UIC John Marshall Journal of Information Technology & Privacy Law

Volume 19
Issue 1 *Journal of Computer & Information Law - Fall 2000*

Article 7

Fall 2000

Toward an Architecture of Privacy for the Virtual World, 19 J. Marshall J. Computer & Info. L. 151 (2000)

Paul Toscano

TOWARD AN ARCHITECTURE OF PRIVACY FOR THE VIRTUAL WORLD

by PAUL TOSCANO†

I. INTRODUCTION

The cyber universe,[1] like the real universe, is expanding. Functions, applications, and uses grow daily as more people become computer literate. With every year that has passed since the early 1950s, the real world has become more reliant upon the virtual or cyber world. Since the advent of the Internet[2] and wireless communication,[3] a vast amount of messaging and commerce is now taking place among many people of

---

† Paul Toscano (M.A., J.D.) is the Director of The USERTrust Network, a public key, private repository, and data and transaction management infrastructure comprised of Cybercitizens Trust, Universal Secured Encryption Repository Company ("USERFirst"), and USERTrust Inc. a Digital Analog Technology Applications Corporation ("USERTrust Inc."). These allied companies provide encryption products and fiduciary repository services to facilitate e-commerce/e-business worldwide. Since 1997, Mr. Toscano has devoted himself to developing legal/technological structures that safeguard informational privacy in electronic and digital transmissions through the use of public key encryption. Mr. Toscano has published several articles and a book on First Amendment freedoms. Mr. Toscano wishes to express his appreciation to Nicole Milos for inviting and encouraging the presentation and publication of this paper and to Hillary Victor and Keri Ellis for enriching it with their remarkable research and editorial skills.

1. *See* Jay Krasovec, *Cyberspace: The Final Frontier for Regulation?*, 31 Akron L. Rev. 101 n. 1 (1997). "Cyber universe" is a synonym for "cyberspace," a term coined by author William Gibson and used as a metaphor to describe the non-physical terrain created by computer systems, including the links through which people can communicate with one another (via e-mail), do research, or shop. *Id.* Like physical space, cyberspace contains objects (such as files, mail messages, graphics, etc.), but unlike real space, cyberspace does not require any physical movement other than pressing keys on a keyboard or moving a mouse apparatus that triggers the transmission of electromagnetic impulses or waves. *Id.*

2. *See* Marcus Maher, *An Analysis of Internet Standardization*, 3 Va. J.L. & Tech. 5 (1998) <http://vjolt.student.virginia.edu/graphics/vol3/home_art5.html> (accessed Dec. 6, 2000). "Internet" is the term used to describe the interconnected networks employing the Transmission Control Protocol/Internet Protocol (TCP/IP) communications protocols. *Id.*

3. *See Gulf Power Co. v. FCC*, 226 F.3d 1220 (11th Cir. 2000). "Wireless communication" refers to communication by way of systems that are linked in whole or in part through high-frequency radio transmissions rather than physical means such as wires or fiber optical cable. *Id.*

many countries at virtually light speed—although it does not always seem that fast. Currently cyberspace is still very much a frontier—as was America in about the year 1650.[4] The cyber frontier[5] has only recently been colonized by ordinary people following in the footsteps of the intrepid cyber explorers who built ARPANET,[6] the Internet, and the World Wide Web ("Web").[7]

Life in cyberspace for its early settlers is promising but difficult. Although technological pioneers thrive in this environment, the less able can find life there ineffectual or worse; it can be "solitary, poor, nasty, brutish, and short."[8] In spite of this, the population of cyber settlers[9] is growing exponentially. Cyber colonists[10] sense the frontier's untapped power to increase efficiency of information transmissions and business transactions, while decreasing costs and creating gains. Though they intuit these opportunities, many Internet users continue to harbor anxieties about the risks and dangers of Internet use caused by uncertainty about the privacy of transmissions and the legal enforceability of electronic contracts.[11] Worries aside, Internet users continue to make forays into the unknown.[12] They quarry out habitations, establish networks, create enterprises, and engage in commerce. Every day more and more

4. Finley P. Maxson, *A Pothole on the Information Superhighway: BBS Operator Liability for Defamatory Statements*, 75 Wash U. L.Q. 673 n. 1 (1997) (explaining that cyberspace is a new frontier).

5. *See generally* Krasovec, *supra* n. 1. "Cyber frontier" is a metaphor for cyberspace in its current formative period. *Id.*

6. Internet.com, *ARPANET* e.g. <http://webopedia.internet.com/TERM/A/ARPANET.html> (accessed Oct. 19, 2000). ARPANET was a large wide-area network created by the United States Defense Advanced Research Project Agency ("ARPA"). *Id.* Established in 1969, ARPANET is considered the "precursor to the Internet." *Id.*

7. The World Wide Web ("Web") is a system of Internet servers that supports documents formatted in hypertext markup language ("HTML"), which supports links to other documents as well as to graphics and audio-video files that are hosted on different computers linked together through the Internet. The Internet and the World Wide Web are not the same entity; not all Internet servers are part of the Web. Applications (complex software programs) called browsers allow users to access the Web. Two of the most popular browsers are Microsoft's Internet Explorer and Netscape Navigator.

