Fordham International Law Journal

Volume 22, *Issue* 5 1998 *Article* 1

Does the EC Council Directive No. 95/46/EC Mandate the Use of Anonymous Digital Currency?

Julia Alpert Gladstone*

*

Does the EC Council Directive No. 95/46/EC Mandate the Use of Anonymous Digital Currency?

Julia Alpert Gladstone

Abstract

This Essay focuses on the relationship between the privacy and the retail payment systems on the Internet. Part I of this Essay reviews several payment mechanisms that are in use or that have been introduced for retail commerce on the Internet. The description is not intended to offer a thorough study of the technology, but rather to highlight the data trail that is created under each method. Part II reviews the relevant statutory and self-regulatory mechanisms that have been applied to the Internet to ensure privacy. This leads to a discussion of the European Community's data protection directive, Council Directive No. 95/46/EC ("EC Directive"). The EC Directive became effective in October 1998, and its impact on the Internet is still uncertain, although the global community is certainly taking it seriously. Part III begins with an analysis of the EC Directive, followed by the proposal that the EC Directive may influence the direction of the development of electronic currency towards an anonymous or un traceable product. This is a controversial proposal on an interpretative level because of the national security and monetary concerns of governments throughout the world. We have just begun our journey into the "information age," and the conclusion of this Essay suggests that thoughtful legal responses to technological changes are needed.

ESSAYS

DOES THE EC COUNCIL DIRECTIVE NO. 95/46/EC MANDATE THE USE OF ANONYMOUS DIGITAL CURRENCY?

*Julia Alpert Gladstone**

INTRODUCTION

As we approach a new millenium, it is appropriate to reflect upon the social environment in which we live. Advancements in telecommunications technology continue to impact dramatically the way that we conduct our personal, social, and business lives. Use of the Internet as a medium through which to transact business has established an electronic commerce industry that generated US$73.9 billion in 1998 and that is projected to grow to US$717 billion by 2001.[1] As these technological and economic achievements have evolved, the fundamental basic right to privacy of the participants has been compromised.[2] This situation is a result of both the unregulated nature of the Internet and the sophistication of the technology that supports the infrastructure.

Telecommunications technology has exposed our private lives on several levels. This Essay focuses on the relationship between the privacy and the retail payment systems on the Internet. Digitization of information has begun to change the music, software, and film industry, but arguably the greatest change is being experienced in the area of generic information trans-

* Julia Alpert Gladstone is a Professor of Legal Studies at Bryant College in Smithfield, Rhode Island. She is Chairperson of the American Bar Association's Committee of the Law of Commerce in Cyberspace. Prior articles by the author that address legal developments in cyberspace have appeared in various law reviews and business journals.

1. This data was collected by Activ Media in their fifth annual study of web-generated revenues. *See E-commerce Revenues to Leap over $1.2 Trillion by 2002* (visited June 27, 1999) <http://sellitonthweb.com/ezine/news0043.shtml> (on file with the *Fordham International Law Journal*).

2. CONSUMER ELECTRONIC PAYMENTS TASK FORCE, THE REPORT OF THE CONSUMER ELECTRONIC PAYMENTS TASK FORCE (Apr. 1998) [hereinafter CONSUMER ELECTRONIC PAYMENTS] (addressing consumer concerns raised by emerging electronic money technologies); Mark E. Brudnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate*, 49 S.C. L. REV. 847 (1998).

fer.[3] Consumers will pay for information according the benefit or value received, and this economic behavior will define the "information age" of the twenty-first century.

