UIC John Marshall Journal of Information Technology & Privacy Law

Volume 14
Issue 2 *Journal of Computer & Information Law - Winter 1996*

Article 5

Winter 1996

The High Price of a Cashless Society: Exchanging Privacy Rights for Digital Cash, 14 J. Marshall J. Computer & Info. L. 303 (1996)

Catherine M. Downey

COMMENTS

THE HIGH PRICE OF A CASHLESS SOCIETY: EXCHANGING PRIVACY RIGHTS FOR DIGITAL CASH?

I. INTRODUCTION

Imagine the typical excursion to a shopping mall. Shoppers must load their purses or wallets with cash, checks and credit cards, travel to the shopping mall and then drive up and down the aisles looking for a parking spot. Once inside, their adventure continues with overzealous salespeople, and of course, waiting in the check-out line in order to pay with "cash, check or charge," each method involving its own clumsy process.

Now, imagine making the same trip to a shopping mall on the Internet. Shoppers can sit leisurely at their home computers and arrive at the shopping mall instantly with the click of a mouse. Then, shoppers can browse through the electronic shops and sample products without encountering even one ambitious salesperson. The shoppers' excursion ends by simply clicking a button, enabling them to pay with digital cash.[1]

Digital cash will transform the "Internet from a huge virtual community into a huge virtual economy."[2] Developers have already created on-line shops, even "electronic shopping malls."[3] Recent advancements allow credit card purchases over the Internet ranging from computer-related items to music, clothes and even vacations.[4] Digital cash, fast and flexible in form, will enable consumers to purchase these items in

1. Digital cash is the currency used in a system which transfers money over the Internet from the bank to a user or from a user to another. *What is E-Cash?*, AM. LAW., Mar. 1995, at 17.

2. *Electronic Money: So Much for the Cashless Society*, ECONOMIST, Nov. 26, 1994, at 21 (explaining the dynamics of digital cash, its development and its potential security issues).

3. *Id.* Most electronic "shopping malls" sell items including words, pictures, computer programs, and services. *Id.*

4. *See* WWW Page: *The Internet Mall*, URL: http://www.meclerweb.com/imall/; WWW Page: *The Shopper Expressway*, URL: http://shopex.gens.com, Last Revised: June 5, 1995,

cyberspace[5] with the same freedoms they enjoy with paper cash.[6] Many digital cash systems conceal users' identities and guard against the discovery of financial information by the government, businesses and computer hackers.[7]

Complete user anonymity over the Internet, however, makes the user's transactions untraceable. As a result, these transactions extend beyond the reach of current law enforcement policing methods.[8] Thus, the use of digital cash over the Internet creates the challenge of balancing privacy concerns with the government's legitimate security interests. In order to effectively harmonize these competing interests, this Comment asserts that Congress must enact a federal statute directly addressing the use of digital cash.

Part II of this Comment describes what the advent of digital cash means to the average user, examining the dynamics of the Internet and digital cash. In order to explore current privacy laws, Part II further focuses on the Privacy Act of 1974,[9] the Right to Financial Privacy Act,[10] and the Electronic Communications Privacy Act.[11] Finally, Part II reviews the courts' interpretation of privacy legislation and its applicability to digital cash transactions. Part III argues that the Internet's regulatory system does not effectively protect digital cash users' privacy. Part III also asserts that the current statutory privacy laws and court decisions offer an inadequate framework for protecting privacy in digital

---

Operator: VP (Internet site offering on-line shopping); WWW Page: *PL Travel*, URL: http://www.PCtravel.com, American Travel Corporator (site offering on-line vacation planning).

5. Author William Gibson popularized the term "cyberspace" in the early 1980's. Don Oldenberg, *The Law: Lost in Cyberspace*, COMM. DAILY, Mar. 27, 1991, at 9. "Many Internet users use the term to describe the electronic continuum they metaphorically inhabit." *Id.*

6. Carol Levin, *The PC in Your Wallet; Smart Cards are Poised for Mass Consumption*, PC MAG., Mar. 29, 1994, at 29. The development of digital cash expands well beyond use on the Internet. Many companies have been designing and attempting to implement electronic cash systems to work between banks, merchants and consumers for use on smart cards. *Id.* Smart cards look much like standard credit-cards, yet they contain a microprocessor and storage function for recording and storing massive amounts of data. *Id.*

7. Jonathan Graham, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395 (1987) (explaining how the government uses personal information to develop personality profiles of individuals which include, *inter alia*, the spending patterns, lifestyle and other personal choices of the individual).

8. Benjamin Wittes, *Government Seeks a Way to Keep Tabs on Computer Cash*, THE RECORDER, Feb. 2, 1995, at 1. According to concerned officials, certain digital cash schemes now being developed make anonymous financial transactions "a law enforcement nightmare." *Id.* Allowing untraceable transactions enables money launderers, drug dealers and terrorists to move cash freely over computer networks, while "cops only wring their hands." *Id.*

9. The Privacy Act, 5 U.S.C. § 552(a) (1982).

10. The Right to Financial Privacy Act, 12 U.S.C. § 3401 (1978).

11. The Electronic Communication Privacy Act, 18 U.S.C. § 2510 (1986).

cash transactions. Finally, Part IV concludes that Congress must enact a federal statute to protect the financial privacy of digital cash users on the Internet. Without new federal legislation, users will not trust the Internet to serve as a secure, global banking community, and as a result, the laws of today will stifle the technological expansion of tomorrow.

II. BACKGROUND

The framers of the Constitution could not have planned for, much less imagined, the technological explosion that has rocked our conventional world. Even a century after the Constitutional Convention, when Samuel Warren and Louis Brandeis published their famous privacy article in 1890,[12] no one could envision that the "right to be let alone"[13] would someday encompass people using computers to communicate across the globe on the Internet.[14] Now, the creation of digital cash further challenges the parameters of privacy laws.

