Technology Trust: An Inventory of Trust Infrastructures for Government and Commercial Information Systems In Support of Electronic Commerce

Susan K. Lippert
Drexel University, Philadelphia, United States

lippert@drexel.edu

Abstract

Electronic business transactions have exploded in the 21st century. End users rely on Internet security and privacy systems for safeguarding personal information and protection from unauthorized use. While these systems focus on safety, security and privacy, infrastructures supporting predictability, reliability and utilization of technology, classified as *technology trust*, are underdeveloped. This benchmark review will identify, catalog, and report on existing technology trust structures within commercial and government electronic networks. Increased trust in technology leads to more effective utilization and rapid adoption of electronic commerce. The technology trust elements can have a profound affect on speed and efficiency of technology adoption, use, and acceptance.

Keywords: technology trust, electronic commerce, trust structures, technology adoption, technology acceptance, benchmark, technology predictability, technology reliability, technology utility

Introduction

Trust in information systems technology is becoming more important to academics (Lippert, 2001b) and practitioners (Lippert, 2001c, 2001d) alike. The notion of technology trust (Lippert, 2001a, 2002) attempts to quantify what is meant by the user's trust in the inanimate information systems technologies – hardware and software – employed in daily life. Various organizations provide privacy assurance services including TRUSTe, BBBOnline, and WebTrust. Each of these assurance seals are designed to increase trust in privacy and security associated with commercial website applications. Some IS research has investigated commercial Internet trust symbols (Sivasailam, Kim & Rao, 2002) as dimensions of web assurance in business to consumer (B2C) electronic commerce.

Electronic commerce has exploded within the last several years from almost $40 Billion in B2C revenues in 2000 to an estimated revenue output of over $125 billion by 2004 (http://www.emarketer.com/about_us/press_room/press_releases/103100_eb2c.html). An underlying structure to electronic commerce is the technology itself, which facilitates the transactions. As commerce has grown and technology developed, the consumer structures – both individuals (consumer to consumer, C2C and B2C) and organizations (B2C and business to business, B2B) – have identified the need for infrastructures that create and promote trust. An alternative notion of technology trust – the Trust in Information Systems Technology (TIST) model – attempts to expand the concept of trust to the user of the information systems technology.

The U.S. Government determined that the commercial sector lead in the development of trust infrastructures. Recognition of trust issues has been demonstrated by the government through a variety of programs, policies, and practices that encompass

a restricted approach to trust in information systems technology.

A combined 1991 National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) initiative resulted in the establishment of the Trust Technology Assessment Program (TTAP) (http://csrc.nist.gov/ttap/, http://radium.ncsc.mil/tpep/ttap/conceptpaper.txt, http://www.radium.ncsc.mil/tpep/ttap/TTAPpaper.html). The TTAP concept is a product evaluation and certification effort aimed at increasing the number of trusted commercial "off-the-shelf" products to both government and commercial consumers through quality assurance. With three goals, the TTAP is geared toward (1) increasing the number of evaluated IT products beyond vendor specific security claims, (2) conducting shorter and more timely product evaluations, and (3) establishing international reciprocity of evaluations, standards and certification procedures (www.radium.ncsc.mil/tpep/library/ramp-modules/mod_02.txt). The purpose of this program is to offer customers an independent, expert evaluation of vendor security claims.

While the United States has taken an active role in establishing evaluation and certification programs, several national governments have developed international standards for trusted product evaluation programs (http://www.radium.ncsc.mil/tpep/library/ramp-modules/mod_02.txt). International efforts within Australia, Canada, France, Germany, the Netherlands, New Zealand and the United Kingdom were directed toward the creation of hardware and software evaluation criteria. Efforts for "common criteria" will enable acceptance of evaluations conducted in one country to be adopted within another country.

Steinauer, Wakid & Rasberry (1997) of the National Institute of Standards and Technology (NIST), Information Technology Laboratory, investigated trust and traceability in electronic commerce. Trust, in this context, referred to the "confidence that participants in commerce have that their activities (transactions and other exchanges of information, goods, and services), will be protected and conducted as intended" (http://nii.nist.gov/pubs/trust-1.html). The authors' focused on the commercial aspect of electronic commerce where trust is increased through risk transfers to vendors such as credit card companies. An additional component of this exploration includes the notion of "trustworthy" which arise from systems or processes demonstrating trustworthiness in the past. Trust is enhanced if participants know that the transaction elements are traced from origin to completion or when endorsements from major firms, the U.S. Government or other respected organizations attest to adoption of a certain process, product, or technology.

Other government reports address public/private encryption key technology as a mechanism for agencies to safely replace paper forms of communication (http://www.accessamerica.gov/text/privacy.html). In the Steinauer, Wakid & Rasberry report, the government offers a privacy and security guarantee that addresses issues of integrity and confidentiality. *Integrity* exists because the data maintained within the system is secure from unauthorized modification. *Confidentiality* connotes the inaccessibility of private information to unauthorized parties.

A 1997 report from the National Performance Review and the Government Information Technology Services Board cited the importance of improving the public's access to government services (http://www.accessamerica.gov/reports/public2.html) and the need to implement nationwide, integrated electronic benefits transfer (http://www.accessamerica.gov/reports/ebt.html). The United States Government provides an electronic commerce policy (http://www.ecommerce.gov), which offers a framework for global electronic commerce. These reports address trust in the processes of electronic transactions, but do not investigate nor report on user trust of the technologies themselves – the information system technology.

