Taming the Cyber-Frontier: Security is Not Enough!

Paul Toscano
USERTrust Inc.

A major problem in cyberspace is the lack of security, privacy, and integrity in the creation, collection, transmission, processing, storage, and use of electronic and digital information. Before users fully adopt e-business enabling technologies, they will consider the total context of what is required for them to feel safe in the virtual world. Security alone will not be enough. In addition, users will require all aspects of informational privacy and integrity through data vaulting and trusted third-party data management in order to feel as safe with e-business as they now do with paper transactions.

The cyber-universe, like the real universe, is expanding. Functions, applications, and usages grow daily as more people become computer literate. Since the early 1950s, the real world has become more reliant upon the virtual or cyber-world. With the Internet and wireless communication, a vast amount of messaging and commerce is now taking place globally at virtually light speed—although it does not always seem that fast.

Currently, cyberspace is still very much a frontier—just as America was in about 1650. It has only recently been colonized by ordinary people who followed in the footsteps of those intrepid cyber-explorers who built ARPAnet, the Internet, and the World Wide Web. Life in cyberspace for its early settlers is promising, but hard. Although technological mountain men thrive in this environment, the less able can find life there ineffectual or worse; it can be nasty, cruel, brutish, and short.

In spite of this, the population of cyber-settlers is growing exponentially. Cyber-colonists sense the cyber-frontier's untapped resources. They intuit its opportunities. Many of them also harbor anxieties about its risks and dangers; yet, they continue to make forays into the unknown. They quarry out habitations, establish networks, create enterprises, and engage in commerce. Much of this is taking place without any settled assurances of security, privacy, or integrity with respect to the collection, transmission, storage, and use of electronic and digital information.

The Problem

One of the chief strengths of cyberspace is that it transcends the borders of states and nations. This is also one of its chief weaknesses. Because the cyber-frontier is not subject to the laws of any one country or jurisdiction, laws regulating cyber-transactions do not exist. Where they do, they are not standardized and uniformly enforceable and, therefore, do not have the dignity or effect of true laws. They are more like customs or norms. They are usually drafted or promoted by private parties or groups from differing traditions. They seldom share similar objectives and outcomes, and often conflict. They tend to be self serving rather than self regulating. They are more likely to inspire competing rules than compliance. And whatever compliance there is cannot be reliably verified.

For all these reasons, security, privacy, and integrity of information and transactions in the cyber-frontier are available only to a small minority and only in restricted cyber-communities (usually either governmental or commercial intranets or extranets) where authority structures have been established and are managed according to uniform policies, procedures, protocols, and practices. Outside these communities, cyber-citizens are on their own for the most part. Or else, they must rely on experts offering partial solutions for commercial gain.

The thorniest problem hindering the entire cyber-frontier is the lack of security, privacy, and integrity in the creation, collection, transmission, processing, storage, and use of electronic and digital information. Like the wild, wild west (another WWW), the cyber-frontier needs to be tamed. But unlike the citizens of the wild west, cyber-citizens cannot rely on a local sheriff or a federal marshal to bring order out of chaos. Because the cyber-frontier overlays many nations, cyber-rules and laws cannot be created or enforced effectively by any one government. "Who is going to perform this mediating function?," is a recurring question that so far has no satisfactory answer. Any government seems disabled by its inability to enforce order beyond its jurisdictional limits; moreover, for-profit companies are disqualified by the profit motive, which encourages them to tip any level playing field in their favor, making it easier for them to create wealth for their shareholders.

To date, there is not even a workable consensus on what security, privacy, and integrity of information actually mean, let alone on how these values can be preserved in cyberspace.

What Will It Take?

In the balance of this paper, I would like to propose a working definition of terms and to provide a suggested list of minimal requirements necessary for cyber-citizens to enjoy the same informational security, privacy and integrity in the virtual world that they have come to expect in real world paper transactions.

In the computer industry the term *security* means something different to non-experts than it does to computer experts. To non-experts, security means that a user's data transmissions and transactions are safe. *Safe* implies to the layperson that electronic and digital information is: safe from technological failure, hackers, loss or corruption; safe from prying eyes; and safe in the sense that it will be available and reliable in the future. For non-experts, security not only means data protection, it also means data privacy and data reliability or integrity.