8. *See generally* Thomas Hobbes, *Leviathan* ch. xviii (Norton 1996).

9. "Cyber settlers" is a metaphor for Internet users.

10. "Cyber colonists" is a metaphor referring to regular users of the Internet for business or commercial transactions.

11. *See* Amelia H. Boss, *Electronic Commerce & the Symbiotic Relationship Between International & Domestic Law Reform*, 72 Tul. L. Rev. 1931 n. 71 (1998) (citing Electronic Data Interchange, *Preliminary Study of Legal Issues Related to the Formation of Contracts by Electronic Means: Report of the Secretary-General*, U.N. Doc. A/CN.9/333 (1990), which discusses legal enforceability of electronic transactions).

12. *See e.g.* Constance K. Robinson, *Network Effects in Telecommunication Mergers MCI WorldCom Merger: Protecting the Future of the Internet*, 1192 PLI/Corp 517, 529 (2000) (explaining the Internet has grown from 100 million users in 1995 to over 140 million in 2000).

information is migrating into the cyber frontier where it is accessible to the whole world. Much of this transfer 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.[13]

II. THE PROBLEM

Cyberspace transcends the borders of states and nations.[14] This is one of its chief strengths and also one of its chief weaknesses.[15] The cyber frontier is not subject to the laws of any one country or jurisdiction.[16] Sectoral laws and regulations exist, but they are not uniformly enforceable upon the global population of Internet users.[17] Outside their zones of enforceability, these laws assume the nature of customs or norms, like professional ethics or rules of etiquette. Many have been drafted or promoted by private parties or groups from differing traditions and with differing objectives. These regulations can be both redundant and conflicting.[18] Some are more self serving than self regulating.[19] Others are more likely to inspire competing rules than compliance, and compliance is at best difficult to verify.

For all these reasons, security, privacy, and integrity of information and transactions in the cyber frontier are available only to a 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.[20] Outside these communities, cyber citizens are either on their own or they must rely on experts offering partial solutions

13. *See generally* Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (Michie Law Publishers 1996).

14. *See generally id.* Because cyberspace has no physical borders, persons from any nation, state, or territory who have adequate technology and connectivity can access the Internet and engage in personal, business, or commercial transactions. *Id.*

15. This weakness is repeatedly demonstrated by hackers—usually men in their teens and twenties—who introduce into the Internet computer programs called "viruses" that can potentially destroy electronic information, software, and hardware on remotely located computers and servers, thus causing millions of dollars in damages worldwide.

16. *Id.*

17. David Johnson & David G. Post, *The Rise of Law on the Global Network*, in *Borders in Cyberspace* 3-47 (Brian Kahnin & Charles Nesson eds., MIT Press 1999).

18. *See e.g.* McBride, Baker, and Coles, *Summary of E-Commerce and Digital Signature Legislation* <http://www.mbc.com/ecommerce.html> (last updated Oct. 17, 2000).

19. *See generally* Henry H. Perritt, Jr., *Regulating Models for Protecting Privacy on the Internet* <http://www.ntia.doc.gov/reports/privacy/selfreg3.htm> (accessed Oct. 19, 2000).

20. *See generally Health Insurance Portability & Accountability Act of 1996*, Pub. L. No. 104-191, 110 Stat. 1936 (1996) ("HIPAA") (requiring efficiency in healthcare delivery by standardizing electronic data interchange and the protection of confidentiality and security of health data); *see also* Council Directive 95/46/EC 1995 O.J. (L 281) 31 (enumerat-

for commercial gain.[21]

The thorniest problem hindering the cyber frontier, including the Internet, the Web, and wireless communication, is the lack of security, privacy, and integrity in the creation, collection, transmission, processing, storage, and use of electronic and digital information.[22] Like the frontier of the American West, the cyber frontier must be tamed.[23] But cyber citizens cannot rely on a local sheriff or a federal marshal to do it. Governments are disabled by their inability to enforce order beyond its jurisdictional limits. For-profit companies are disqualified by the profit motive, which encourages them to tip any level playing field in their own favor to make it easier for them to create wealth for their shareholders. Who is going to perform this policing or mediating function? This is a recurring question that as yet has no satisfactory answer.

To date, there is no workable consensus on what security, privacy, and integrity of information actually mean or how these values can be preserved in cyberspace. For example, in the computer industry, the term "security" is used a great deal. However, the exact meaning of "security" can vary considerably.

III. SECURITY AND ENCRYPTION

To computer experts, security may or may not include informational privacy and integrity. An expert may consider a transaction to be secure if in transmission the electronic and digital information ("data") flows through a secure channel—even though the source of the message is uncertain, its recipient's identity cannot be assured, and the message 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.