The purposes of this monograph are to identify, catalog, and report on existing technology trust structures within electronic networks; to establish the need for technology trust within both government and commercial systems; and to propose an additional view of technology trust (TIST). Technology trust structures are bounded by measures of technology predictability, reliability, and utility. Technology predict-

ability involves the degree to which a user can determine that the technology will be working in the future based on past usage experiences. Technology reliability is the degree to which the technology is up and running on the day and time needed by the user to access information from an electronic source. Technology utility is a measure of usefulness in terms of accessing information from the site/source and whether the available information meets the user's needs. Dependence upon technology is the requisite use of hardware and software to accomplish the task. Predilection to trust technology is a generalized expectancy held by an individual that technology related to his/her reliance upon technology. Technology trust is the willingness to be vulnerable to the information systems technology based on expectations of predictability, reliability and utility and influenced by one's predilection to trust technology (Lippert, 2001a). Figure 1, a Model of Trust in Information Systems Technology (Lippert, 2001a) graphically depicts the relationship between technology trust and its associated constructs.

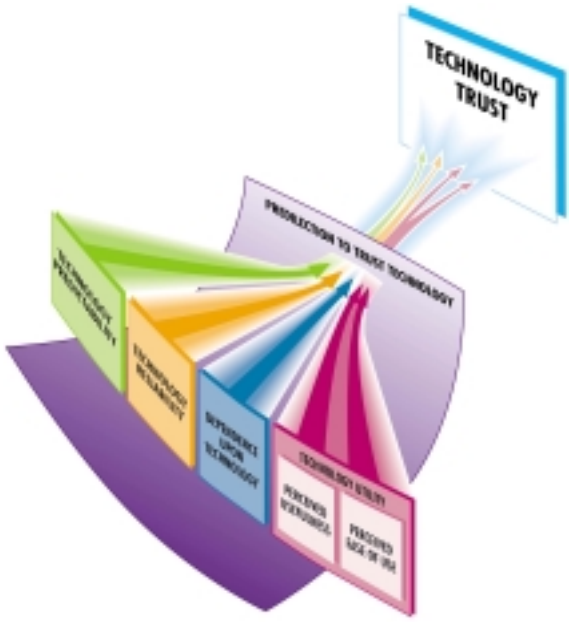

Figure 1: Model of Trust in Information Systems Technology (Lippert 2001a)

There are many programs, applications, systems and products that deal with trust. Within the context of this manuscript, an inventory is provided in order to explicate and categorize the nature and degree of technology trust as practiced by government and commercial enterprises. Any inventory of programs/systems, must insure that the nature of trust within the context of a program, application or product is defined. Trust as an end state of the use of technology can be applied to either the technology or to the outcome from using the technology. The following provides some identification, classification and cross-references for technology trust as practiced both within the U.S. Government and through commercial applications. Note that the nature of technology trust in these cases refers to issues of trust by the consumer of the outcome of technology and not necessarily the technology proper. The Trust in Information Systems Technology Model has application to each of these programs, systems, application and products directly linked to the technology utilization process – the use of software and hardware to accomplish a goal.

Current Commercial and Government Infrastructures

TRUSTe Program

TRUSTe (http://www.truste.org/index.html), commenced in March 1996, is a global nonprofit initiative designed to build user trust and confidence in the Internet. TRUSTe functions as a third-party oversight mechanism, which is independent of both industry and government. The initiative includes a "seal" pro-

gram aimed at accelerating Internet growth by alleviating users concerns about online privacy. Web sites that display the TRUSTe seal abide by four tenets, regarding the handling of consumer data, set forth by the program. These principles include: (1) notice, (2) choice, (3) access, and (4) security.

Companies provide written and accessible on-line *notice* of what consumer information is collected and with whom this personal data is shared. Users are given the *choice* to prevent a website from "selling, sharing, renting, or disseminating" (http://www.truste.org/index.html) their information which uniquely identifies the individual. Reasonable *access* to personal information is mandated as part of this program while *security* necessary to protect the collected data is a requirement. On-line businesses, which meet the program's core requirements for data gathering and dissemination, may include the visual TRUSTe symbol on their website. The TRUSTe program is geared toward increasing user trust in the online business so as to facilitate purchases and/or providing personal information online. The TRUSTe campaign began the process of building guidelines to support Internet safety, security and privacy in online transactions (http://www.truste.org/resourcebook.html).

BBBOnline

BBBOnline is a Better Business Bureau product (http://www.bbbonline.org/privacy), which offers a reliability program for online businesses. The BBB privacy seal provides a measure of consumer confidence that the Internet business is reputable and trustworthy. The BBBOnLine Privacy Program awards the privacy seal to businesses meeting four established standards. These include: (1) disclosing online enterprise privacy principles, (2) obtaining a BBB privacy assessment, (3) agreeing to a review and monitoring by a third-party, and (4) participating in the BBB consumer dispute resolution process.