A. THE INTERNET AND DIGITAL CASH

The Internet[15] is a large computer network[16] consisting of millions of computers hooked together through telephone lines into one more or

12. Samuel Warren & Louis Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193 (1890).

13. *Id.*

14. JOHN R. LEVINE & CAROL BAROUDI, THE INTERNET FOR DUMMIES 7 (1993).

15. Peter E. Dyson, *Publishing on the Internet for Fun and Profit*, SEYBOLD REP. ON DESKTOP PUB., Apr. 4, 1994, at 3. The Internet originated as a project of the Department of Defense called the Advanced Research Projects Agency ("ARPAnet"). *Id.* It served as a means of linking the defense department with university computer-science departments doing military-funded research across the country. *Id.*

However, during the 1980's, the Internet became a tool for academics. *Id.* The National Science Foundation ("NSF") actively encouraged universities to connect their computers to national supercomputer sites using its high-speed backbone lines. *Id.* However, a very fine line developed between distinguishing the open use of academic research from private commerce. *Id.* As a result, the NSF attempted to develop a policy for the acceptable use of the NSF-funded portion of the network. *Id.*

The NSF policy for the acceptable use of the NSF-funded portion of the network states that the "NSFnet backbone services are provided to support open research and education in and among U.S. research and instructional institutions, plus research arms of for-profit firms when engaged in open scholarly communication and research. Uses for other purposes is not acceptable." *Id.* This regulation only added more confusion, providing new motivation for the private sector to move toward commercial network backbones. *Id.*

16. *Clinton Administration Report on the Global Information Infrastructure "Agenda for Cooperation,"* NAT'L AFFAIRS, Feb. 16, 1995, at 32. The Internet connects fifty-nine countries, 3.8 million computers and an estimated 20-30 million users, and is growing at a rate of 10-15% each month. *Id.* Therefore, a new network is connected to the Internet every thirty minutes. *Id.*

less unified system.[17] The computers on the Internet correspond using agreed-upon methods of communication.[18] As a network, the computers freely exchange information, and dynamic rerouting[19] ensures that information flows between the network links without interruption.[20] Today, people use the Internet to exchange e-mail, access digital libraries, publish multimedia documents and coordinate worldwide business, academic and social activities.[21]

While digital cash has surfaced in various forms, including the smart card[22] or bank card form, the Internet lures common shoppers and business people alike because of its experimental forum, global community and relaxed regulatory system.[23] Beneath the complex technology, digital cash systems function over the Internet quite simply.[24] Visually, the user views options on the computer screen for withdrawing, paying or finding out the status of an account.[25] To make a purchase, a user simply chooses "get $X from bank" and "send $X to merchant," and the transaction occurs automatically within the Internet.[26]

Functionally, the typical digital cash system follows a logical process. First, the user establishes an account with the bank in the ordinary manner.[27] When the user wants to purchase an item from a merchant, he simply sends the bank a special electronic message, encoded with a unique digital signature[28] requesting the money.[29] The

17. Dynamic rerouting ensures the reliability of the Internet. LEVINE & BAROUDI, *supra* note 14, at 12. If one of the network links becomes disrupted, traffic can automatically be rerouted to other links. *Id.*

18. Common Data Protocol are "agreed-upon methods of communications used by computers and by people." LANHAM, THE INTERNET CONNECTION 6 (1995).

19. The Internet started as a project by the Department of Defense ("DOD") in 1969 as an experiment in reliable networkings to link together DOD and military-funded research. LEVINE & BAROUDI, *supra* note 14 at 11-12. The reliable networking developed into dynamic rerouting: "If one of the network links became disrupted by enemy attack, the traffic on it could automatically be rerouted to other links. Fortunately, the Net rarely has come under enemy attack, but, an errant backhoe cutting a cable is just as much a threat, so it's important for the Net to be backhoe-resistant." *Id.*

20. *Id.*

21. Dyson, *supra* note 15 at 3.

22. *See* Levin, *supra* note 6, at 29. Smart cards—credit cards with tiny built-in microprocessors—provide another method of digital commerce. *Id.*

23. Benjamin Wittes, *A (Nearly) Lawless Frontier; The Rapid Pace of Change in 1994 Left the Law Chasing Technology on the Information Superhighway*, AM. LAW., Jan. 3, 1995, at 1.

24. *What Is E-Cash?*, *supra* note 1, at 1. (describing step-by-step, how a typical digital cash system would work using fictional characters to represent average users).

25. *Id.*

26. *Id.*

27. *Id.*

28. John B. Kennedy & Rebecca R. Davids, *The Paper Paradigm Becomes Obsolete; Electronic Surrogates Require New Standards*, N.Y. L. J., Jan. 23, 1995, at S1. While a full

bank debits the user's account and sends "e-cash"[30] to the user's computer via the Internet. After receiving the e-cash moments later, the user's computer immediately transmits it to the merchant's computer, which reads the bank's "signature," verifies the authenticity of the e-cash with the bank and credits it to the merchant's account.[31]

B. Digital Cash Systems: Identification of the User

Some digital cash proposals allow the bank to identify the recipient of the original e-cash,[32] while others make it possible for a user to make

---

discussion of data encryption is beyond the scope of this Comment, it does have a place in the digital cash system. Most digital cash systems use a digital signature to authenticate a transaction by implementing "key encryption" technologies. *Id.* The debate over encryption centers around which encryption standard digital cash systems should use and the merits of public and private key encryption. *Id.* Kennedy and Davids explain key encryption in the following manner:

> Key encryption uses a pair of numbers as an encryption code. In private key encryption, both keys are privately exchanged by the contracting parties. In public key encryption, one key is publicly available and associated with an individual or a corporation (the public number is the product of two large primes, one of these prime factors is the private key). To sign a document digitally, the sender uses his or her private key to encode all or part of the document, and the receiver decodes it using the public key. Both private and public key encryption enable digital signature authentication as well as privacy or secrecy. When a particular encryption key is linked definitively to an individual or organization, a encrypted document using such key is effectively signed.

Id.

The importance of determining encryption standards directly relates to the success of digital cash. As a recent Office of Technology Assessment study warns, "[t]he benefits of electronic commerce might be squandered unless Congress brings privacy laws up to date and helps resolve the debate over key escrow encryption." Kevin Power, *OTA Says Congress Should Act to Safeguard Data; Office of Technology Assessment*, Gov't Computer News, Oct. 17, 1994, at 61.

29. *See What is E-Cash?*, *supra* note 1, at 17 for a description of digital cash.

30. "E-cash" stands for electronic cash. The term is interchangeable with the term "digital cash." *What is E-Cash?*, *supra* note 1.

31. *What is E-Cash?*, *supra* note 1.