To laypeople, security means that a user's data transmissions and transactions are safe. "Safe" implies to the layperson that data is safe from technological failure, hackers, loss or corruption; is safe from prying eyes; and will be available and reliable in the future. Laypeople, then,

---

ing the protections of individuals with regard to the processing of personal data and on the free movement of such data) [hereinafter Council Directive].

21. David H. Flaherty, *Controlling Surveillance: Can Privacy Protection Be Made Effective?* in *Technology and Privacy, The New Landscape* 168–192 (Philip E. Agre & Marc Rotenberg eds., MIT Press 1998).

22. *See generally* Schwartz, *supra* n. 13.

23. *See e.g.* David Allweiss, *Copyright Infringement on the Internet: Can the Wild, Wild West Be Tamed?*, 15 Touro. L. Rev. 1005 (1999) (comparing the Internet to the American Old West).

interpret security to mean not only data protection but also data privacy, reliability, and integrity. For lay 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 in the narrow expert sense is not enough in spite of the fact that high levels of security can now be achieved through one of two encryption methods: single key encryption or public key encryption (also known as asymmetrical twin key encryption).[24]

Single key (or shared secret) cryptography is an unacceptable way to protect digital and electronic information.[25] This is so because in single key cryptography the same cipher or code used to encrypt a message is also used to decrypt it. When a single-key encrypted text is transmitted, the key must be shared with the recipient so the scrambled message can be deciphered. Sharing the single secret key, however, exposes it to capture. Any party capable of purloining the scrambled message is probably capable of capturing the single key as it is being conveyed to its intended recipient. This weakness makes symmetrical key encryption insecure in an environment of public messaging such as e-mail or wireless communication. As soon as the secret is shared, it is open to capture; and as soon as it is captured, it is exposed to compromise. Once compromised, the shared secret can be used to subvert the authenticity of a cyber identity and to compromise the privacy and integrity of information that is logically connected with or accessible through such a shared cipher. To compromise a person's cyber identity and private information is to deprive them in cyberspace of personal freedom to safeguard and use private resources to pursue private objectives.

Public key encryption is a coding system or, more accurately, a ciphering system that uses two related ciphers (code numbers) called keys—a public key available to everyone and a private or secret key available only to the holder of the key pair.[26] The term "asymmetric" is used because a message encrypted with the private key can be decrypted only with its twin, the corresponding public key and vice versa.[27] Thus, if John wants to send a secure message to Jane, he can use Jane's public key (available to anyone) to encrypt the message so that Jane, using her private key (available to her alone), is the only person who can decrypt it.

---

24. *See generally* Paul Toscano, *Cyber, Cypher, and Sense: Are You Ready for O.D.A.—Year Zero of the Digital Age?*, 12 Utah. B.J. 8 (Nov. 1999).

25. *See* Kenneth P. Weinberg, *Cryptography: "Key Recovery" Shaping Cyberspace (Pragmatism and Theory)*, 5 J. Intell. Prop. L. 667, 674 (1998) (describing the "shared single key" cryptography system).

26. *See generally* Christopher C. Miller, *For Your Eyes Only? The Real Consequences of Unencrypted E-Mail in Attorney-Client Communication*, 80 B.U. L. Rev. 613, 625 (2000) (describing public and private key cryptography).

27. *Id.*

This relationship between the public and private keys of a twin key pair allows a person to encrypt a message with a key (the private key) that never needs to be shared with anyone else.[28] This is because the message can be decrypted with the corresponding twin key (the public key), which is available to anyone.[29] The importance of this fact cannot be overstated. Asymmetrical twin key encryption is a vastly better than symmetrical encryption as a means of securing the transmission of personal, sensitive, or legally significant digital and electronic information.[30] This is true despite the fact that, until recently, it has been somewhat more cumbersome to employ than symmetrical (single key) encryption or other security protections such as passwords, digital fingerprints, and retinal scans.[31]

What is at stake is personal autonomy. The risks involved were dramatically addressed in a different context by Viktor Frankl.[32] In his book, *Man's Search for Meaning*,[33] Frankl recalls his experiences in a Nazi concentration camp and refers to the number stitched on the clothes or tattooed on the skin of camp prisoners.[34] Each number represented a prisoner.[35] In time, the guards stopped looking at the prisoners and looked only at the numbers.[36] The prisoners themselves became invisible.[37] The numbers were all that mattered.[38] Individuality was objectified.[39] Personhood was reduced to digits.[40] This historical example should serve as a cautionary tale for the digital age where, in cyberspace, people are necessarily represented by identifying numbers and where their personal identifying information, communications, transactions, educational and credit records, financial and health records can be connected with and accessed by these numbers. Lives and meaning in the real world depend upon the form, content, accuracy and use of such infor-

28. *See* Gary Rice, *Strategies for Financial Institutions in the New E-Commerce Economy*, 1156 PLI/Corp 803, 915–16 (Dec. 1999).

