SSL certificates and thereby create a false sense of security by displaying the padlock icon, which appears on the browser bar when a Web site has an SSL certificate, on their fraudulent Web sites.<sup>118</sup> Businesses injured by harmful misinformation that frightens customers away use trusted sources to combat these harmful effects. In addition to having SSL certifications, Internet businesses often utilize trusted third parties, such as VeriSign, to serve as another source of authentication for consumers. So rather than just relying on the padlock on their browser bars, careful consumers can click on the VeriSign seal and receive real time updates on the status of the Web site's SSL certification, and confirmation that the site is what it claims to be and not a fake designed by a phisher to steal their personal information.<sup>119</sup> The important point is that corrections come from a trusted source. And, of course, some businesses choose not to disclose the problems they have, but to simply correct them.

Online dispute resolution (ODR) is a growing field with a plethora of tools and services that can be used to foster online trust. ODR can best be described as any method of alternative dispute resolution, such as mediation or arbitration, that utilizes the Internet.<sup>120</sup> While traditional legal remedies are important tools in the upholding of online trust, some problems are best solved through alternative means. Recent numbers show that the average transaction on the Internet is approximately \$146.00; considering the costs and effort of pursuing legal remedies for disputes regarding Internet transactions, it is simply not worth it for most people to seek legal recourse in online transaction situations.<sup>121</sup> This knowledge combined with the frequency of online scams makes the use and evolution of different forms of ODR critical to the maintenance of an online culture that can sustain trust. EBay's online mediation service SquareTrade illustrates the impact an ODR system can have in maintaining a trusting online environment. From February 2000 to June 2004, SquareTrade resolved over 1,500,000 disputes.<sup>122</sup> A large number of these disputes would not have been settled without SquareTrade or some other form of ODR, and thousands of

<sup>118</sup> The problem of fake SSL certificates is being combated by the introduction of a new form of SSL certification called Extended Validation Secure Socket Layer certification (EV SSL), which adds a green bar in addition to the familiar padlock to verify the safety of a Web site. See Byron Achohido, *Don't Do Business Online Without the Green Bar*, USA TODAY, June 6, 2008, <http://blogs.usatoday.com/technologylive/2008/06/dont-do-business.html>.

<sup>119</sup> See VERISIGN UK LTD., ESTABLISH TRUST TO PROTECT AND GROW YOUR ONLINE BUSINESS, <http://www.verisign.co.uk/static/029631.pdf> (last visited Dec. 10, 2008).

<sup>120</sup> See Philippe Gilliéron, *From Face-to-Face to Screen-to-Screen: Real Hope or True Fallacy?* 23 OHIO ST. J. ON DISP. RESOL. 301 (2008).

<sup>121</sup> See *id.*

<sup>122</sup> See *id.*

consumers presumably would have been left even more dissatisfied with their online auction experiences.

Digital identities (DIDs) also play an important role in the cultivation and maintenance of Internet trust going forward. Identification and verification are difficult to achieve on the Internet, which in turn makes the development of trust difficult to achieve as well. When interacting with others in the physical world, we use our real names, look at each other's faces, and can show government-issued identification. On the Internet we are primarily identified through various pseudonyms, which are usually only verified through the use of single passwords. The relative anonymity and lack of security with respect to this system seriously hinder trust relations on the Internet because people have virtually no way of verifying who the person behind the pseudonym is. However, there has been progress in the realm of verification and DIDs that should prove conducive to trust building on the Internet. One advance that has been gaining steam in certain areas is the use of biometrics in identification.<sup>123</sup> By requiring a fingerprint or retinal scan in addition to a password, a physical connection is made with the user that provides a very solid form of verification in that it cannot be easily replicated or stolen by a third party or given away by the user. Another method to improve the authenticity of DIDs that has been proposed is to make a "second layer" of identification on the Internet referred to as "Identity 2.0."<sup>124</sup> Instead of carrying multiple usernames and passwords, users under Identity 2.0 would have a single online identification that they would use for banking, shopping, e-mailing, and other online activities. Under this model, DIDs would be closely tied to the individual user and would produce an accurate online reputation to reflect the user's dealings on the Internet.

With every passing year the Internet becomes further integrated into our lives. Trust on the Internet becomes increasingly important. This is especially true in the case of Internet voting, which may play a very important role in the future of democracy. Internet voting has already been used widely by corporations for the purpose of shareholder voting,<sup>125</sup> and millions use the Internet for extremely important activities such as banking and paying taxes. However, it must be recognized that the use of Internet voting for democratic elections would bring certain problems with it. While current voting methods are not 100 percent fraud-proof, they have earned the trust of the voters. The Internet opens up whole new possibilities of fraud, verification problems, and exclusivity, which could have potentially devastating

<sup>123</sup> See Aresty, *supra* note 54 at 154–55.

<sup>124</sup> See *id.* at 153–54.