32. Brad Templeton, *USENIX - Race to Develop Internet Commerce*, Newsbytes, Jan. 23, 1995, at 1. Several systems on the market allow electronic financial transactions on open computer networks on the Internet. According to Nathaniel Borenstein, chief scientist at a company called Virtual Holdings, all of the systems have remarkable differences. *Id.* Templeton explains the following example:

> First Virtual's plan is to act as an intermediary between traditional credit card processing and the Internet (or electronic-mail)-based electronic information merchant. Each user signs up with a credit card then gets a different account number to use in the making of purchases. Each purchase made with this account number gets verified with a piece of e-mail to the owner of the account, and the money is not debited unless confirming e-mail is returned. As such, these account numbers can be sent over public channels since they can only be used by the person whose e-mail address they are associated with.

Id.

a transaction without leaving a paper or electronic trail.[33] Privacy laws impact both of these proposed systems. The decision to reveal or conceal the identity of the user determines whether or not others can obtain the key to the user's financial information. With such access, the government, business and computer hackers become privy to users' private lives.[34] An intruder could examine a person's spending habits, preferences in purchases and personal associations.[35] Moreover, an intruder could use that information to make illicit purchases and transactions.[36] Current privacy laws fail to guard against this dangerous infringement upon privacy.

C. Current Financial Privacy Legislation

The legal system relies on current privacy legislation to dictate the scope of a third party's ability to access a person's financial information. In particular, this legislation proves useful in the electronic funds area.[37] However, current privacy legislation does not address the heightened privacy concerns raised by the use of digital cash on the Internet.[38] The

---

The security and privacy problem with this system is that the account numbers travel over public channels, allowing any person with e-mail to participate in the system. Without encryption, the digital cash system opens the door for "computer abuse." *Id.* Computer abuse is the "unauthorized viewing, alteration and misappropriation of data on networked computer systems." Michael Dierks, *Electronic Communications and Legal Change: Computer Network Abuse*, 6 Harv. J. L. & Tech. 307, 308 (1993).

33. Robert Metcalfe, *New Technologies Provide Better Combinations of Privacy and Anonymity*, Info World, Nov. 28, 1994, at 65. DigiCash, of Amsterdam, The Netherlands, created ECASH, a more secure electronic currency which conceals the user's identity. As Robert Metcalfe explains:

> [T]o use e–cash, the user generates random numbers that serve as bank notes and asks the bank to sign them. The bank signs the note with a secure signature that includes its value, then debits the user's account. When the note is deposited, the bank credits the merchant's account. The bank's signature is blind - meaning it does not see or record the numbers the user assigns to the notes.

Id.

34. *Id.*

35. *Id.*

36. *Id.*

37. Electronic funds transfer ("EFT") is "any transfer . . . of funds initiated through an electronic terminal, telephone, computer, or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account." 15 U.S.C. § 1693(a)(6) (1995).

38. The traditional privacy torts also fail to address the heightened privacy concerns raised by digital cash use on the Internet. There are four distinct privacy tort classifications as outlined by Professor Prosser: (1) intrusion into an individual's private affairs; (2) public disclosure of embarrassing private facts about the individual; (3) publicity that places the individual in a false light in the public eye; and (4) appropriation of an individual's name or likeness for another's advantage without consent. Restatement (Second) of Torts § 652B (1977). These classifications do not directly encompass digital cash. The rapid growth of technology has made Prosser's classifications outdated for dealing with what Professor George B. Trubow of The John Marshall Law School has called, "informa-

following discussion outlines the most important laws in this area: The Privacy Act of 1974,[39] the Right to Financial Privacy Act of 1982[40] and the Electronic Communications Privacy Act of 1986.[41]

1. *The Privacy Act of 1974*

In 1974, Congress enacted The Privacy Act.[42] The Privacy Act was the first federal statute recognizing the need to balance an individual's concern for information privacy with the institutional practice of storing information in a computerized record-keeping system.[43] The Privacy Act regulates the practices of federal agencies regarding personal information.[44] Each federal agency must register the existence of every federal data bank in the Federal Register.[45] With certain exceptions,[46] no fed-

---

tion privacy." George B. Trubow, *The Development and Status of Information Privacy Law and Policy in the United States*, INVITED PAPERS ON PRIVACY LAW: LAW, ETHICS, AND TECHNOLOGY 1 (collection of papers presented at the National Symposium on Personal Privacy and Information Technology, Oct. 4-7, 1981).

The components of information privacy include "(1) what personal information is collected, (2) the circumstances in which someone can see personal information, and (3) how personal information is protected." *Id.*

Other legal scholars have also pointed out the inadequacy of Prosser's classifications to various technological advancements. John Shattuck, *In the Shadows of 1984: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991 (1984) (relying on the privacy torts as a remedy for privacy invasions caused by computer matching systems); Spiros Simitis, *Reviewing Privacy in An Information Society*, 135 U. PA. L. REV. 707 (1987) (discussing the applicability of the privacy torts to modern technologies).

39. 5 U.S.C. § 552(a).

40. 12 U.S.C. § 3401.

41. 18 U.S.C. § 2510.

42. 5 U.S.C. § 552(a).

43. H.R. REP. No. 1383, 95th Cong., 2d Sess. 33, 34 (1978). The drafters of the Privacy Act had three primary goals: (1) to protect individuals' interest in government records concerning those individuals, (2) to regulate practices of federal agencies regarding personal information, and (3) to balance the need of the individual for privacy and that of the government for information about the individual necessary to perform its legitimate functions. *Id.*

44. 5 U.S.C. § 552(a).

45. *Id.*

46. *Id.* §§ 552(a)(1)-(12). The Privacy Act of 1974 lists several exceptions by which federal agencies may gain access to an individual's records to combat criminal activity and to achieve other governmental goals:

> (b) Conditions of disclosure — No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be —
>
> (1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;
>
> (2) required under section 552 of this title;

eral agency may disclose any record contained in its system to any other person or agency without the written request or consent of the individual.[47] Furthermore, the Privacy Act allows an individual to copy, correct and challenge his personal information stored in the data banks of the federal agencies.