29. *See* James Hill, *Lock and Load*, 8 Bus. L. Today 8, 10 (Nov/Dec 1998).

30. *See generally* Toscano, *supra* n. 24.

31. *Id.*

32. *See Viktor Frankl, Renowned Austrian Psychiatrist, Dead at 92* <http://www.rigeib.com/thoughts/frankl/frankl.html> (accessed Nov. 10, 2000). Viktor Frankl, born in 1905, was imprisoned at Auschwitz in 1942, survived, resumed his work as a psychiatrist after World War II, founded the school of logotherapy in Vienna, Austria, and died in March 1999. *Id.*

33. Viktor Frankl, *Man's Search for Meaning: An Introduction to Logotherapy* 63 (Simon & Schuster 1959).

34. *See id.* 9063.

35. *See id.*

36. *See id.*

37. *See id.*

38. *See id.*

39. *See* Frankl, *supra* n. 33, at 63.

40. *See generally id.*

mation. To the extent that such information is not in the control of the person it identifies, that person has in some measure lost the power of self-determination over his or her past, present, and future. Identifying information outside the control of the identified person may be altered, corrupted, manipulated, and used in ways that can subvert truth, damage or rob the identified person, or do injury to that person's relationships. To avoid these harms, the person whom the information identifies must maintain ownership and control of much of this information.

Encryption is an indispensable tool in achieving this result. But which type of encryption should be used, symmetrical encryption (where one key only is used to both encrypt and decrypt) or twin-key encryption (where a text encrypted with one can be decrypted only with its mate)? Single-key encryption requires an individual to be represented in cyberspace by a single shared secret. This approach invokes the insecurity of a shared secret code and the potential of dehumanization of identification numbers that can be manipulated outside the control of the identified person. Twin-key encryption, however, allows a person to be represented by two mathematically related keys, one private and the other public. The two keys correspond to the dual nature of human identity: mind and body. This duality of interior and exterior forms the basis of human identification in the real world where we distinguish one another by such exteriorities as unique facial and bodily characteristics and by such externally manifest interiorities as knowledge, personality traits, attitudes and habits of communication. For example, even though identical twins might be indistinguishable by their exterior traits, one twin could distinguish herself from her sister by revealing something about herself that her twin could not know.

In the cyber world, asymmetrical twin key encryption allows a person to be represented by a key pair, of which the private key represents the person's interior (which is unknowable unless the person chooses to reveal some manifestation of it) and of which the public key represents the person's exterior (which can be relied upon as a means of verifying that person's cyber identity).[41] Together, the two keys comprise an individual's single cyber identity.[42] This precision of representation allows an individual to use his or her private key to manifest interior intent using the private key as an encryption code.[43] This is possible because the private key is unique to and is held solely by its owner.[44] The encryption the key produces is unique and can be decrypted only with the

41. David L. Gripman, Student Author, *Electronic Document Certification: A Primer on the Technology Behind Digital Signatures*, 17 John Marshall J. Computer & Info. L. 769, 775 (1999).

42. *Id.* at 775, nn. 51, 53.

43. *Id.*

44. *Id.*

corresponding public key, which is embodied in a digital certificate that contains the identifying information of the owner of the unique key pair.[45]

The application of private key encryption to a document is called a "digital signature."[46] Unlike a digitized signature (which is merely a piece of digital art made to look like a signature and can be copied from one document and pasted to another), a digital signature is a mathematical operation involving the use of the private key to alter the fundamental nature of a document being signed.[47] Once digitally signed, a

45. *Id.*

46. *See generally* NIST, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication* <http://csrc.nist.gov/publications/nistpubs/800-25/sp800-25.pdf> (accessed Dec. 18, 2000).