While the volume of electronic commerce continues to increase, there is consensus among various industry experts[4] that the consumer's desire to keep her buying behavior anonymous, or at least unexposed, to unknown parties has tempered the growth of Internet commerce. Part I of this Essay reviews several payment mechanisms that are in use or that have been introduced for retail commerce on the Internet. The description is not intended to offer a thorough study of the technology, but rather to highlight the data trail that is created under each method. Part II reviews the relevant statutory and self-regulatory mechanisms that have been applied to the Internet to ensure privacy. This leads to a discussion of the European Community's data protection directive, Council Directive No. 95/46/EC ("EC Directive").[5] The EC Directive became effective in October 1998, and its impact on the Internet is still uncertain, although the global community is certainly taking it seriously. Part III begins with an analysis of the EC Directive, followed by the proposal that the EC Directive may influence the direction of the development of electronic currency towards an anonymous or untraceable product. This is a controversial proposal on an interpretative level because of the national security and monetary concerns of governments throughout the world. We have just begun our journey into the "information age," and the conclusion of this Essay suggests that thoughtful legal responses to technological changes are needed.

The infrastructure of open networks of computers connected to one another, also known as the Internet, allows the rapid creation, publication, and storage of information on an international basis. Virtual communities have evolved where in-

3. Interview with Russ Jones, Market Development Director at Millicent; *see* A. Michael Froomkin, *Regulation and Computing and Information Technology, Flood Control on the Information Ocean: Living with Anonymity, Digital Cash and Distributed Databases*, 15 J.L. & COM. 395 (1996) (discussing information commerce).

4. *See* CONSUMER ELECTRONIC PAYMENTS, *supra* note 2, at ii. In addition, a 1998 poll by *Business Week* magazine showed that 61% of those who do not use the Internet would do so if personal information were protected.

5. Council Directive No. 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 2(c), O.J L 281/31, at 38 (1995) [hereinafter Directive].

dividuals engage in business transactions or communicate about intimate personal matters. While the technological innovations that have lead to the development of "cyberspace" have improved people's lives, they have also challenged social and economic order.

I. *ELECTRONIC RETAIL PAYMENT OPTIONS*

A large number of individuals and businesses have chosen to conduct their commercial activities by electronic means. Spurred by convenience and efficiencies, the Internet is emerging as a shopping mall, not only for traditional physical products similar to catalogue shopping, but also significantly as a market for information that has developed on the Internet.[6] The Internet is a vast repository of information that may be viewed by anyone, almost anywhere in the world. In addition, contributions to the repository are being made by millions of people on a daily basis.[7] Since its inception in 1969 as a communications tool for academics and government officials, the Internet has transformed the nature, use, and value of information to society. As society places greater importance on information, an economic market for information is emerging. Free access to World Wide Web pages is being limited as information providers realize the economic worth of their product and obtain the technology to extract a fee for the material.

Commerce in information, and other digitally transferable products, has led to the development of a number of different digital means or medium to transfer units of value. There are essentially two general categories or models for the exchange of value on the Internet; they are the credit-debit card[8] and digital currency.

At the present time, credit cards are the most widely used method of payment for Internet products.[9] A credit card trans-

6. *See* Froomkin, *supra* note 3.

7. For a general discussion of the growth of electronic information available on the Internet, see Joel Rothstein Wolfson, Symposium, *Contract and the Copyright Are Not at War*, 87 CAL. L. REV. 79 (1999).

8. For a discussion of the relevant differences between debit and credit cards, see Froomkin, *supra* note 3, at 450 n.211.

9. Peter P. Swine, *Financial Privacy and the Theory of High-Tech Government Surveillance* (working paper) (visited Apr. 14, 1999) <http://www.acs.ohiostate.edu/units/law/swire1/hightech.htm> (on file with the *Fordham International Law Journal*).

action on the Internet requires that the customer either e-mail her credit card/personal identification details to the merchant or enter the credit card information onto the merchant's web page. In the later situation, which is becoming the preferred method, the information is automatically encrypted using either Netscape's Secure Socket Layer ("SSL") technology or the Secure Electronic Transaction ("SET") standard.[10] The credit card information then passes on the open Internet with little security risk of copying or interception by a nefarious third party. Credit card transactions are governed by Regulation E of the Electronic Fund Transfer Act[11] ("EFTA"), which further protects the consumer's interest by limiting her liability for misappropriation to US$50.[12]

The issues of consumer privacy when using a credit card for an online transaction are no different than in the physical world, and the relevant legal protections apply. The vendor/merchant maintains a record of the consumer's identity and product purchased; the credit card issuer maintains a record of all purchases of the credit card user. Consumers have accepted such data collection practices in the physical world where the average purchase is greater than ten dollars presumably by relying on the existing legal protections.[13] The Internet information market is much broader, more inclusive, and personally revealing. This trend suggests that the consumer may not want to create a credit card purchasing history of all the information that she receives off the Internet. In addition, the transaction costs of a credit card purchase may be prohibitive for the small microtransactions that characterize retrieving information from the Internet.