---

(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

(4) to the Bureau of the Census for the purpose of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

(6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States Government, or the designee of the Archivist to determine whether the record has such value;

(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency . . . which maintains the record specifying the particular portion desired and the law enforcement activity of which the record is sought;

(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

(9) to either House of Congress, or, to an extent of the matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress of subcommittee or any such joint committee;

(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of General Accounting Office;

(11) pursuant to the order of a court of competent jurisdiction; or

(12) to a consumer reporting agency in accordance with section 3711(f) of title 31.

5 U.S.C. § 552(b).

47. *Id.* § 552a(b). The Act also contains legislative initiatives. For example, Congress enacted the Tax Reform Act to limit access to such information by Internal Revenue Agents. *See* 26 U.S.C. § 6103 (1995). Section 6103 of the Internal Revenue Code, entitled "Confidentiality and Disclosure of Return Information," states that as the general rule, "returns and return information shall be confidential, and except authorized by the title (1) no officer or employee of the United States, (2) no officer or employee of any State . . . and (3) no other person . . . who has had access to returns or return information . . . shall disclose any return or return information obtained by him in any manner in connection with his service as such an officer or employee . . . ." 26 U.S.C. § 6103 (1995).

2. *The Right to Financial Privacy Act of 1982*

Congress enacted the Right to Financial Privacy Act ("RFPA")[48] in 1982 to further protect financial records.[49] The explicit purpose of the RFPA is to balance the need for privacy protection of customers' bank records against the needs of law enforcement.[50] To accomplish this goal, the RFPA does not compel the subject of an investigation to voluntarily provide the government with access to his records.[51] Rather, in order to obtain a customer's[52] financial records[53] from a financial institution,[54] the federal government must follow the procedural requirements of the RFPA[55] and submit a written certification indicating its compliance.[56]

Provided that the government agency has subpoena power,[57] the agency must serve a subpoena on the customer before or concurrently with service on the bank.[58] The government serves the subpoena to-

48. Pub. L. No. 95-630, 92 Stat. 3679 (codified at 12 U.S.C. § 3404 (1995)).

49. 12 U.S.C. § 3404. The RFPA protects an individual's financial records by requiring that "no government authority may have access to or obtain copies of information contained in the financial records of any customers from a financial institution unless the customer has authorized access, or there is an appropriate administrative subpoena or summons, or an appropriate search warrant and unless the financial records are reasonably described." *Id.*

50. H.R. REP. No. 1383, 95th Cong., 2d Sess. 33, 34 (1978). The RFPA balances the need for privacy protections in customers' bank records against the needs of law enforcement investigation by (1) permitting the federal government access to an individual customer's bank records according to certain procedures and (2) giving the customer, in most cases, the right to notification of the government's access attempt and the opportunity to contest the access in court. *Id.*

51. *Id.* An individual need not supply a bank with his financial records voluntarily. *Id.* A bank can not require a customer to give authorization to the federal government to access his financial records as a condition of doing business with the customer. *Id.*

52. "Customer" is a person, an individual, or partnership with five or fewer partners, or an authorized representative of that person who uses a financial institution's services in relation to an account maintained in the individual's name. RFPA, 12 U.S.C. § 3401(4)-(5).

53. "Financial record" means "an original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution." *Id.* § 3401(2) (1995).

54. "Financial institution" generally includes depository institutions and card issuers under the Consumer Protection Act, 15 U.S.C. § 1602(n) (1995). 12 U.S.C. § 3401(1).

55. *Id.* § 3402. The government must use one of the five methods listed in the RFPA to access an individual's records: (1) customer authorization; (2) administrative subpoena or summons; (3) search warrant; (4) judicial subpoena; or, (5) "formal written request." *Id.*

56. Section 3403(b) of the RFPA states, in relevant part, "a financial institution shall not release the financial records of a customer until the Government authority seeking such records certifies in writing to the financial institution that it has complied with the applicable provisions of this chapter." 12 U.S.C. § 3403(b).

57. *Id.* § 3408(1). The use of the formal written request is only available to agencies lacking administrative summons or subpoena authority. *Id.*

58. *Id.* § 3409(a). The RFPA requires service of the subpoena on the customer before or concurrent with service on his bank. However, the court may delay serving the individual

gether with a notice to the customer stating that: (1) the records are relevant to a "legitimate law enforcement inquiry";[59] and, (2) the customer can take steps to block the bank's disclosure of the records.[60] Yet, the customer faces difficult obstacles in challenging or blocking the disclosure of his financial records and must usually wait until after such disclosure to dispute the government's intrusion.[61]

3. *The Electronic Communications Privacy Act of 1986*

The Electronic Communications Privacy Act of 1986 ("ECPA")[62] protects the individual against the unauthorized interception of electronic communications.[63] Titles I and II of the ECPA pertain to common computer-to-computer communications, which include the transmission of financial records or funds transfers among financial institutions.[64] Title I focuses on the interception of wire,[65] oral[66] and electronic communications.[67] Thus, Title I directly applies to most of the data exchanged be-

---

when "there is reason to believe" that such notice will result in a threat to life or physical safety, flight from prosecution, destruction of evidence, intimidation of witnesses, or other serious jeopardy to legal processes. *Id.*

59. 12 U.S.C § 3401(8) defines "law enforcement inquiry" as a "lawful investigation or official proceeding inquiring into a violation of, or failure to comply with, any criminal or civil statute or any regulation, rule, or order issued pursuant thereto." *Id.*

60. *Id.*

61. RFPA, 12 U.S.C. § 3401(8). A customer must usually bring an action in court after the agency has accessed his financial records. The RFPA does not promote the use of preemptive measures to block an agency's access to financial records. A customer must show that the agency failed to comply with the RFPA or that the agency does not seek the records for a "legitimate law enforcement inquiry." *Id.* The RFPA does not detail how the customer must prove either the illegitimacy of the injury itself or the irrelevancy of his EFT records to a "legitimate law enforcement inquiry." *Id.*

62. The ECPA, Pub. L. No. 99-508 (codified at various sections of 18 U.S.C., primarily at 18 U.S.C. §§ 2510-2518); *see generally* Russell S. Burnside, *The Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Telecommunications Technologies*, 13 RUTGERS COMPUTER & TECH. L.J. 451 (1987) (commenting that the ECPA serves as a means of protecting individual privacy in light of new and growing government and private intervention techniques).

63. The ECPA defines an electronic communication as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire . . . that affects interstate or foreign commerce . . . ." 18 U.S.C. § 2510(12).