Two seal programs, the reliability seal program and the privacy seal program, are available through the BBBOnLine programs. The *BBBOnLine Reliability seal* is designed to inform potential consumers that a "sealed" enterprise upholds four practices: (1) has an ethical level of operation, (2) has existed as a business for a minimum of one year, (3) has a clear/clean record with the Better Business Bureau, and (4) is willing to employ dispute resolution through the Better Business Bureau when disagreements between customers and vendors/enterprises arise. The *BBBOnLine Privacy seal* offers customer protection that certified enterprises engage in ethical treatment and practices of personally identifiable information. A *BBBOnLine Japanese Privacy seal* is available as a secondary privacy protection. This partnership with the Japanese Privacy Seal authority (JIPDEC) (http://bbbonline.org/privacy/jipdec.asp) offers a combined seal recognized in both the United States and Japan.

An advantage of the BBBOnLine Reliability seal and the BBBOnLine Privacy seal is the Better Business Bureau name recognition and reputation that succeeds from the brick and mortar marketplace. Several surveys and testimonials (http://www.bbbonline.org/reliability/benefits.asp) promoted by the BBBOnLine program assert that sites receiving this certification are among the most trusted on the Internet because of the BBB reputation.

WebTrust

WebTrust is a program (http://www.cpawebtrust.org/onlnover.htm) that offers independent verification for customers that the website satisfies requirements set forth to minimize risk and fraud and to protect the customer's privacy. The WebTrust seal is designed to build customer trust and confidence in online business commerce. The principles of WebTrust are designed to cover four enterprises: (1) business to consumer (B2C) sites; (2) business to business (B2B) activities; (3) service providers; and, (4) certification authorities. Certification is offered by CPAs who certify that the enterprise website complies with the international WebTrust Standards for electronic commerce. Enterprises receiving WebTrust certification disclose their policies related to the established WebTrust standards. WebTrust maintains seven standards

including (1) online privacy, (2) confidentiality, (3) security, (4) business practices and transaction integrity, (5) availability, (6) non-repudiation and (7) customized disclosures.

The practice of *online privacy* ensures that personal information, which identifies consumers, is protected through the inclusion of an online privacy statement. The privacy statement addresses four privacy elements including (1) the use of cookies, (2) the use, distribution, and modification protocols associated with collected personally identifiable information, (3) the sources of information collected, and (4) guidelines for declining collection of information. *Confidentiality* pertains to the safeguarding of collected information so that access and dissemination is restricted to authorized and intended individuals and sources. Procedures pertaining to *security* address the issue of restricting access to legitimate individuals, and establishment of policies and procedures to handle security breaches, disaster recovery, system backups and encryption protocols.

Enterprises certified with the WebTrust seal are expected to completely and accurately disclose their *business practices* and to ensure *transaction integrity*. This standard includes informing consumers of enterprise practices including transaction timeframes, payment and delivery terms, descriptions of merchandise condition, assurance that goods and services are provided as requested, canceling orders, and customer service. *Availability* addresses the terms and conditions associated with system and data accessibility including assurances that hardware and software meet availability objectives. WebTrust certified enterprises ensure the authentication and integrity of electronic messages and transactions. *Non-repudiation* clauses pertaining to user authentication, safeguards against unauthorized use, and establishment of liability levels throughout the transaction process are set forth within the sixth WebTrust standard. *Customized disclosures* including the number of site hits within a specific timeframe and the size of the website business are made available (disclosed) to enterprise users.

The WebTrust enterprise certification accomplished through the seven standards are designed to communicate a level of trust, security, privacy and confidence in the process of electronic transactions to current and potential enterprise customers. These standards offer customers a procedurally based threshold for developing confidence in the online enterprise.

Online Privacy Alliance

The Online Privacy Alliance (http://www.privacyalliance.org/businesses/) is a multi-disciplinary industry-based coalition committed to promoting individual online privacy (http://www.privacyalliance.org/facts/). The Alliance uses a self-regulatory enforcement procedure to insure compliance; has a specialized feature in the creation and proliferation of standards and policies for online use by minors less than 13 years old; and supports the existence and use of certification standards and seals.

More than 80 global companies and associations comprise the Online Privacy Alliance (OPA) that began in 1998. The alliance aims to define online privacy policies and to offer guidelines for businesses, consumers and children regarding steps an individual should take to ensure privacy of personally identifiable information. Five essential elements to online privacy are identified: (1) adoption and implementation of a privacy policy, (2) notice and disclosure, (3) choice/consent, (4) data security, and (5) data quality and access.

The first guideline addresses the importance of establishing a *privacy policy* to protect consumer's personally identifiable information. Enterprises are encouraged to share best practices with business partners in order to establish a responsible sequence of steps aimed at protecting individual privacy.

Notice and disclosure involves a formal announcement to the consumer of seven specifications of personal information privacy: (1) what information can be collected, (2) how that information will be used, (3) how the information will be distributed, (4) what choices are available to the individual in the information collection procedures, (5) how data quality assurance is maintained, (6) how access is controlled, and

(7) through a formal statement of commitment to data security. These notifications must be explicitly identified and made available to the consumer prior to or at the time the personally identifiable information is collected. *Choice/consent* enables the consumer to decide how his/her information may be used beyond the original purpose for which the information was collected. Guidelines include a provision for consumers to choose that their information be excluded. Consumer's consent for third party use and distribution is required as part of this privacy standard. *Data security* consists of organizational systems that protect information through reasonable precautions and procedures to protect against loss, alteration, or misuse. *Data quality and access* involves enterprise responsibility to ensure the accuracy, completeness and timeliness of information. In the event of error, timely correction is required.