47. To understand the fundamental nature of a digital document, it is necessary to understand that cyberspace is, in essence, comprised of electronic impulses. Digital information consists of patterns of electromagnetic charges that can be transmitted or preserved in such media as silicon (as in silicon chips), magnetic tape (as in floppy disks), or as light patterns in plastic (as in CDs). The presence and absence of electromagnetic charges can constitute a microcosmic code—analogous to Morse code—and used to communicate with machines. This is possible because a machine can be made to respond to a given pattern of such charges. A computer is just a machine. To a computer, a human readable text is merely a stream of electromagnetic impulses. These impulses can be expressed by humans as patterns of zeros and ones, where a one represents the presence and a zero the absence of an electromagnetic charge. Most people in the world use the ten Arabic digits (0–9). However, any number can be written using only the digits 0 and 1 by adopting the logic of the binary number system (0 = 0, 1 = 1, 2 = 10, 3 = 11, 4 = 100, 5 = 101, 6 = 110, 7 = 111, 8 = 1000, 9 = 1001, 10 = 1010, etc.). This system is used to create patterns of zeros and ones that represent patterns of electromagnetic charges. Using binary numbers, a computer programmer can create computer codes or programs. For example, the binary number 1011 can be used to represent the letter "A." The number 1011 actually represents a pattern of electromagnetic impulses (1 = Charge, 0 = No charge, 1 = Charge, 1 = Charge). The programmer can tap out the binary number on a keyboard and cause the equivalent charge or no charge to be created as a pattern of impulses. The computer can be made to receive this pattern and save it. It can also be made to receive this pattern and compare it against an already saved version of it. Upon comparison, if the two patterns match, the computer can be made to send a signal that creates a light pattern on a monitor that, to a human, is readable as the letter "A." Every symbol readable to humans is really a binary code that represents a corresponding pattern of electromagnetic impulses that is readable by the computer. A text made up of such symbols is a digital text because its symbols are comprised of patterns of the digits 0 and 1. To encrypt such a text, it is necessary only to alter the 0s and 1s from the standard patterns used to represent the alphabet into idiosyncratic patterns that produce gibberish instead. Such an encryption process treats the string of digits constituting the plain text as if those digits were a single number. The process then performs on that number a mathematical operation such as multiplication and applies to that operation another number such as a public or private encryption key. Thus, by taking the plain text number and multiplying it by the encryption code number, the resulting product will be a number that constitutes the encrypted message or cipher text. When the computer reads this cipher text, it will produce not the letters of the alphabet, but a text of nonsense. This is because the 0s and 1s of the cipher text no longer correspond to the codes for the letters of the alphabet. The only way a human can read this message is to decrypt it

document cannot be altered without nullifying any digital signature applied to it.[48] The use of a private key as a digital signature is the way the private key owner manifests in cyberspace his or her interior intent and willingness to be bound by the terms and provisions of a digital or electronic contract or document.[49] Anyone can verify a digital signature on the document by using the private key owner's corresponding public key to decrypt the document and reveal the signer's identity.[50] A digital signature can also be used as proof that the signatory of an electronic or digital record is its putative owner.[51]

A message can also be encrypted with the intended recipient's public key.[52] By doing this, a sender can be assured that the encrypted message can be read only by the intended recipient, who alone can decrypt it with the corresponding private key held solely by its owner. Sending a transmission encrypted with the public key of the intended recipient is tantamount to identifying a person by his bodily characteristics and then whispering a message in his ear to ensure that only he hears it.

Asymmetrical twin key cryptography avoids the dangers and potential evils of the shared secret. It allows individuals to control their personal, sensitive, and identifying digital and electronic information by digitally signing it.[53] Whatever information is not digitally signed is unclaimed, unacknowledged, or disavowed and, therefore, unreliable.[54] It also allows people to control access to information by encrypting it so that only intended parties can read it.[55]

Public key systems employing asymmetrical twin key cryptography are becoming more and more popular for transmitting information via the Internet.[56] These systems are extremely secure. It is practically impossible to derive the private key from the public key.[57] Mathematically, the computation time required to derive one 1024–bit cipher from its twin would take about 5 million years, even if supercomputers were employed in the process of cryptanalysis.[58] Though difficult to crack, these

---

by returning the 0s and 1s to their original plain text pattern. If a public key was used to encrypt such a text, then only the corresponding private key can be used to reverse the mathematical operation and return the scrambled 0s and 1s and corresponding electromagnetic impulses back to their original readable pattern.

48. Gripman, *supra* n. 41, at 777.
49. *Id.*
50. *Id.*
51. *Id.*
52. *Id.* at 779.
53. Toscano, *supra* n. 24, at 9.
54. *Id.*
55. *Id.*
56. *Id.*
57. *Id.*
58. *See* Bruce Schneier, *Applied Cryptography* 160 (2nd ed., Willey & Sons 1996).

keys are simple to use, and more importantly, they appropriately reflect the mind–body duality of human personhood and allow individuals to enjoy security in the transmission of data.[59]

IV. DEFINITIONS AND REQUIREMENTS FOR INFORMATIONAL SECURITY, PRIVACY, AND INTEGRITY

In the balance of this paper, I will propose working definitions of informational security, privacy, and integrity that create distinctions among these concepts even though it is possible to define them as synonyms. I will also provide a suggested list of minimal requirements necessary for cyber citizens to enjoy the same degree of informational security, privacy, and integrity on the Internet and in wireless communications that they have come to expect in paper transactions.

A. SECURITY

As used herein, the term "security" refers, at a minimum, to three different protections. First, security refers to any protection that enables data to be transmitted from a known source to an intended recipient only.[60] Second, security refers to any protection that enables such information to be stored, transmitted, processed, or used without compromise, alteration, or corruption.[61] Finally, 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 identifier.[62]

---

59. *See* Whitfield Diffie & Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* ch. 2 (MIT Press 1999). Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman and is sometime called Diffie-Hellman encryption. *Id.*

60. For example, an e-mail message may, before it is sent, be encrypted with the unique encryption key of its sender thereby identifying the source of the message. It can also be encrypted again with the unique encryption code of the intended recipient, thereby ensuring that only he or she can read it.