64. ECPA, Pub. L. No. 99-508.

65. The ECPA defines a wire communication as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception . . . ." 18 U.S.C. § 2510(1).

66. The ECPA defines an oral communication as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." 18 U.S.C. § 2510(2).

67. 18 U.S.C. § 2510 (12).

tween parties using the Internet.[68] Title II of the ECPA[69] addresses access to stored wire and electronic communications and transactional records.[70] Title II explicitly states that a communications service provider "shall not knowingly divulge the contents of a communication while in electronic storage"[71] when communications arrive electronically and the service provider retains records solely for processing and storage.[72]

D. Right to Financial Privacy in the Courts

Legal precedent also shapes an individual's right to financial privacy. According to the Supreme Court,[73] certain aspects of an individual's life fall within a "zone of privacy."[74] Two Supreme Court decisions, *California Bankers Association v. Schultz*[75] and *United States v. Miller*,[76] define the zone of privacy for an individual's financial information.

In *California Bankers Association v. Schultz*,[77] the Supreme Court upheld a challenge to the constitutionality of the Bank Secrecy Act of 1970 ("BSA").[78] Because the BSA aimed to curb crime in interstate and

68. *Id.*

69. Title II of the ECPA resembles Title I in several ways. Both titles exempt disclosure to the intended recipient or an agency of the intended recipient, disclosures to third parties for the purpose of rendering further authorized services, disclosure pursuant to the consent of the originator or the intended recipient, and disclosure of communications information received inadvertently that pertains to the commission of a crime. 18 U.S.C.A. §§ 2702(b)(1)-(4). Title II differs from Title I by setting additional barriers for third party access to an individual's personal records. *Id.* For instance, § 2703 distinguishes between information retained under 180 days and over 180 days. 18 U.S.C.A. § 2703(a). Information stored under 180 days may only be accessed pursuant to a federal or state search warrant. *Id.*

70. 18 U.S.C. § 2510.

71. *Id.*

72. *Id.*

73. *See* Roe v. Wade, 410 U.S. 113 (1973) (finding that a right to privacy exists as to the choice to terminate a pregnancy); Griswold v. Connecticut, 381 U.S. 479 (1965) (holding married couples' choice to use contraception as within the scope of the right to privacy).

74. The Fourth Amendment affords protection to those things that fall within an individual's zone of privacy. The Fourth Amendment states that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

75. 416 U.S. 21 (1974).

76. 425 U.S. 435 (1976).

77. 416 U.S. at 1501.

78. Pub. L. No. 91-509, 84 Stat. 1114 (codified in various sections of 12, 15, and 31 U.S.C.A. (1995)). The U.S. Treasury Department's requirement of detailed record-keeping on all wire transfers, regardless of dollar amount, spurred an important change in the BSA in 1991. Congress enacted the provision to help the government trace and intercept illicitly derived money that moves by wire. *Id.* While performing its investigations, the provision

foreign commerce, the Court found that the record-keeping requirements of the BSA constituted a proper exercise of congressional power.[79] The Court found no Fourth Amendment violation of the rights of the bank or its customer, concluding that record-keeping requirements did not amount to an illegal search and seizure.[80] Moreover, the Court rejected the argument that the BSA violated the Fifth[81] and First Amendments.[82] Thus, following the *Schultz* decision, courts today could reject constitutional challenges and allow the government to monitor a digital cash user's financial transactions in a detailed fashion.

In *United States v. Miller*,[83] the Supreme Court held that a criminal defendant had no Fourth Amendment right to protection of his bank records.[84] The defendant, who had been charged with various federal offenses, made a pretrial motion to suppress the microfilms of checks, deposit slips and other records relating to his accounts at two separate banks.[85] The Court held that the defendant did not have a legitimate expectation of privacy regarding these papers.[86] The Court reasoned

---

has enabled the government to collect, disseminate and store highly detailed information. *Id.*

Before the enactment of the amendments, the BSA explicitly targeted the examination of bank records or wire transfers and telex logs in amounts exceeding $10,000. 31 C.F.R. § 103.11(q) (1995). Now, the government can examine this information with ease regardless of dollar amount. Because of the BSA amendments, bankers must keep uniform records of the following personal information: (1) name of wire transfer and initiator and beneficiary; (2) account numbers of initiator and beneficiary; (3) amount and date of wire transfer; and (4) any other payment instructions. *Id.*

While the BSA does not detail how the government may obtain the records the banks must keep, the Act's legislative history reflects that Congress intended government access only by "existing legal process." *See* H.R. REP. No. 975, 88th Cong., 2d Sess. 10 (1970). Case law suggests that bank records are not within the Fourth Amendment's zone of privacy; thus the "existing legal process" would allow for minimal protection. *See Miller*, 425 U.S. at 439.

79. *California Bankers*, 416 U.S. 21.

80. *Id.* at 52-53.

81. *Id.* at 49.

82. *Id.* at 75-76.

83. 425 U.S. 435 (1976).

84. The Defendant Miller was convicted of moonshining and tax fraud. *Id.* Before the trial, using grand jury subpoenas, Treasury Department agents gained access to Miller's bank account records at two separate banks. *Id.* at 438. These subpoenaed records had been maintained under the record-keeping rules of the BSA. *Id.* at 436. When served with the subpoenas, the banks fully complied by making Miller's records freely available to the agents, who copied various checks, deposit slips, financial statements and monthly statements. *Id.* at 437-38. Neither the banks nor the government advised Miller of the disclosure to the government agents. 425 U.S. at 438. The Supreme Court sustained the use of the subpoenaed records in obtaining the conviction, holding that Miller's interest in the bank records was entitled to no Fourth Amendment protection. *Id.* at 441.

85. *Id.* at 438.

86. *Id.* at 442-43.

that the subpoenaed records did not constitute the defendant's private papers because the bank already voluntarily conveyed the records to various banks and employees in the ordinary course of business.[87] Thus, the *Miller* case clearly restricts an individual's right to financial privacy.

Without a digital cash statute, the courts will adhere to the limitations set by legal precedent.[88] This reliance on the past leaves the present digital cash user without guarantees of financial privacy protection.[89] Thus, both current legislation and legal precedent fail to adequately address the privacy concerns raised by the Internet and digital cash.