To the expert, however, security may or may not include informational privacy and integrity. An expert may consider a transaction secure if the data in transition flowed through a secure channel—even though the source of the message is uncertain, the recipient's identity cannot be assured, and the message itself can be read by any party who can capture it. An

expert may consider information in a database or data warehouse to be secure if it is protected by firewalls and managed according to acceptable security standards—even though the data consists of the personal and sensitive information of parties who have no knowledge or control of how the data was collected, is processed, or will be used. For non-expert users to have confidence in the enabling technologies of e-business, they will consider the total context of what is required to feel safe. In doing so, they will conclude that security is not enough.

Working Definitions

Security refers, at a minimum, to three different protections. First, security refers to any protection that enables electronic and digital information to be transmitted from a known source to an intended recipient only. Second, it applies to any protection that enables such information to be stored, transmitted, processed, or used without compromise, alteration, or corruption. Third, security refers to any protection that enables such information to be linked to any real world person whose identity has been reliably authenticated and represented by a verifiable cyber-identity, such as a digital certificate, digital signature, or other electronic ID.

Privacy is a bit more challenging to define. Currently, there is no universally accepted definition for privacy or for informational privacy. Seeking a normative definition—that is, one that defines privacy in terms of what normally should be kept private—does not work because people from various cultures cannot agree on what should be kept private. (This is clear to any American who has visited the beaches of southern Europe.)

I propose an analytical definition—one based on an analysis of the recurring elements essential to privacy regardless of what is being kept private. Take land, for example. To establish private property, it must first be separated from the surrounding property. Then access must be restricted. Finally, the land use must benefit only its owners or a tenant with the right to occupy, farm, or mine the property.

What is true of land use is also true of any property, including bodies of information, whether electronic or otherwise. Informational privacy depends on (a) separateness (b) restricted access, and (c) beneficial use. In discussions of informational privacy, little is said about these essentials—probably because they are so fundamental they are left unaddressed as unstated assumptions. Let me review these briefly:

(a) Separateness. Before a legitimate claim of informational privacy can be sustained, the information in question must be rendered separate and identifiable. This involves the process of partitioning the data. Until this takes place, there is nothing to which a claim of ownership can attach. Once partitioned, privacy requires that a claim of right in the separate data be asserted. This claim of right can be a claim of ownership or a claim of use. In either case, the claim must be grounded in law—that is, the claim must be one the law recognizes. For example, a claim of ownership in data may be based on an author's common law copyright or on a publisher purchase contract. Or it may be based on inheritance, lease, license, or other instrument of title or conveyance.

The process of separating digital information and establishing title to it is merely a way of creating enforceable cyber-boundaries to digital or electronic information. Title to data cannot be enforced, however, if it exists only in the mind of the claimant. It must somehow be declared, if not publicly, then at least before credible witnesses. This requires that some kind of notice be available that describes the property, the boundaries, and those with ownership or access rights to it.

"I propose an analytical definition—one based on an analysis of the recurring elements essential to privacy regardless of what is being kept private. Take land, for example. To establish private property, it must first be separated from the surrounding property. Then access must be restricted. Finally, the land use must benefit only its owners or a tenant with the right to occupy, farm, or mine the property."

In the virtual world, such boundaries and claims of ownership and use can be established by companies that assure the reliability of encoded cryptography. Public and private encryption keys can now be issued to users. These public and private keys can be certified to users whose identities have been acceptably authenticated. Such users can encrypt or digitally sign data streams with these keys. They can separate and identify data streams and establish an initial claim of right to the data as its originator, owner, or user. Of course, this claim can be challenged. But at a minimum, public key encryption technology allows data boundaries to be established and title to data to be asserted in the cyber-frontier. This is an important step forward.

(b) Restricted Access. Setting legally enforceable boundaries alone does not ensure confidentiality or restrict access. Privacy is nothing unless the identified data can be protected from unwanted interlopers. Restricted access can also be achieved by the use of public key cryptography. Data can be encrypted with a person's public key so that it can be decrypted only with the corresponding private key held solely by the holder of the unique key pair. This technique will render data confidential. The problem is that it is not a reliable technique because there is only one private key in the hands of its owner. If that key were lost, stolen, or damaged, then the encrypted information would remain virtually irretrievable. This is not a very attractive prospect, especially in a commercial environment where documents are vital.

However, it is not a solution to make a copy of a private key and put it in a safe place. This approach, referred to as private key escrow or management, creates significant security risks. The private key is a digital signature. Under current law, if a private key is used to sign a digital document, that digital signature is considered binding. If a private key is copied to a floppy disk, for example, it could be stolen and used to create legally binding documents without the knowledge or authorization of the owner of the private key. If the private key were put in escrow with an agent, the agent or an employee of the agent might compromise the key or use it improperly. What is more troubling, the private key owner could allege that his or her digital signature was used without authorization and thus repudiate the enforceability of a digital signature to avoid obligations under an electronic contract.