61. An e-mail message is merely a string of binary numbers that represent the numerical codes that are translated by the computer into letters, numbers, and symbols readable by human beings. Before an e-mail message is sent, the binary numbers that constitute the message can be treated as a single number and arithmetically reduced to a smaller, one-of-a-kind number, called the hash number. This hash number can be sent with the message. Upon its arrival, the message can be hashed again. The two hashes can be compared. An exact match is proof that the message sent is identical to the message received. A mismatch is proof that the message sent differs in some respect from the message received and, therefore, should not be trusted. Hash numbers are used in this way to make digital transmissions tamper proof.

62. The reliability of any cyber identifier depends entirely upon the reliability of the practices used to authenticate, document, and certify the identity of the real world person and bind the authenticated identifying information to that person's cyber identifier.

B. PRIVACY

Establishing a clear meaning for informational privacy is a bit more challenging. There is no universally accepted definition for privacy or for informational privacy.[63] A normative definition of privacy—based on what "normally" should be kept private—does not work because on this subject, people from culture to culture cannot agree.

Rather than a normative definition, I propose here an analytical one that is based on an analysis of the recurring elements that are essential to privacy regardless of what is being kept private.[64] This approach requires some reflection on how privacy is established in other contexts. For example, how is privacy created or preserved with respect to real property? The answer is based on experience and intuition. The first step in creating private property is to separate it from the property around it. Separation is what the word "private" actually means. It is derived from the Latin *privates*, which comes from Latin *privo*[65] meaning, "to separate." The word was used to describe property that had been partitioned from community property and was identifiable as belonging to or concerning an individual.[66] The next step after partition is to restrict access to the property to its owners or their designees. The final step is to assure that the beneficial use of the property flows only to its owners or someone authorized by the owners such as a tenant with the right to occupy, farm, or mine the property or someone to whom an easement has been granted.

When it comes to something more personal than real estate—one's body, for example—the same principles apply. To be assured of bodily privacy, one's body must first be identifiable as separate from anyone else's body. Once a separate body is established, there is little doubt that bodily privacy includes the right of a person to control and restrict access to his or her own body. Without such control, personhood could not be possible, and one would be merely the object of others. Bodily privacy also requires that a person have the exclusive beneficial use of his or her body and the right to decide who else can benefit from that use.[67]

What is true of the human body and of bodies of land is also true of any property, including bodies of information, whether electronic or otherwise. Informational privacy, then, can be defined analytically as sepa-

63. Ira Glasser, *The Struggle for a New Paradigm: Protecting Free Speech and Privacy in the Virtual World of Cyberspace*, 23 Nova L. Rev. 627, 627-28 (1999).

64. Paul J. Toscano, Presentation, *Taming the Cyber Frontier: Security Is Not Enough!* (Carnegie Mellon Institute for Survivable Systems, July 24, 2000).

65. *Webster's Third New International Dictionary* 1804–05 (3rd ed., Merriam –Webster 1993)

66. *Fahnestock v. Fahnestock*, 76 Cal. App. 2d 817, 819 (Cal. App. 1946).

67. Donna M. Lambert, Fernando R. Laguarda, & Amy L. Bushyeager, *Overview of Internet Legal and Regulatory Issues*, 544 PLI/Pat 179, 230 (1998).

rate ownership or control, restricted access, and beneficial use of digital or electronic information. In discussions of informational privacy, little is said about these essentials—probably because they are so fundamental they are left unaddressed as *a priori* assumptions.

C. SEPARATENESS

Before a legitimate claim of informational privacy can be sustained, the information in question must be rendered separate and identifiable.[68] This involves the process of partitioning the data, that is, quarrying it out of the data with which it is commingled.[69] Until partition takes place, there is nothing to which a claim of ownership can attach.[70] 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.[71] For example, a claim of ownership in data may be based on an author's common law copyright or on a publisher's purchase contract. It may be based on inheritance, a lease, a 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 given that describes the property, the boundaries, and those with ownership or access rights to it.

In the virtual world, such boundaries and claims of ownership and use can be established by public key infrastructures[72] managing asymmetrical twin key cryptography. Public and private encryption keys can now be issued to users. These public and private keys can be certified to

68. *See generally* David F. Linowes & Ray C. Spencer, *Privacy: The Workplace Issue of the '90s*, 23 John Marshall L. Rev. 591 (1990).