III. ANALYSIS

The move to a "cashless society"[90] stretches the parameters of current legislation and legal precedent regarding the right of financial privacy. As a result, the issue of financial privacy on the Internet has reached the forefront of legal debate.[91] While detecting criminal activity on the Internet requires the identification of the digital cash user in some capacity, privacy laws must protect an individual's right to privacy while making financial transactions over the Internet.[92] Without such protection, a third party could easily follow a user's every move, create a personal profile for commercial use or learn the intimate details of a person's everyday life, all by tracing his financial transactions conducted over the Internet.[93]

Congress must enact a new federal statute[94] to balance the competing interests raised by digital cash. With uniform guidelines, digital cash users conducting business in the "virtual economy"[95] will face con-

87. *Id.*

88. *See California Bankers*, 416 U.S. at 21 (rejecting constitutional challenges to the Bank Secrecy Act); *Miller*, 425 U.S. at 435 (concluding that an individual had no legitimate expectation of privacy in bank records).

89. *Miller*, 425 U.S. at 435.

90. *See Electronic Money*, *supra* note 2, at 21 (explaining a future without the use of paper cash).

91. *See* Wittes, *supra* note 8, at 1 (discussing the privacy concerns presented by the creation and use of digital cash).

92. Graham, *supra* note 7, at 12 (explaining how the government uses personal information to develop personality profiles of individuals which include, among numerous other data, the spending patterns, lifestyle and other personal choices of the individual).

93. Graham, *supra* note 7, at 12.

94. Article I, § 8 of the Constitution grants Congress the power to regulate commerce among the states: "The Congress shall have Power . . . . To regulate Commerce with foreign Nations, and among several States, and with Indian Tribes . . . ." U.S. CONST. art. 1, § 8. The commerce clause was designed to promote the economic welfare of citizens throughout the country. United States v. Darby, 312 U.S. 100 (1941).

95. *Electronic Money, supra* note 2.

sistent laws, regardless of the borderless nature of the Internet.[96] Furthermore, users will spend e-cash over the Internet with the same level of freedom and anonymity as paper cash, without the "physically cumbersome, difficult to transport and easy to steal" problems inherent in paper cash.[97]

A. The Difficulty with the Internet's Regulatory Structure

Part of the thrill of the Internet stems from its infinite potential and relaxed regulatory structure.[98] The Internet has expanded into a global community with its own moral attitudes, standards of conduct and methods of discipline.[99] To a large extent, the users themselves set the norms by establishing a level of civility, an appropriateness for disclosures of various kinds and a limited tolerance for advertising on the Internet.[100] Yet users face increasing difficulty in their ability to self-regulate as the Internet moves into the world of commerce.[101]

The introduction of digital cash threatens the success of the Internet's relaxed regulatory structure.[102] A system that fails to guard

---

96. *Electronic Money*, *supra* note 2.

97. "Existing paper money, to be sure, is inconvenient (physically cumbersome, difficult to transport and process, easy to steal) and it has been steadily losing 'market share' to other payment systems (checks, credit cards, electronic funds transfer) that seem better suited to the needs of the modern world of electronic commerce." *Plugging In – E-cash: Can't Live With It, Can't Live Without It*, Am. Law., Mar. 1995, at 116. "[S]horn of these disadvantages, cash is pretty wonderful stuff: portable, instantly recognizable, instantly accepted by everyone without any of the overhead associated with the other payment systems, and entirely anonymous. Any form of cash that can retain these features and be utilized in the world of electronic commerce is going to prove extremely attractive." *Id.*

98. The Internet ignites technological developments because the relaxed regulatory structure encourages experimentation. Companies capitalize on the Internet's unique functions. One company, for instance, designed a concert ticket purchasing center, where users select their preferred concert tickets after viewing an auditorium seating chart. *First Union and Open Market Join Forces to Create a Virtual Community on the Internet*, Bus. Wire, Mar. 15, 1995, at 1.

99. *Id.* "In the eyes of its members, the Internet is not so much a commodity as it is a shared resource, to be husbanded and maintained for the common good. It is a global community with its own values, its own standards of conduct and its own ways of disciplining the wayward." *Id.*

100. *Id.*

101. Laura Smith, *Internet 'Nowhere Near' Ready for Big Business: Many Still Concerned Over the Security of Online Financial Transactions*, PCWeek, Nov. 24, 1994 (describing the legal problems, such as security obstacles, presented by digital cash).

102. According to journalist David Post:

> The Internet today looks a lot like the Wild West: Dazzling, thrilling to ride through, unlimited in potential—but fundamentally lawless . . . . For many people . . . that is one of the Internet's peculiar charms. But lawlessness does have its drawbacks. Travelers on the Internet are a bit like travelers on a stagecoach through the Dakota territory; their property may be subject at any time without their consent.

against unauthorized intrusions into a user's financial information jeopardizes the individual's privacy.[103] Society's inevitable evolution from paper money to digital cash requires Congress to enter cyberspace in order to protect these privacy concerns.

B. Privacy Concerns, Security Interests & Insufficient Federal Legislation

1. *The Privacy Concerns of the User*

Current federal legislation[104] does not directly address the privacy and security threats inherent in digital cash systems. Without adequate privacy protections, transactions conducted on the Internet will become vulnerable to detailed, step-by-step examination and use by third parties.[105] These open transactions allow the government a strong involvement in personal matters and allow businesses a method for compiling detailed personal profiles based on a user's spending patterns.[106] Even more troubling, these open transactions allow thieves unauthorized access to a user's account.[107] A thief may transfer funds into another account, make unauthorized purchases or even obtain money from others while posing as the true user.[108]

2. *The Security Interests of Law Enforcement Agencies*

Privacy concerns also create security obstacles for law enforcement.[109] The same anonymity that protects a legitimate user's identity

---

David Post, *Encryption—It's Not Just for Spies Anymore*, Am. Law., Dec., 1994, at 106.

103. *Id.*

104. The Privacy Act, 5 U.S.C.A. § 552(a); RFPA, 12 U.S.C.A. § 3401; ECPA, 18 U.S.C.A. § 2510.

105. Benjamin Wittes, *The Dark Side of Digital Cash*, Legal Times, Jan., 30, 1995, at 1 (explaining the privacy dangers stemming from the documentation of digital cash transactions).