Trusted Product Evaluation Program

The Trusted Computer System Evaluation Criteria (TCSEC) and the Trusted Product Evaluation Program (TPEP) emerged in response to the need for basic requirements for secrecy, integrity and availability of government information assets. These initiatives have roots in a 1967 task force assembled by the Defense Science Board charged with identifying computer security safeguards designed to protect classified information maintained on government computer networks. Later efforts sponsored by the Department of Defense (DoD) and the National Bureau of Standards (now known as the National Institute for Standards and Technology – NIST) in the 1970s resulted in an initial set of computer security evaluation criteria. These criteria were designed to evaluate the degree of trust an individual could place in the hardware and software to protect sensitive data. (For an extensive historical perspective, see http://www.radium.ncsc.mil/tpep/library/ramp-modules/mod_01.txt). Evaluation criteria developed from these and several other ongoing efforts between 1967 and 1989 resulted in three principals (confidentiality, integrity, and availability) required to ensure computer security. The principals deal with unauthorized disclosure, manipulation, or use of information and resources. *Confidentiality*, also referred to as secrecy, involves controlling unauthorized disclosure of information. *Integrity* involves thwarting unauthorized changes to information or information resources. *Availability* involves preventing the unauthorized delay or denial of use of information and resources.

Technology Trust Assessment Program (TTAP)

Premiered in January 1997, the Trust Technology Assessment Program (TTAP) functions as a joint effort between the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) (http://radium.ncsc.mil/tpep/ttap/basics.html). The TTAP effort is designed to oversee the evaluation of commercial-off-the-shelf (COTS) products to ensure a greater number of evaluated products for both the classified and non-classified communities (Connolly & Abramowitz, 1995; Flahavin & Toth). Products include both hardware and software such as IBM AS/400, Oracle 7, SQL Server 2000 Version 8.0, and Trusted IRIX/B by Silicon Graphics Inc. (http://www.radium.ncsc.mil/tpep/epl/historical.html). The TTAP functions within five specific objectives aimed at providing users with secure and acceptable products. Objective 1 is geared toward providing Federal government users with product evaluations when needed. Objective 2 is aimed at providing a single US-based evaluation of all worldwide products. Objective 3 asserts that evaluation criteria and assurances be easily understandable by all individuals who are required to utilize this technology. Limiting resource consumption including time, effort and cost are the central tenets of objective 4. Objective 5 is directed toward increasing trust in these evaluated products. The TTAP program offers a mechanism for both the government and private sector to evaluate products and certify these products as "trusted" through systematic evaluations achieved at reasonable costs. This enables vendors to sell more "trusted" products and users to purchase a wider variety of products.

Trust and Traceabilty in Electronic Commerce

In September 1997, Steinauer, Wakid & Rasberry (http://nii.nist.gov/pubs/trust-1.html) suggested that two elements, trust and traceability, are necessary concepts in the electronic commerce infrastructure. *Trust* was defined as "the confidence that participants in commerce have that their activities (transactions and other exchanges of information, goods, and services) will be protected and conducted as intended" (http://nii.nist.gov/pubs/trust-1.html). *Traceability* occurs when a purchaser can track each step in the purchasing process to show the procedural activities, which transpired along the transaction route. The notion of traceability enables an individual or organization to be held accountable based on receipts, sales slips, or transaction records.

Trustworthy operations occur if a system or process was found to be "trustworthy" by an individual based on past experience. Trustworthy protocols include identification and authentication needed to achieve a level of system trust thereby guarding against unauthorized access and use. Several authentication options – smart cards, tokens and biometrics – are offered as replacements to passwords. Although smart cards and tokens are active security devices, the potential for duplication and theft make these devices less desirable than the use of fingerprint technology. Using a fingerprint biometric for authentication purposes facilitates information access through a higher level of secure identification.

Integrity refers to the reliability of the data and information maintained within the system. Integrity of data is maintained by controlling information modification and through detection protocols designed to identify information changes. *Confidentiality* of information can be controlled through encryption mechanisms. Given that several parties are generally involved in a single transaction, a level of confidentiality is required to ensure protection of personal data. These technological solutions help to build and sustain system confidence between buyers and sellers. However, these trust mechanisms deal with process issues of trust rather than trust in the technology itself.

Trusted Network Interpretation Environments

The National Computer Security Center (NCSC) (http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-011.html#HDR1.1%20%20%203%2018) establishes and maintains technical standards and criteria used to evaluate trusted computer systems. NCSC guides how new security technology is used by (1) establishing a categorization system based on the level of security protection offered by the technology, and (2) determining the minimum-security protection required in different threat environments.

Computer systems are categorized into hierarchical classes based on the evaluation of security features and assurances. Document standards exist for both stand-alone computer systems (the TCSES Environment guidelines) and for networks (the TNI guidelines). These guidelines include procedures for determining security level requirements. A combination of data classification and user security clearance is connected to compute a risk index determining the NCSC evaluation rating assigned to the system. An overall risk assessment is used to determine security requirements unique to each site or setting.