For these reasons, confidentiality and restricted access to cyber-information is not reliably achieved by encrypting data

with a public key. A better method of assurance is needed—more about this later.

(c) Beneficial Use. In addition to the separate and restricted access to data, there must also be a means to insure that only data owners or authorized parties receive the benefit of such information. When it comes to real estate, we understand that a residence is not private if anyone can live there. Electronic information is not private if anyone can see it, use it, or benefit from it. A contract is useless if any non-party can claim its benefits or avoid its burdens. An essential element of privacy, then, is beneficial use (or proprietary utility).

To assure beneficial use means to assure that data is accessible, readable, and useable only by authorized parties and in spite of technological advances or obsolescence. To achieve beneficial use requires data vaulting. Information, such as e-contracts, personal identifying information, or sensitive medical or legal information, must be preserved so that it will be available to authorized parties in the indefinite future. To achieve this end, digital document signatures must remain identifiable and legally binding. Document form and content must be rendered persistent. A document's admissibility as court evidence must be assured. A record must be kept of the source, date of origin, history, and chain of custody of the document together with the identity of its owners and any parties with authorized rights of access and use. In addition an auditable record of access and retrieval must be kept to prevent confusion and maintain record chronology.

Without these safeguards, users have no assurance they will receive the beneficial use of the information and obligations memorialized in their digital documents. Without these assurances, users will be reluctant to bring their paper process on line. Hence, they will not reap the cost savings, gains, and other benefits of the Internet, the World Wide Web, or wireless communications systems. This is especially true for professionals in the legal, health care, accountancy, real estate, lending/leasing, and intellectual property industries—professionals with a duty to protect the confidences and secrets of their clients or patients.

Integrity is the third assurance the cyber-frontier needs in addition to the three security protections and the three elements of privacy discussed. Informational integrity refers to the retention of data and documents according to rules that ensure their preservation in a trustworthy environment so they will continue to serve their intended purposes. Integrity means that personal data will remain personal, sensitive information will remain confidential, and legal documents will remain enforceable. Informational integrity in cyberspace is achievable only when digital and electronic information is securely retained in the possession of trusted third-party custodians.

The most troubling problem plaguing the cyber-frontier is the retention of data by non-neutral, biased, interested parties. User information is typically warehoused with digital database services offered by for-profit companies. These companies are run by management teams and boards of directors whose overriding duty is to their company shareholders, not to the data owners. A subscriber to such a service places personal, sensitive, legally significant, or valuable proprietary information in the care of companies whose self-interest may conflict with the subscribers' interests. Even when such companies sign contracts promising to preserve subscriber privacy, the underlying conflicts of interests together with the pressures of undue influence and the profit motive still exist. This is not an environment of trust in which the security, privacy, and integrity of information can be guaranteed.

Informational integrity requires data custodians to be neutral, even handed, independent, and free from disqualifying conflicts of interests. Informational integrity can be assured only when it is in the safekeeping of trustee-like custodians who have only one duty—to apply fair information practices in order to preserve the original form and content of information so that it will continue over time to serve the purposes for which it was created, collected, stored or processed. Only such custodians can reliably certify a traceable and auditable document registry, provide a reliable chain of custody, or assure the evidentiary integrity of documents.

Legal and Technical Requirements

The cyber-frontier must be tamed; however, security is not enough. What is required is full informational privacy consisting of all the aspects of security, privacy, and integrity discussed here. Without full informational privacy, individual autonomy cannot exist in cyberspace. Individual autonomy is the prime value of an open, democratic society and should never be sacrificed on the altar of expedience, digital or otherwise.