106. "Privately owned computers hold vast quantities of information concerning our personal lives . . . , [such as] where, when, and with whom we travel, how much money we make, what we buy, our health, and our marital status . . . . Sophisticated programming techniques enable companies to discover an individual's attitudes, values, interests, and opinions." Graham, *supra* note 7, at 1401.

107. Benjamin Wright, The Law of Electronic Commerce 37-43 (1991). On-line computerized databanks may hold many personal details accompanying a transaction. *Id.* A third party can use these details to form a concrete picture of an individual's person life and character. *Id.* Computer systems, centralized and easy to access, increase the opportunity for such threats to the safety and security of the information. *Id.*

108. Wittes, *supra* note 105, at 1.

109. Wittes, *supra* note 105, at 9. The government, specifically law enforcement officials, must have access to financial transactions in order to conduct successful money-laundering, drug-trafficking and anti-terrorism investigations. *Id.*

likewise masks a criminal's identity,[110] erecting additional obstacles for law enforcement officials to overcome in their quest to combat criminal activity.[111] Furthermore, unlike paper bills, which have distinctive marks and often pass between individuals in person, digital cash travels the Internet unbranded and faceless.[112] As a result, any new legislation must allow the government to learn a user's identity in certain limited situations.

3. *Insufficient Legislation*

Current federal legislation does not directly address the privacy and security threats presented by digital cash. The Privacy Act,[113] the RFPA,[114] and the ECPA[115] all cater to the privacy needs of the past. Current technological advancements, like digital cash, call for updated and comprehensive federal statutes.

The Privacy Act of 1974[116] fails to protect the digital cash user's financial privacy. The Act's main limitations stem from the fact that it only applies to data banks held by federal agencies and focuses on intrusions made by the federal government.[117] Thus, the Act does not sufficiently guard against third parties, such as businesses and computer hackers, accessing a user's identity, financial status and record of spending patterns.[118] Moreover, due to the fleeting nature of transactions over the Internet, third parties are not limited to records stored in the bank's database.[119] Rather, they can access the user's financial information as it passes over the Internet from the bank to the user or from the user to the merchant.[120]

The RFPA[121] faces similar obstacles. The RFPA does not sufficiently guard against intrusion by third parties such as businesses and

110. "Particularly worrisome to law enforcement is the prospect of large quantities of cash being moved around the Internet — where identities are easy to conceal, communications are instantaneous, and international borders are meaningless." Wittes, *supra* note 105, at 9.

111. Wittes, *supra* note 105, at 9.

112. Wittes, *supra* note 105, at 9.

113. The Privacy Act, 5 U.S.C. § 552(a).

114. 12 U.S.C. § 3404.

115. 18 U.S.C. § 2510.

116. The Privacy Act, 5 U.S.C. § 552(a).

117. *Id.*

118. *Id.*

119. *Id.*

120. *See supra* notes 24-31 (illustrating how digital cash travels over the Internet permitting third party intrusions).

121. 12 U.S.C. § 3404.

computer hackers.[122] In addition, the RFPA offers only limited protection against intrusion by the government.[123] For example, if the government suspects a person of using the Internet to launder money, it merely needs to claim that the user's records are relevant to a "legitimate law enforcement inquiry"[124] in order to force the bank to disclose the user's records.

In order to prevent disclosure, the party must rely on the Act's blocking procedures.[125] These procedures do not stop the bank's production of records long enough to test the government's access claim.[126] Implementing a higher standard, such as probable cause,[127] would offer the user more protection because the government would have to show a substantial connection between the funds and the criminal activity in all circumstances.

Of the current legislative choices, the ECPA[128] offers the most protection to a digital cash user. It extends protection to stored or transmitted information and regulates the access of federal agencies.[129] However, the ECPA only protects financial communications to a limited extent,[130] as it applies only to interceptions of financial transfers "through the use of any electronic, mechanical or other device."[131] Thus,

122. Suburban Trust Co. v. Waller, 408 A.2d 758 (1979). An individual does have some basic expectation of privacy. *Id.* For instance, a bank depositor has a right to expect that the bank will, to the extent permitted by law, treat as confidential all information regarding his account and any transactions related to that account. *Id.* Absent compulsion by law, a bank may not make any disclosures concerning a depositor's account without express or implied consent of the depositor. *Id.*

123. Waye v. Commonwealth Bank, 846 F. Supp. 321, 325 (M.D. Pa. 1994). A federally chartered bank did not violate the RFPA when it reported to federal authorities that customers were guilty of conducting check-kiting schemes, rather than merely reporting its suspicion that a customer was involved in such scheme. *Id.* The court held that bank acted consistently with federal law in reporting the customers' acts to federal authorities, and failure to preface report of such activities the word "suspected" gave rise to no cause of action. *Id.*

124. *See supra* note 60 for a definition of "law enforcement inquiry."

125. *See supra* notes 55-61 and accompanying text for an explanation of how the government can access an individual's financial records under the RFPA and the consumer can, although often met with procedural obstacles, attempt to block such access.

126. *See supra* notes 55-61.

127. Probable cause is the constitutional standard for the determination of sufficiency of the justification for an arrest or search. The Supreme Court in *Beck v. Ohio*, 379 U.S. 89 (1964), defined probable cause regarding arrest in the following manner: "[W]hether at that moment the facts and circumstances within [the law enforcement official's] knowledge and of which they had reasonably trustworthy information were sufficient to warrant a prudent man in believing that the petitioner had committed or was committing an offense."

128. Pub. L. No. 99-508.

129. *Id.*

130. 18 U.S.C. §2511(1)(b).

131. *Id.*

if a third party first obtained the user's identity directly from a bank, then the ECPA would not cover the intrusion. Therefore, the ECPA's scope would not successfully protect the digital cash user's financial privacy rights over the Internet.

C. The Limitations of the Supreme Court's Decisions

The Supreme Court's tendency to limit the scope of an individual's financial privacy is indicative of its position towards financial privacy on the Internet.[132] The decisions in *Schultz*[133] and *Miller*[134] deny individuals the financial privacy protection implicitly guaranteed in the Constitution.[135]

The *Schultz* Court closed the avenues for obtaining constitutional protection of financial privacy[136] by rejecting arguments based on the Fourth,[137] Fifth[138] and First Amendments.[139] Likewise, *Miller* limited the individual's financial privacy protections by establishing that a customer has no standing to contest disclosure of his bank records.[140] Some states responded to these decisions by formulating rights based on their state constitutions, while other states declined to assert a higher constitutional standard than *Miller*.[141]

---

132. *See supra* notes 75 and 76 citing cases limiting an individual's financial privacy.