<sup>125</sup> See Joshua F. Clowers, *I E-Vote, U I-Vote, Why Can't We All Just Vote?!: A Survey of the Changing Face of the American Election*, 42 GONZ. L. REV. 61 (2006).

effects on an election. One hurdle that Internet voting would have to overcome is the current “digital divide.”<sup>126</sup> That is, while in theory Internet balloting would make voting more accessible for the masses, it would really only serve to further widen the gap between the rich and the poor voters, as the rich are far more likely to have Internet access. Beyond this problem are the various new security issues that would crop up. A recurring theme in the discussion of Internet trust is the problem of verification, which would be especially problematic in the context of Internet voting. Since the voting would be taking place away from a polling station, there would also be greater opportunity for voter bribery or coercion, as a third party could be present while the voter cast his votes.<sup>127</sup> Lastly, there is the ever-present danger of hackers manipulating voter data or otherwise disrupting the system.<sup>128</sup> Even if these problems can be dealt with, as long as there is the public perception that Internet voting is less trustworthy than the current voting forms, Internet voting should be refined to put to rest the public’s doubts.<sup>129</sup> If trust cannot be established in Internet voting to the extent that it is already established in current voting procedures, then it should not be adopted.<sup>130</sup>

## 6. Conclusion

In real space and on the Internet, trust and non-trust pose the same issues. The ways people come to trust in real space and cyberspace differ, however. That is mainly because the benefits, costs, and risks in Internet interaction have changed and have been reallocated among

<sup>126</sup> The “digital divide” is “an invisible chasm sitting between those in society who have the means to own—or at least have access to—a computer, BlackBerry, or mobile phone with Internet connectivity and those who do not.” See David M. Thompson, *Is the Internet a Viable Threat to Representative Democracy?* 2008 DUKE L. & TECH. REV. 10, 26.

<sup>127</sup> See Clowers, *supra* note 125, at 83.

<sup>128</sup> Security patches are implemented in response to threats, and Internet security is in a constant state of catch-up with the latest dangers. Since there is an inevitable lag between the aggressors and the defenders of Internet security, some feel that Internet voting will never be a safe or viable alternative to traditional methods. See *id.* at 86–87.

<sup>129</sup> Absentee ballots have a lot of the same security issues as Internet voting, such as coercion and fraud, yet they are for the most part trusted and have been widely accepted and used by the populace. See Bryan Mercurio, *Democracy in Decline: Can Internet Voting Save the Electoral Process?* 22 J. MARSHALL J. COMPUTER & INFO. L. 409 (2004).

<sup>130</sup> “If voting technology mediates the relation between people and democracy in such a way that the experience of trust and stability is reduced, for whatever reason, the actions that are invited are political passivity on the one hand, and protest and obstruction on the other.” See W. Pieters & M. J. Becker, *Ethics of E-Voting: An Essay on Requirements and Values in Internet Elections*, in *ETHICS OF NEW INFORMATION TECHNOLOGY: PROCEEDINGS OF THE SIXTH INTERNATIONAL CONFERENCE OF COMPUTER ETHICS: PHILOSOPHICAL ENQUIRY* (Philip Bray, Frances Grodzinsky & Lucas Introna eds., 2005).

sellers and buyers. The costs have shifted to sellers in order to achieve the same goal—establishing trusting relationships on which economic activity depends.

The model that emerges is that of “layered trusting supports.” No one layer can create a culture of trust. Reputable institutions and intermediaries, verifiers, and providers of trust services contribute to public trusting. But more of them are needed on the Internet, and the law must continue to provide the backbone of legitimacy for their trustworthiness. Perhaps stronger support is needed on certain issues. For example, the Internet offers grand-scale opportunities to destroy software in which communications and ideas are stored. To prevent such destruction we may need a worldwide meta-norm. Today, destructive hackers are not just the “smart kids” who playfully show off their genius.

Hackers have become vital centerpieces in organized crime and terrorist groups, both as weapons and sources of funding through frauds such as identity theft.<sup>131</sup> As hacking has been increasingly integrated into larger criminal schemes, focus has intensified on finding ways not only to provide greater security on the Internet but also to change the culture that nurtures and develops these hackers.

Against such damaging games, there is no strong norm that brings a general revulsion. If children were told, with their first computer, that computers are for creating, not for destroying, and develop this attitude as they develop the inhibition about playing with matches to avoid destruction—while recognizing that fire is good, as the parents show by lighting candles and the fireplace—then over time a meta-norm can rise to be enforced not only by governments but also by the public. As the meta-norm becomes stronger, law’s interference can become weaker. But this is a goal for the future. We can begin by using the tools, based on the elements of benefits, costs, and risks, and adjusting them to the new Internet environment.

Tamar Frankel, Professor of Law  
Boston University School of Law  
765 Commonwealth Ave., Room 1144  
Boston, MA 02115  
Phone: (617) 353-3773  
Fax: (617) 353-2444  
E-mail: Tfrankel@bu.edu

---

<sup>131</sup> See Michael Ena, *Securing Online Transactions: Crime Prevention Is the Key*, 35 FORDHAM URB. L. J. 147 (2008).