69. *Id.*

70. *Id.*

71. *Id.*

72. *See* The Usertrust Network, *What Is a PKI?* <http://www.usertrust.com/pki/index.asp> (accessed Oct. 17, 2000) [hereinafter *Usernet*]. A public key infrastructure ("PKI") is an arrangement of technological, organizational, legal, and security systems that supports the integrity, reliability, and inter-operability of digital certificates, digital signatures, and applications based on digital signature technology. *Id.* A PKI can consist of policy approval authorities, certificate authorities, and registration authorities that verify and authenticate the identity of each party involved in an Internet transaction. *Id.* PKIs are currently evolving and there is no single PKI or even agreed-upon standard for organizing a PKI. *Id.* However, nearly everyone agrees that reliable PKIs are necessary before e-commerce and e-business can become widespread. *Id.* In sum, a PKI is what makes a digital signature valid. *Id.*

users whose identities have been acceptably authenticated. Such users can encrypt or digitally sign data streams with these keys. In this way, 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—an important step forward.

D. 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 interlopers. Restricted access to digital and electronic information can also be achieved using 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 to each key pair. If that private key were lost, stolen or damaged, then the encrypted information would remain virtually irretrievable. This is not an attractive prospect, especially in a commercial environment where documents are vital. 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.[73] The private key is a digital signature.[74] 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.[75] Or, even more troubling, the private key owner could allege that his or her digital signature had been used without authorization and thus repudiate the enforceability of a digital signature to avoid obligations under an electronic contract.[76] A partial solution to this problem is to generate two key pairs for each subscriber and require the subscriber to dedicate one key pair for digital signing only and the other key pair for encryption only.[77] In this way, the private key of the encryption key pair could be

73. *See* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 142 U. Pa. L. Rev. 709, 712 (1995).

74. *Id.*

75. *Id.*

76. *Id.*

77. *Id.*

escrowed or copied since it is used only in encryption functions.[78] The problem with this approach is that the escrowed or copied private key could be used maliciously or inadvertently to digitally sign a document.[79] If this occurred, it could be argued that a legally binding document had been created even though it had been signed with a private key that was not issued as a digital signature.[80] This multi-key pair approach could lead to uncertainty as to the enforceability of digital signatures.[81] The resulting uncertainty would fuel unnecessary disputes and litigation as to the enforceability of digital and electronic contracts. In any case, to restrict key pair use in this way calls for the trustworthy management of key pairs according to fair, reliable, and evenhandedly enforced rules. For these reasons, confidentiality and restricted access to information is not reliably achieved by encrypting data with a public key. A better method of assuring confidentiality and restricting access to cyber information is needed.

E. Beneficial Use

In addition to the separateness of and restricted access to data, informational privacy requires the assurance that only data owners or parties authorized by them 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 will be accessible, readable, and usable only by authorized parties, and in spite of technological advances or obsolescence. To achieve beneficial use requires data vaulting.[82] Information, such as e-contracts, personal identifying information, or sensitive medical or legal information must be preserved to ensure its availability to authorized parties in the indefinite future.[83] To achieve this end, digital signatures with which documents are signed

78. *Id.*

79. *See* Michael J. Osty & Michael J. Pulcanio, *The Liability of Certification Authorities to Relying Third Parties*, John Marshall J. Computer & Info. Law 961, 967–68 (1999) (stating that electronic transactions are still susceptible to fraud).

80. *Id.*

81. *Id.*

82. Symposium, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 Wash. U. L.Q. 461, 462 (1999).

83. *See* NARA, *Records Management Guidance for Agencies Implementing Electronic Signature Technologies* <http://www.nara.gov/records/policy/gpea.pdf> (accessed Dec. 18, 2000).

must remain both identifiable and legally binding.[84] Documents must be rendered persistent both as to form and content.[85] A document's admissibility as evidence in a court must be assured.[86] A record must be kept of the source, date of origin, history, and chain of custody of a document together with the identity of its owners and any parties with authorized rights of access and use.[87] In addition, an auditable record of access and retrieval must be kept to prevent confusion and maintain record chronology.[88]

Without these safeguards, users can have no assurance that they will receive the beneficial use of information and of the obligations memorialized in digital documents. Consequently, they will be reluctant to bring their paper process online and forego the cost savings, gains and other benefits of the Internet, the Web, and wireless communications systems. This is especially true for professionals in the legal, health care, accounting, real estate, lending/leasing, and intellectual property arenas—professionals with a duty to protect the confidences and secrets of their clients or patients.[89]

F. INTEGRITY

In addition to the three security protections and the three elements of privacy discussed here, e-business customers need information integrity as well. They need the assurance that digital and electronic information will be retained according to rules that ensure its preservation in a trustworthy environment so it continues to serve the purposes for which it was intended.[90] Information integrity means that personal data will remain personal, sensitive information will remain confidential, and legal documents will remain enforceable. Information integrity in cyberspace is achievable only if digital and electronic information is securely retained in the possession of trusted third-party custodians.