International Safe Harbor Privacy Principles

In 1998, the European Union (EU) initiated a directive on data protection aimed at establishing privacy safeguards for non-European Union countries (http://www.ita.doc.gov/td/ecom/shpirn.html). The seven principles developed as part of the international safe harbor privacy policy are designed to protect personally identifiable information of European Union residents when collected by U.S. corporations. These principles were solely designed for this unidirectional "safe harbor" of personal EU resident data. The seven principles include: (1) notice, (2) choice, (3) onward transfer, (4) security, (5) data integrity, (6) access, and (7) enforcement.

Notice refers to organizational disclosure of use, purpose and dissemination of personally identifiable information. Notification must be available to consumers before or at the time the information is collected. Furthermore, notification is required prior to dissemination to a third party. *Choice* enables individuals to exclude their personal information from disclosure to third parties. Explicit choice must be given to individuals before sensitive information such as personal medical or health data is transferred to a receiving source. *Onward transfer* prohibits the disclosure of personal information to third parties, unless explicit permission is obtained and the third party adheres to the safe harbor privacy principles.

Organizations are expected to ensure *security* of information through policies and procedures aimed at protecting private data from loss, misuse, alteration, destruction, disclosure and unauthorized access. The *data integrity* principle guarantees data that are current, accurate and complete. *Access* permits individuals to obtain their personal information for correction or modification purposes. The safe harbor principles are protected through *enforcement*, which offers recourse in situations where non-compliance occurs.

Safe harbor principles establish a control mechanism for members of the EU whose personal information may be collected, used or disseminated to a United States corporation. These principles facilitate the maintenance of U.S. law enforcement and EU public interest through adherence to guidelines designed to establish international safe harbors.

ISO 9000 and ISO 14000

The International Standardization Organization (IS0) is an association that sponsors the creation of international standards for products and services (Clinton, 1995; http://www.isoeasy.org/.). ISO 9000 and 14000 represent widely known and successful specifications for products and processes. ISO 9000 is an international standard for quality requirements in business-to-business (B2B) transactions. ISO 14000 is an international standard for environmental management challenges. Both ISOs are generic in nature, however ISOs are continually developed that address specific product, material, or process specifications.

These generic management standards ensure specification transferability to any organization or to products, services, or activities regardless of size. ISO 9000 addresses quality management through fulfillment of regulatory requirements and by enhancing customer satisfaction. ISO 14000 is primarily concerned with environmental management. This standard guards against harmful environmental outcomes of organizational activities or practices.

Global Information Infrastructure (GII)

The U.S. Government recognizes that the future will be influenced through merging electronic technology and commerce. Changes in information system processing, both quantity and type, proliferate the world scene through international networks, most notably the Internet. The new millennium has brought a different government view of its relationship to enterprise processes. The Government has adopted a set of policies that both recognize these changes and facilitate development of electronic commerce. The government continues to employ a non-regulatory, market-oriented approach to transactions facilitated by technology.

The Global Information Infrastructure (GII) (http://www.giic.org) is both a vision and a goal. The vision is for an infrastructure to support global electronic information exchange that addresses growth, technology advancements and security. The goal is to continue to build infrastructures that support the vision, through public support for a global and mobile marketplace. Standardization efforts, for electronic commerce are aimed at the global economy and use international standardization bodies, such as ISO.

The GII began in 1995 and continues through changes in U.S. governing administrations. This initiative embraces five principles and supports public policy congruent with those principles.

1. The private sector takes the lead in the infrastructure development (engineering, prototyping and funding);
2. Governments will avoid restrictions that limit the development of electronic commerce at the market's pace;
3. When required, a minimalist approach to government involvement will support and enforce a simple legal environment for conducting commerce;
4. Government will recognize the unique technological qualities of the Internet which can encourage innovative online ventures; and,
5. Electronic commerce through the Internet should function at a global level without encumbrances, such as import/export tariffs.

The Need For An Additional Perspective of Technology Trust

The need for trusted systems and what constitutes trusted systems have been thoroughly investigated and partially addressed within the commercial sector. To a lesser extent, the U.S. Government has also recognized the effect of trust on electronic commerce. A clear need exists for trust systems in all venues of electronic functions, including commerce, management, operations and development. Electronic commerce is accomplished using information systems technology, commonly identified as the computer hardware and software.

Unfortunately neither the commercial sector nor the U.S. government has addressed technology trust (Lippert, 2001a) from the prospective of trust in the technology itself. The current notions of trust in technology are limited to achieving a goal or producing an outcome of a technology based information system, such as data security, accessibility or certification. The other perspective of trust, i.e. technology trust, focuses on the user's trust in the information systems technology itself as a catalyst to enhance electronic commerce. Integration of these two perspectives will increase use and ultimately help to expand the quantity and quality of commerce through information systems technologies.

There are some specific needs beyond the current notions of trust in technology, including:

- the standardization of language;
- the creation of support infrastructures to facilitate communications about technology trust and trust in technology;
- the development and expanded use of measures/metrics for the evaluation of trust;
- the establishment of standardized practices and broadly recognized certifications of technology;
- the recognition, understanding, and acceptance of technology trust using Trust in Information Systems Technology (TIST) as the backbone to support the development of U.S. Government infrastructures; and,
- the dissemination of information on technology trust to the widest possible audience of technology users.