133. *California Bankers*, 416 U.S. at 21.

134. *Miller*, 425 U.S. at 435.

135. *See Roe*, 410 U.S. at 113 (finding that a right to privacy exists as to the choice to terminate a pregnancy); *Griswold*, 381 U.S. at 479 (holding married couples' choice to use contraception as within the scope of the right to privacy).

136. *Schultz*, 416 U.S. at 1513-5.

137. U.S. Const. amend. IV.

138. The Fifth Amendment provides that no person shall "be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation." U.S. Const. amend V.

139. The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people to assemble, and to petition the Government for a redress of grievances." U.S. Const. amend I.

140. *See* Shattuck, *supra* note 38 for an explanation of the diminishing right of privacy due to rapid technological advancements. Many fear that due to the government's ability to so easily obtain an individual's information, George Orwell's fictional depiction of the world in his novel 1984 has become reality in 1990s:

> There was of course no way knowing whether you were being watched at any given moment . . . . It was even conceivable that they watched everybody all the time. But at any rate they could plug into your wire whenever they wanted to. You had to live—did live, from the habit that became instinct—in the assumption that every sound you made was overheard, and except in darkness, every movement scrutinized.

Id. at 991 (quoting George Orwell, 1984 6-7 (1949)).

141. The State of California's highest court, for instance, found privacy protection for individuals in Article I, Section 13 of the California constitution. This section almost mirrors the pertinent language of the Fourth Amendment of the United States Constitution,

Thus, courts have no consistent standard with which to approach the legal problems associated with digital cash. As a result, courts encountering this issue will most likely not provide relief for aggrieved users of digital cash.

IV. PROPOSAL AND THE DIGITAL CASH STATUTE: A CHECKLIST

A. PROPOSAL

Because cyberspace transcends state borders, Congress must enact a new statute in order to provide users with guidance and uniformity. At a minimum, a new federal statute should directly address the use of digital cash. It should also balance a digital cash user's privacy concerns with law enforcement's legitimate security interests. However, the success of the Internet as a global economy hinges on the digital cash user's confidence in the anonymity of his financial transactions. Thus, any new statute should focus on the assurance of privacy as a prevailing priority.

The user's identity serves as the key to unlocking detailed financial information. This information should remain personal and confidential. Therefore, at a minimum, a new federal statute should safeguard a user's identity by endorsing anonymity through encryption methods. However, in order for law enforcement officials to combat criminal activity on the Internet, a statute should permit the government to access the user's identity under certain limited circumstances.

A viable federal statute should raise the standard for government access during investigation from *relevant legitimate law enforcement in-*

---

providing that "[t]he right of the people to be secure in their persons, houses, papers and effects against unreasonable seizures and searches may not be violated . . . ." CAL. CONST. art. 1, § 13.

In *Burrows v. Superior Court*, 529 P.2d 590 (Cal. 1974), the court held that under Article 1, Section 13 of the California constitution, an accused individual has a reasonable expectation of privacy in his bank records. *Id.* at 243 n.2. Furthermore, the court found that the bank's voluntary disclosure at the informal request of law enforcement officials did not constitute a valid consent by the accused. *Id.* at 245. Therefore, these actions resulted in illegal search and seizure. *Id.* The California Court of Appeals later applied the same reasoning to documents obtained by defective subpoena procedures. *See* Carlson v. Superior Court, 58 Cal. App. 3d 13 (Cal. Ct. App. 1976) (holding that an accused individual has a reasonable expectation of privacy in his bank records).

Therefore, California law provides higher privacy protection to its citizens than federal law. The California courts hold that an individual has a legitimate expectation of privacy that exists as to bank records and that subpoenas fall within the constitutional protections against unreasonable search and seizures. However, some states follow the limitations placed on financial privacy as established in *Schultz* and *Miller*. In *State v. McCray*, 551 P.2d 1376, 1381 (Wash. Ct. App. 1976), the appellate court held that a police phone call to a bank in order to find out the status of defendant's bank account did not violate his constitutional right of privacy. *Id.*

quiry to *probable cause* in *all* circumstances. This provision would require the government to show a substantial connection between the funds and the illegal activity in order to search a person's financial transactions. As a result, the burden would rest on the government to gain evidence from other sources in order to build the probable cause necessary to access an individual's records. This standard better protects the user's privacy rights while also allowing the government to curb criminal activity on the Internet.

Furthermore, an optimal federal statute must also provide provisions that block access by businesses, interest groups and others. A third party should not have access to the user's identity and records unless the user provides written, verified consent. The statute should also determine the access right of the Internal Revenue Service. Moreover, the statute should outline strict sanctions against parties, such as computer hackers, who obtain the digital cash user's identity by illicitly intercepting the transmission of digital cash over the Internet.

B. The Digital Cash Statute: A Checklist

In sum, a viable digital cash statute must:

- Directly address digital cash
- Focus on individual privacy as the prevailing priority
- Recognize law enforcement's legitimate security interests
- Endorse anonymity through encryption methods
- Raise the government's standard for access during investigation from relevant legitimate legal inquiry to probable cause
- Block access by third parties, such as businesses and interest groups
- Define the accessibility rights of the Internal Revenue Service
- Include strict sanctions against unauthorized intrusion by computer hackers

V. CONCLUSION

Conducting business over the Internet entices people because of its efficiency, convenience and technological edge. Yet, even with all of the riches of digital cash, users will not fully embrace this new currency if it means sacrificing the treasures of privacy. In a day and age when the government, business and even thieves invade every aspect of our lives, people want and need privacy.

Anonymity over the Internet masks users from the outside world, giving them the same freedom and ease to spend digital cash as found in paper money. Breaking through that anonymity would allow others to access our financial records and become privy to the intimacies of our daily lives. However, complete anonymity also stifles the law enforcement's ability to curb criminal activity on the Internet.

Congress must enact a statute that effectively harmonizes these prevailing concerns. The statute should place the protection of individual privacy as its highest priority. Without such legislation, the Internet may never realize its full potential.

CATHERINE M. DOWNEY