The most troubling problem plaguing e-commerce is the retention of proprietary data by non-neutral, biased, interested parties.[91] User information is typically warehoused with digital database services offered by for-profit companies.[92] These companies are run by management teams and boards of directors whose overriding duty is to their company share-

84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.*
88. *Id.*
89. *See generally* Jeffrey Rosen, *The Eroded Self*, N.Y. Times Mag. 46 (Apr. 30, 2000).
90. Federal Trade Comm., *Online Profiling Workshop of 1999* (Nov. 8, 1999) (provided by Alderson Reporting Company at 1-800-FOR-DEPO) [hereinafter FTC Workshop].
91. *Id.*
92. *See Usernet*, *supra* n. 72.

holders, not to the data owners.[93] Subscribers to such services place personal, sensitive, legally significant, or valuable proprietary information in the care of companies whose self interest may conflict with the subscribers' interests.[94] 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 in which the security, privacy, and integrity of information can adequately be guaranteed.

Information integrity requires data custodians to be neutral, even-handed, independent, and free from disqualifying conflicts of interests.[95] Informational integrity can be assured only when it is in the safekeeping of trustee-like custodians who have one duty only: to apply fair information practices to preserve for data owners or originators 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.[96] Only such custodians can reliably certify a traceable and auditable document registry, provide a reliable chain of custody, or assure the evidentiary integrity of such information.

V. PRIVACY ARCHITECTURE AND PERSONAL AUTONOMY

What is required is a privacy architecture that can assure full information reliability, consisting of all the aspects of security, privacy, and integrity discussed here. Without these assurances, there can be no guarantee in the virtual world of personal autonomy—the unimpeded use of private resources and information to pursue individual, self-determined ends and outcomes apart from the requirements of the collective. Personal autonomy is the prime value in an open, democratic society and should not be sacrificed on the altar of expedience, digital or otherwise. Personal autonomy in the virtual world requires a neutral, independent, non-governmental, self-regulatory architecture that combines law and technology to ensure data originators, owners, and users the following privacy protections:

1. That data can be rendered separate and identifiable;

2. That data ownership and access rights can be identified, registered, and properly managed;

3. That data will not knowingly be viewed, altered, intercepted, copied, confiscated, or divulged without authorization of its owners or originators;

---

93. *Id.*

94. *See generally* Rosen, *supra* n. 89; *see also Usernet*, *supra* n. 72.

95. *See id.*

96. *See* Osty & Pulcanio, *supra* n. 79, at 964–67.

4. That a person's digital likeness will not be appropriated;[97]

5. That there will be no intrusions upon a person's solitude or seclusion by eavesdropping on digital or electronic communications or by persistent unwanted communications;[98]

6. That there will be no disclosure of information that puts a person in a false light;

7. That personal and sensitive information will be collected, stored, processed, retrieved, and used only according to published fair information practice rules;[99]

8. That data management risks and liabilities will be minimized;[100]

9. That data owners will maintain control of their own personal, sensitive, and legally significant information;

10. That a reliable, auditable record of data will be kept and its chain of custody be maintained for certification to authorized requesting parties;[101]

11. That data owners and authorized users will be identified by cyber IDs that have been acceptably authenticated and certified; and

12. That cyber ID authentication and certification along with the collection, storage, processing, retrieval, and use of personal, sensitive, confidential and secret data will be managed reliably by private, unbiased, trusted third-party fiduciary custodians with an unconflicted duty of care to data owners or putative owners and parties authorized by them.[102]

VI. CONCLUSION

For cyber citizens to feel safe on the cyber frontier, they must be confident that information security, privacy, and integrity will be ensured. Internet, Web, and wireless communication must be preserved as an open and level foundation for all. There must, however, be built on this foundation, a private, trust-based and supra-jurisdictional architecture, managed by neutral third-party custodians who serve in the place

97. *See Perfect 10, Inc. v. Talisman Communications, Inc.*, 2000 WL 364813 (C.D. Cal Mar. 27, 2000).

98. *Electronic Communications Privacy Act*, 18 U.S.C. §§ 2701–11, 3117–27 (2000).

99. *See* FTC Workshop, *supra* n. 90.

100. *Id.*

101. *See* Keith Perine, *The Persuader*, The Industry Standard 154, 161–62 (Nov. 13, 2000).

102. This list is the result of my analysis of various aspects of informational privacy concerns, protections and assurances. *See* Council Directive, *supra* n. 20; William L. Prosser and W. Page Keeton, *Prosser and Keeton on the Law of Torts* (West 1984); *see also* Ellen Alderman & Caroline Kennedy, *The Right to Privacy* 157 (Vantage Books 1997) (explaining the invasion of privacy torts).

of government to act without bias, undue influence, or profit motive to assure the evenhanded administration of fair information policies, procedures, protocols, and practices that 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 this architecture is available to all cyber citizens on an equal footing, cyberspace will be safe for e-business. Rather than take the many decades it took to achieve the constitutional foundations for an open society and a free market in the real world, the opportunity exists now to move at Internet speed to adopt in the virtual world technologies, definitions, legal structures, and business processes indispensable to personal autonomy, individual liberty, and the pursuit of e-commerce and e-business worldwide.