To further facilitate the establishment of a government technology trust infrastructure, trust dimensions identified within this monograph are categorized in Table 1. The dimensions or principles identified within the commercial or government source are illustrated. A concise description of the dimension is provided. Outcome goals provide a shared foundation for consolidating the varying dimensions into a unified language oriented toward classification consistency.

Source	Dimension	Description	Goals	Sector
TRUSTe	Notice	Written public disclosure of personal information usage	Disclosure	Commercial
	Choice	Decision-making control related to personal information	Control	
	Access	Controlled access to personal information	Control	
	Security	Safety from unauthorized disclosure	Safety	
BBBOnLine	Notice	Written public disclosure of policy information	Disclosure	
	Evaluation	Privacy assessment for consumers	Standardization	
	Monitoring	Judgment of business operations by an impartial entity	Certification	
	Mediation	Dispute resolution between consumers and vendors	Agreement	
WebTrust	Privacy	Written public disclosure of policy information	Disclosure	
	Confidentiality	Authorized access to personal information	Control	
	Security	Safety against unauthorized access to personal information	Safety	
	Integrity	Secure from unauthorized modification	Warranty	
	Availability	Ready for use when needed	Access	
	Non-Repudiation	Safeguarding against refusal related to authentication	Recourse	
	Disclosure	Usage statistics	Public Information	
OPA	Policy	Written public disclosure of policy information	Disclosure	
	Notice	Written policy on collection, use, dissemination, individual choice, quality, access, and security	Disclosure	
	Choice	Consent for third party distribution	Control	
	Security	Data protection from loss or misuse	Safety	
	Access	Accurate and timely action to handle information data	Quality	
TCSEC	Secrecy	Confidentiality through a formal classification system	Safety	Government
	Integrity	Secure from unauthorized modification of public data	Warranty	
	Availability	Ready for use when needed	Access	
TTAP	Evaluation	Product assessment for consumers	Certification	
	Standardization	Unified evaluation for international products	Classification	
	Meaning	Criterion assurance of common meaning for users	Standardization	
	Efficiency	Control of resources to optimize performance	Optimization	
	Trust	Trust development of evaluated products	Warranty	
Steinauer, et al. (1997)	Trust	Consumer confidence through predictability	Safety	
	Trustworthy	System quality demonstrating trust	Quality	
	Traceability	Capacity for an audit trail	Safety	
	Integrity	Secure from unauthorized modification	Warranty	
	Confidentiality	Privacy protection	Privacy	
NCSC	Standardization	Common security taxonomy	Classification	
	Evaluation	Minimum standards for security	Limitation	
Safe Harbor	Notice	Written public disclosure of personal information usage	Control	
	Choice	Consent for third party distribution	Control	
	Transfer	Explicit disclosure permission to third parties	Disclosure	
	Security	Data protection from loss, misuse, alteration, destruction, disclosure, and unauthorized access	Safety	
	Integrity	Data are current, accurate and complete	Warranty	
	Access	User restricted access for data modification	Control	
	Enforcement	Recourse for non-compliance	Resolution	
NPR & GITSB	Accessibility	Ease of access to services	Simplicity	

Table 1: Categorization of Trust Dimensions

There appears to be some clustering of dimensions (notice, choice, security, access/accessibility, integrity, and availability) when defining trust. Interestingly, although certain dimensional nomenclatures are included from diverse sources, functional definitions vary. For example, three sources (Steinauer, et al., 1997; WebTrust; TCSEC) define integrity as security from unauthorized modification. Yet, the Safe Harbor definition refers to integrity as data that are current, accurate and complete. Notice and choice appear to contain some overlap particularly in the disclosure of personal information and the distribution to third party users. Although the notion of the basic elements such as disclosure and dissemination are repeatedly addressed by commercial and government sources, the internal consistency of the fundamental definitions are often blurred.

Government and commercial goal identification is comparable in terms of overall frequency distribution. Yet, the specific distribution of underlying principles varies across the sectors. The notion of disclosure appears with greater frequency within the commercial sector whereas control is more dominant within the government sector. Time constraints are important within government principles as evidenced through warranty – the guarantee for a specific time.

Table 2 offers a sector consolidation across dimensions. Clustering within sectors and across dimensions exist. Commercial policies and practices are geared toward consumer protection through establishment of explicit principles aimed at informing and protecting individual privacy. Dimensions of monitoring, mediation and privacy initiate procedural safeguards to ensure recourse should disputes arise. Traceability was absent from the commercial inventory. However, this notion is captured within the monitoring and mediation dimensions. In an electronic commerce environment, the idea that consumers could obtain a traceable transaction record appears reasonable to ensure control and to facilitate trust should trust breaches result. Government dimensions of public disclosure and choice to relinquish personally identifiable information to third party sources overlap their commercial counterparts.