Several digital money schemes have been developed that facilitate electronic commerce for information products.[14] The

---

10. For a non-technical review of these technologies, see Wells Fargo, *Small Business Banking* (visited Apr. 15, 1999) <http://www.wellsfargo.com/biz/merchant/internet/secure> (on file with the *Fordham International Law Journal*).

11. 15 U.S.C. §§ 1601-1693r (1994 & Supp. 1997).

12. *Id.* For a thorough discussion of the application of Regulation E to digital currency, see VARTANIAN ET AL., 21ST CENTURY MONEY, BANKING AND COMMERCE ch. 4 (1998).

13. *See generally* Elizabeth de Grazia Blumenfeld, *Privacy Please: Will the Internet Industry Act to Protect Consumer Privacy Before the Government Steps In?*, 54 BUS. LAW. 349 (1998).

14. A precise definition of digital money is difficult to provide because it is an

technology of the various digital currency models can either create a complete audit trail that is more extensive than the credit card purchasing record or provide greater anonymity than cash.[15] All digital money protocols are actually a series of bits, or packets of information, which are initially purchased by the consumer for cash denominated in U.S. dollars, French francs, German Deutsche marks, etc. The bits are aggregated and distributed to the consumer's computer and referred to as "tokens" or "coins." Without cryptographic protections, these tokens could be easily intercepted at any point in the creation, transmission, or redemption process and used by a malevolent third party. Therefore, all digital currency protocols contain algorithms that act as locks on the information to provide security in the digital currency transaction. A system of keys that is unique to each digital currency protocol is used to decipher the algorithm or cryptographic locks.

The differences in privacy protection provided by the different digital currencies depend on the extent of information that each party in the digital currency transaction is allowed, or required by the protocol, to access. For example, imagine that A wishes to buy an item from B with digital currency. Under the basic digital currency model, A deposits one hundred dollars in Bank X, and Bank X issues a "token" or "coin," which is a series of bits identified by a long random serial number.[16] This "token" is on A's computer until she sends it to B in exchange for the item. B can then convert the "token" into cash at Bank X. The serial number on the "token" that was issued to A is unique; thus, Bank X now has a record of A's completed purchase. This form of digital currency has certain advantages over credit cards for small value purchases particularly if the item purchased is digital, but it offers no privacy advantage over credit cards.

On the opposite side of the privacy spectrum, there is the digital currency protocol developed by David Chaum, who founded Digicash Inc. The same basic "token" model is used where the bank issues "tokens" to A in exchange for cash. Un-

---

evolving product. For an excellent review of the breadth of the industry, see Group of Ten, *Electronic Money: A Report of the Working Party on Electronic Money* (visited Apr. 12, 1999) <http://www.bis.org/publ/index.htm> (on file with the *Fordham International Law Journal*).

15. CONSUMER ELECTRONIC PAYMENTS, *supra* note 2.

16. *See* Froomkin, *supra* note 3, at 52.

like the basic designated model, the serial number of the "token" is authored by A. Pursuant to a computer blinding process, the serial number designated by A remains unknown to the bank.[17] Thus, when the bank redeems the "token" transferred to it from A's merchant, it can verify its authenticity but cannot identify it with A.

The dissemination of the Digicash model of digital currency onto the Internet has been very limited.[18] Law enforcement agencies' concern that anonymous digital currency can be used easily for money laundering, which threatens national security on several fronts, indicates that certain legal prohibitions may be imposed on these products. David Chaum has obtained patents for the anonymous digital currency protocol, and while innovative work is still being done in this area, to date no other fully anonymous product has been brought to market.[19] David Chaum has thus far chosen not to license this patent, and Digicash filed for bankruptcy protection in 1998 with no digital currency in circulation.