What is desperately needed to tame the cyber-frontier is a neutral, independent, nongovernmental, self-regulatory architecture of privacy that can assure data originators, owners, and users of 12 legal and technical requirements:

1. Data can be rendered separate and identifiable.
2. Data ownership and access rights can be identified and registered.
3. Data will not knowingly be viewed, altered, intercepted, copied, confiscated, or divulged without authorization of its owners.
4. A person's digital likeness will not be appropriated.
5. No intrusions upon a person's solitude or seclusion by eavesdropping on digital or electronic communications, or sending unwanted communications will be tolerated.
6. No information that puts a person in a false light will be disclosed.
7. Personal and sensitive information will be collected, stored, processed, retrieved, and used only according to prepublished fair information practices.
8. Data management risks and liabilities will be kept at a minimum.
9. Data owners will maintain control of their own personal and sensitive information.
10. A reliable, auditable record of data will be kept and its chain of custody will be maintained for certification to authorized requesting parties.
11. Data owners and authorized users will be identified by acceptably authenticated and certified cyber-IDs.
12. ID authentication and certification, with personal, sensitive, confidential data collection, storage, processing, retrieval, and usage will be managed by private, unbiased, third-party fiduciary custodians with an unconflicted duty to data owners or authorized parties.

Conclusion

The cyber-frontier must be civilized in order for cyber-citi-

zens to feel safe. They must be confident that informational security, privacy, and integrity will be ensured. Internet, World Wide Web, and wireless communication must be preserved as an open and level field for all. There must, however, be introduced a private, trust-based supra-jurisdictional architecture, consisting of neutral third-party protective custodians. These custodians serve in the place of government to act without bias, undue influence, or profit motive to assure the even-handed administration of fair information policies, procedures, protocols, and practices. This will enable the delivery of informational security, privacy, and integrity to a global community in desperate need of end-to-end reliability of the digital transactions that form the basis of cyber-relationships of all kinds.

When these essentials are available to all cyber-citizens on an equal footing, then we will have tamed the cyber-frontier. We also have the opportunity to move at Internet speed to adopt the technologies, definitions, trust structures, and legal processes that are indispensable to individual freedom, personal autonomy, a free market, and the pursuit of e-business worldwide.◆

About the Author

Paul Toscano, M.A., J.D., is the executive director of The USERTRUST Network LLC, a public key infrastructure that provides encryption products and fiduciary repository to facilitate worldwide e-commerce. Since 1997, Toscano has developed legal/technological structures that safeguard informational privacy in electronic and digital transmissions through public key encryption. Previously he was an attorney focusing in the commercial arena, specifically in cases dealing with insolvency. Toscano has published several articles and a book on first amendment freedoms.

USERTrust Inc.
265 East 100 South, Suite 306
Salt Lake City, Utah 84111
Voice: 801-363-9748
E-mail: pjt@usertrust.com

Letters to the Editor

Dear Editor:

Somehow I doubt that the quote attributed to Thomas J. Watson in your August issue on p. 21 [*Quote Marks*] occurred in 1965. At that point IBM was in the throes of the development of System 360. I doubt IBM would have undertaken that effort for the sale of five computers. I suspect the actual year of that quote was much earlier, maybe 1935 or 1945. Also, it appears to be attributed to Watson Sr. rather than Watson Jr., making it almost certainly much earlier.

Dr. Nancy R. Mead
Senior Member, Technical Staff
Networked Survivable Systems Program
Software Engineering Institute, Carnegie Mellon University

Ed. Note: *You map out good historical parameters Nancy. Watson Sr. did make this statement in 1949.*

Dear Editor:

I am currently completing my master's in software engineering from the University of West Florida (UWF). My directed study this past summer was to rewrite the process for the graduate software engineering project class. We used a defined software maintenance process to teach software engineering. Class members assumed roles (management, SCM, SQA, SEPG, Metrics, and engineers) and we maintained and enhanced a software tool developed at UWF.

It was a great class, and we all learned a lot about working within a process. The majority (95 percent) of the students are military or contractors involved with some sort of software or hardware development. A lot of different experience is brought together and information is shared about better ways to achieve the goal.

I have referred to CROSSTALK on many occasions and always have found something new and interesting. I will continue to be interested in this area of technology. My company (TYBRIN Corp.) is CMM Level 3, pushing towards level 4, and beginning to get the information concerning CMMI. I was very interested in the latest issue of CROSSTALK for that information. Keep up the great work!

Darsi D. Ewing
TYBRIN Corporation

Free tips from software industry experts!

Subscribe to E-ssentials! ***a free*** **biweekly e-newsletter with how-to's for successful project management and practical software development.**

Subscribe for FREE at http://www.spc.ca/epr9

E-ssentials! offers tips, hot topics and techniques for project management and software development from a variety of software industry experts. Learn how to successfully attack the challenges you face every day through their collective experience. Published by Software Productivity Center Inc.

"This newsletter is well done -- important and useful information succinctly expressed for busy people."

Michael P. Meier
Software Quality Assurance
Mayo Foundation