Sector	Notice	Choice	Accessibility	Security	Evaluation	Monitoring	Mediation	Privacy	Confidentiality	Integrity	Availability	Non-Repudiation	Disclosure	Policy	Secrecy	Standardization	Meaning	Efficiency	Trust	Trustworthy	Traceability	Transfer	Enforcement
Commercial	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲									
Government	▲	▲	▲	▲	▲				▲	▲	▲				▲	▲	▲	▲	▲	▲	▲	▲	▲

Table 2: Dimensional Comparison Between Commercial and Government Sectors

Table 3 offers an integration of TIST constructs (Lippert, 2001a) with the commercial and government sector dimensions. Early support shows evidence of overlays between the trust infrastructures. Government policies demonstrate an awareness of predictability issues through the user's ability to predict future outcome states as an influential factor in assessing trust. Evaluation, as identified by TTAP and by BBBOnline, is oriented toward predictability through product or privacy assessments. Predictability achieved through technology consistency based on past experiences and future performance expectations directly connects to both Steinauer, et al.'s (1997) notion of trust and trustworthiness. Trust, in the Steinauer et al. context addresses consumer confidence through predictability. Trustworthiness is also a measure of predictability where trust increases through system quality.

Integrity and availability address issues of current reliance upon the technology in situations that involve dependence and risk. These notions merge with the TIST construct of reliability. Utility addresses ease of use and usefulness. The TTAP notion of meaning establishes a threshold to facilitate ease of use through a standardized language for users. Accessibility, within the NPR & GITSB framework, addresses ease of access to services.

Commercial	◆ Evaluation (BBBOnline) ◆ Non-Repudiation (WebTrust)	◆ Integrity (WebTrust) ◆ Availability (WebTrust)	
Government	◆ Evaluation (TTAP) ◆ Efficiency (TTAP) ◆ Trust (Steinauer, et al., 1997) ◆ Trustworthy (Steinauer, et al., 1997)	◆ Integrity (TCSEC; Steinauer, et al., 1997; Safe Harbor) ◆ Availability (TCSEC)	◆ Meaning (TTAP) ◆ Accessibility (NPR & GITSB)
	Predictability	**Reliability**	**Utility**

Table 3: Integration of TIST Dimensions

The tables support the need for a standardized language both within and across commercial and government sectors. The diversity of meanings associated with each dimension challenges the user/consumer to

"make sense" of the diverse interpretations offered for his/her protection. The TIST dimensions offer an added view of technology trust from the vantage point of the user.

Conclusions

Information systems technology infrastructures offer a mechanism to facilitate communication about technology trust. A consolidated infrastructure remains underdeveloped. The existing dimensions and structures do not offer a mechanism for the user to evaluate trust. Many of the government trusted system programs offer evaluations of the technology prior to purchase certifying IT products beyond vendor specific security claims. A "trusted" system can be identified through the attached equipment seal. Other programs offer structures to classify a level of trust in either the technology or the process. While these programs offer the user one level of trust, it excludes the possibility for a unified assessment of technology trust (Lippert, 2002). Various forms of trust exist through which the user can make trust determinations. Trust assessments are often based upon a single incident (Denning, 1993). Individuals assess technology each time an information system is used (Denning, 1993). The establishment of measurement processes for both commercial and government users, based on a unified model of trust, may permit a quantifiable assessment of the trust process. The establishment of standardized practices and certifications offer an external evaluation of the technology. A continuing challenge exists in operationalizing the government's current vision for developing electronic commerce.

Measurement, classification and institutionalization of trust constructs are far from complete. Various dimensions are currently in use both within the commercial and government sectors. Definitional diversity intensifies the need for creation of a unified infrastructure to define and assess trust. The use of the Trust in Information Systems Technology (TIST) model merges several commercial and government trust dimensions. Further exploration is needed to quantify these measures prior to development of an instrument to assess the user's trust in the government information systems technology.

References

Access America InitiativesA01. Retrieved March 2, 2002 from the World Wide Web http://www.accessamerica.gov/reports/public2.html.

Access America Initiatives A02. Retrieved February 22, 2002 from the World Wide Web http://www.accessamerica.gov/reports/ebt.html.

Access America E-Gov E-Zine. Retrieved February 19, 2002 from the World Wide Web http://www.accessamerica.gov/text/privacy.html.

A Better Business Bureau Program (BBBOnline). Retrieved February 19, 2002 from the World Wide Web http://bbbonline.org/privacy.

BBBOnLine Japanese Privacy Seal. Retrieved March 2, 2002 from the World Wide Web http://bbbonline.org/privacy/jipdec.asp.

BBBOnLine Participant Benefits. Retrieved March 2, 2002 from the World Wide Web http://bbbonline.org/reliability/benefits.

Clinton, W.J. (1995) *A Framework For Global Electronic Commerce*. Retrieved March 2, 2002 from the World Wide Web http://www.itmweb.com/essay541.htm#privacy.

Connolly, J.L. and Abramowitz, B.S. (1995) *The Trust Technology Assessment Program and the Benefits to U.S. Evaluations*. Retrieved February 21, 2002 from the World Wide Web http://www.radium.ncsc.mil/tpep/ttap/TTAPpaper.html.