There is a digital currency model that offers a middle level of privacy protection and has experienced limited success in several market trials.[20] Under this protocol, A purchases the digital currency referred to as a "scrip," which can easily be broken into smaller denominations. The "scrip" is cryptographically protected and purchased from a bank or broker. When A spends the digital currency, the broker records the merchant that is redeeming the "scrip," but not what is being sold. The merchant records what is sold and the serial number of the "scrip" for subsequent redemption, but nothing more. Therefore, without collusion between the merchant and the broker, consumer privacy is maintained and an audit trail is not readily or easily established.

---

17. For a technical explanation of this protocol, see David Chaum, *Achieving Electronic Privacy*, SCI. AM., Aug. 1992 (visited Apr. 13, 1999) <http://www.digicash.com/index_p.html> (on file with the *Fordham International Law Journal*).

18. *DigiCash Is Dead: Long Live DigiCash*, FIN. TIMES LIMITED, Nov. 16, 1998.

19. For a collection of the work of Stefan Brands, which deals with Internet cash systems, see *Work of Stefan Brands* (visited Apr. 13, 1999) <http://ganges.cs.tcd.ie/mepeirce/Project/Mlists/brands.html> (on file with the *Fordham International Law Journal*).

20. *See Find Out What's New, What's Hot and What's Happening with MilliCent* (visited Apr. 12, 1999) <http://www.millicent.digital.com> (on file with the *Fordham International Law Journal*).

II. *PRIVACY PROTECTION ON THE INTERNET*

The privacy abuse concerns of the Internet user stem from several areas. Personal information is obtained from users and consumers with the use of online registrations, user surveys, order forms, and affinity programs.[21] In addition to these overt methods, a computer technology commonly known as "cookies" allows a web site owner to collect information about a visitor without the user even knowing that her visit was recorded. This information may be obtained each time a user clicks her mouse to surf the Internet.[22] The threat to privacy increases substantially as the separate individual pieces of personal information are collected, categorized, catalogued, and even sold to third parties.[23]

The data gathering potential of certain digital currency models presents the greatest privacy intrusion of all because of the extent and amount of information that can be obtained. Most consumers are aware that a record of their financial transactions is maintained by the participating financial institution, but in a world where information is a highly valued commodity, the use of digital currency presents an alarming intrusion into one's daily life. In addition, it is likely that many of the laws that apply to the traditional data gathering activities of financial institutions may not apply to digital currency.

The U.S. Constitution does not establish a fundamental right to privacy; rather, any privacy protection is gleaned from a desperate handful of U.S. Supreme Court cases that recognize a privacy interest in certain intimate decisions.[24] Unlike the nations of Western Europe that have universal privacy protections, the current federal privacy legislation has evolved in a sectoral process.[25] The following section discusses several key statutes that have the potential to apply to digital currency but have not yet been so implemented.

---

21. *See* Swine, *supra* note 9.

22. A "cookie" refers to data files that allow the website owner to record the trail of sites that a person visited. *See generally* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998).

23. *See* Blumenfeld, *supra* note 13, at 355.

24. For an excellent examination of data protection and privacy law in the United States, see PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996).

25. *See generally* P. Amy Monahan, *Deconstructing Information Walls: The Impact of the European Data Directive on U.S. Business*, 29 L. & POL'Y INT'L BUS. 275 (1998).

EFTA and its consumer protection regulation, Regulation E, address the right of customers who establish accounts at financial institutions from which funds can be electronically transferred. The act has six major substantive requirements, which include obligations on financial institutions to disclose to the customer the terms and conditions affecting electronic fund transfers, the requirement to provide periodic account information, and most notably, a limitation on consumer liability for unauthorized transfers to US$50.[26] In the interest of consumer privacy, it would be desirable for similar requirements to be imposed on digital currency issuers. There has been much activity on administrative and congressional levels to adapt EFTA and Regulation E to digital currency payment products. In 1996, the Federal Reserve Board addressed the treatment of electronic financial products under Regulation E with its Stored Value Card Proposal ("SVC Proposal").[27] The SVC Proposal, which distinguishes stored value products based upon the architecture and function of the product, exempts low denomination value transfers from the requirements of Regulation E. It appears unlikely that digital currency schemes, which would facilitate information purchases over the Internet, will be subject to the rules of Regulation E.

The Fair Credit Reporting Act[28] ("FCRA") regulates the activities of consumer reporting agencies. It provides that a consumer report may be furnished only to a third party who has a permissible purpose for using the information. The list of prerequisites for obtaining a consumer report is based upon finding a legitimate business need.[29] Information sharing among affiliated companies is permissible, provided the consumer has been given the opportunity to opt out. Dissemination of raw transactional information between a consumer and an entity, which includes credit reporting agencies and others, is unrestricted. Raw data is distinguished from the formal "credit report" and given less protection. Given the sophisticated ways in which raw data can be organized, challenges to this distinction or exception may

26. 12 C.F.R. § 205.6(b) (1999).

27. *See* VARTANIAN ET AL., *supra* note 12, at 174.

28. Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681u (1994 & Supp. 1997).

29. For discussion of the provisions and operation of the Fair Credit Reporting Act, see Ronald C. Claiborne, *Credit Reports and the Fair Credit Reporting Act*, 28 J. MARSHALL L. REV. 365 (1995).

be forthcoming. It seems likely that the data collected by digital currency issuers would not fall within the definition of a "consumer report" and therefore the provisions of the FCRA would not protect digital currency users.

The Electronic Communications Protection Act of 1986[30] ("ECPA") protects persons against the unauthorized interception of electronic communication by the government and private sector firms. Electronic communications is broadly defined to include the transfer of signs, images, and sounds of any nature by wire, electromagnetic, or photoelectronic systems. The ECPA's Titles I and II address the treatment of electronic communications in transit and stored communications respectively. The act's prohibition against knowingly divulging the contents of a communication in transmission is more comprehensive than that for stored communications. The application of the ECPA to digital currency remains largely untested. It appears that finding protection will depend upon which point in the lifecycle of the electronic commerce transaction the interception or unauthorized access occurs.[31]

At the present time, digital currency payment systems are being designed for private industry implementation. Thus, it seems unlikely that laws limiting government access to information would directly impact the activities of digital currency issuers; a discussion of two of those laws follows. They are relevant, however, because of the protections that they can provide issuers from the government.

The Right to Financial Privacy Act of 1978[32] ("RFPA") is designed to limit the federal government's collection, and use, of customer records obtained from financial institutions. RFPA requires prior or concurrent consent of the individual even when the government agency uses its subpoena power to obtain the bank record. The term "financial institutions" includes banks, credit card issuers, credit unions, loan and trust companies, homestead, building and loan associations, or consumer finance institutions. The application of this law to digital currency issuers will depend on several factors, primarily, on

30. Electronic Communications Protection Act of 1986, §§ 2701-2711 (1994 & Supp. 1997).

31. *See* VARTANIAN ET AL., *supra* note 12, at 350.

32. Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (1994 & Supp. 1997).

whether issuers will be deemed to be "financial institutions" and whether the transaction account of the digital currency issuer falls within the definition of a "financial record."[33]

The Privacy Act of 1974[34] ("Privacy Act"), which was enacted in response to the privacy intrusions of the Watergate era, balances the individual's privacy interest against the government's need for individual information so that it can perform its public interest function. Only such financial records that are "relevant and necessary" to accomplish the federal agency's purpose may be collected.[35] Subsequent disclosure of the individual's information can only be made with the consent of the person to whom the information pertains. The Privacy Act provides for civil remedies against the federal government, but does not provide a right for consumers against private parties.