Denning, D.E. (1993) A New Paradigm for Trusted Systems. *Proceedings of the 1993 Association for Computing Management SIGSAC on New Security Paradigms Workshop*, August 2-5, 1993, Little Compton, RI, 36-41.

eCommerce B2C Report (2000). Retrieved March 2, 2002 from the World Wide Web http://www.emarketer.com/about_us/press_room/press_releases/103100_eb2c.html.

Flahavin, E.E. and Toth, P.R. *Concept Paper – An Overview of the Proposed Trust Technology Assessment Program*. Retrieved February 17, 2002 from the World Wide Web http://radium.ncsc.mil/tpep/ttap/conceptpaper.txt.

Global Information Infrastructure Commission. Retrieved March 2, 2002 from the World Wide Web http://www.giic.org.

Historical EPL Product Listing. Retrieved February 19, 2002 from the World Wide Web http://www.radium.ncsc.mil/tpep/epl/historical.html.

International Trade Administration: Export.Gov. Retrieved March 2, 2002 from the World Wide Web http://www.ita.doc.gov/td/ecom/shpirn.html.

ISO Easy. Retrieved March 2, 2002 from the World Wide Web http://www.isoeasy.org/.

Lippert, S.K. (2002) Contributing to a Unified Model of Technology Trust: Understanding Trust in Information Systems Technology. Forthcoming at the 2*002 Academy of Business and Information Technology Meeting*, May 2-4, 2002, Pittsburgh, PA.

Lippert, S.K. (2001a) An Exploratory Study into the Relevance of Trust in the Context of Information Systems Technology. *Doctoral Dissertation*. The George Washington University, Washington, D.C.

Lippert, S.K. (2001b) Trust in Information Systems Technology: Implications for Academia. *Proceedings of the Seventeenth Annual Research Forum, Washington Consortium of Business Schools*, April 21, 2001, Washington, DC.

Lippert, S.K. (2001c) *Trust in Information Systems Technology: A Fundamental Metric In Systems Development and Usage*. Washington Metropolitan Best Practices Forum, April 26, 2001,Washington, DC.

Lippert, S.K. (2001d) *Why Trust in Information Systems Technology? Does it Matter For IT Professionals*? Invited Guest Lecturer, Management and Organization Seminar, George Washington University, April 23, 2001,Washington, DC.

Online Privacy Alliance. Retrieved March 1, 2002 from the World Wide Web http://www.privacyalliance.org/facts/.

Online Privacy Alliance For Business. Retrieved March 1, 2002 from the World Wide Web http://www.privacyalliance.org/businesses/.

Steinauer, D.D., Wakid, S.A. and Rasberry, S. (1997) *Trust and Traceability in Electronic Commerce*. Retrieved February 17, 2002 from the World Wide Web http://nii.nist.gov/pubs/trust-1.thml.

Sivasailam, N., Kim, D.J. & Rao, H.R. (2002) *Dimensions of Web Assurance in B2C E-Commerce: A Comparative Study*. Working Paper.

The Need for Trusted Systems. Retrieved February 19, 2002 from the World Wide Web http://www.radium.ncsc.mil/tpep/library/ramp-modules/mod_01.txt.

Trust*E*®, *Building A Framework for Global Trust*. Retrieved October 21, 2001 from the World Wide Web http://www.truste.org/index.html.

Trust*E*®*: Online Privacy Resource Book*. (Fall 2000) Retrieved October 21, 2001 from the World Wide Web http://www.truste.org/resourcebook.html.

Trust Technology Assessment Program (TTAP). (1998) Retrieved February 21, 2002 from the World Wide Web http://radium.ncsc.mil/tpep/ttap/basics.html.

Trust Technology Assessment Program (TTAP). Retrieved February 21, 2002 from the World Wide Web http://radium.ncsc.mil/tpep/ttap/conceptpaper.txt.

Trust Technology Assessment Program (TTAP). Retrieved February 19, 2002 from the World Wide Web http://csrc.nist.gov/ttap/.

Trusted Network Interpretation Environments Guideline. Retrieved March 1, 2002 from the World Wide Web http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-011.html#HDR1.1%20%20%203%2018.

Trusted Product Efforts in the U.S. and Abroad. Retrieved February 17, 2002 from the World Wide Web http://www.radium.ncsc.mil/tpep/library/ramp-modules/mod_02.txt.

United States Government Electronic Commerce Policy. Retrieved March 1, 2002 from the World Wide Web http://www.ecommerce.gov.

WebTrust, Independent Verification. Retrieved March 1, 2002 from the World Wide Web http://www.cpawebtrust.org/onlnover.htm.

Biography

Susan K. Lippert, Ph.D. is an Assistant Professor of Management Information Systems in the Department of Management, Drexel University, LeBow College of Business. Dr. Lippert received her Ph.D. in Information Systems from the George Washington University focusing on technology trust. She also received an M.B.A. from the George Washington University, and a B.S. from The University of Richmond. Her research interests include the use and management of information technology particularly technology trust. She has also researched in the area of technological innovations in education and training. She previously taught both undergraduate and graduate courses at the George Washington University. Professor Lippert has published in the *Journal of End User Computing*, the *Journal of Management Education*, and the *Journal of Mathematics and Science Teaching.* She has numerous articles in conference proceedings such as the Information Resources Management Association (IRMA), the International Academy for Information Management (IAIM), and the Washington Consortium of Business Schools.