Privacy issues in cyberspace were brought to the public's attention when the Information Infrastructure Task Force ("IITF"), an interagency group formed by the Clinton Administration, issued its report *A Framework for Global Electronic Commerce* ("*Framework*").[36] The objective of the *Framework* was to provide direction, policy, and guidelines to advance the development of electronic commerce. The resounding message of the *Framework*, which had been previously circulated and approved by key Internet players, was for the government to adopt a laissez-faire approach to regulating the Internet and to allow the private sector to lead. The *Framework* addressed the economic potential of the Internet and endorsed its lack of a legal framework.

In the area of privacy, the *Framework* recommended that the government defer to the "private sector efforts now underway to implement, user friendly, self-regulatory privacy regimes."[37] Several self-regulatory initiatives have been formed to protect the overall privacy interests of individuals that use the Internet and engage in electronic commerce. The Individual Reference Services Group ("IRSG"), which is composed of database companies, has developed privacy principles that include restrictions on the availability of information, allowing consumers access to col-

33. *See* CONSUMER ELECTRONIC PAYMENTS, *supra* note 2, at 27.

34. Privacy Act of 1974, 5 U.S.C. § 552(a) (1994 & Supp. 1997).

35. 5 U.S.C. § 552(a)(e)(1).

36. PRESIDENT WILLIAM J. CLINTON & VICE PRESIDENT ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997).

37. *Id.*

lected information to ensure accuracy and certain opt-out provisions. Members of IRSG agree to be annually reviewed by an independent professional service to assess whether they are meeting the IRSG's principles.[38] While IRSG has established the most comprehensive voluntary platform in the information sector, the newly emerging digital currency issuers are not likely to view themselves as database companies, and they therefore would not be subject to the IRSG principles.

Founded in 1993, the SmartCard Forum organized representatives, primarily technology and financial services providers, to discuss the interoperability of various smart card protocols. They have developed their own set of privacy guidelines that encourage respect for the consumer's privacy expectations.[39] The principles limit the use, collection, and retention of customer information, offer opt-out provisions for customers who choose not to have personal data provided to third parties, and encourage third parties to use restraint with their use of information. Issuer's online digital currency payment products that do not employ a physical representation on a plastic card, however, may not be obligated to adhere to the SmartCard Forum's principles.

In September 1997, the American Bankers Association, the Bankers Roundtable, the Consumer Bankers Association, and the Independent Bankers Association of America joined together to adopt a common set of privacy guidelines that restrict the collection, use, and retention of individual customer information produced in a financial transaction. The guidelines establish procedures to ensure the accuracy of customer information, to limit employee access and third-party use of the information, and to provide opt-out opportunities for consumers.[40] Although the institutions that have adopted these banking industry principles are working on several implementation plans,

38. Federal Trade Commission, *Individual Reference Services: A Report to Congress* (Dec. 1997) (visited Apr. 12, 1999) <http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm> (on file with the *Fordham International Law Journal*).

39. *See* Legal & Public Policy Committee, Smart Card Forum, *Consumer Privacy and Smart Cards – A Challenge and an Opportunity* (visited Apr. 12, 1999) <http://www.smartcrd.com/news/policy/privdoc.htm> (on file with the *Fordham International Law Journal*).

40. *See* House Committee on Banking, U.S. House of Representatives (visited Apr. 12, 1999) <http://www.house.gov/banking/91897by2.htm> (on file with the *Fordham International Law Journal*).

the banking industry principles and the self-regulatory mechanisms in general have not been successful in protecting the Internet user's privacy.

The evidence suggests that the statutory and self-regulatory mechanisms designed to protect the transactional privacy of Internet users have not yet been successful. In March 1998, the Federal Trade Commission conducted "surfdays" to observe the data collection practices of many websites.[41] The Federal Trade Commission found that while fourteen percent of the sites had provided notice of their information gathering practices, nearly eighty-five percent of the websites surveyed collected personal information without giving such notice.

III. *EC DATA PRIVACY DIRECTIVE*

Unlike the United States, the Western European nations have treated privacy as a fundamental human right for decades and have provided for its protection not only in their enacted legislation, but also in their constitutions.[42] Data protection statutes directed at both public and private sector information processing have been enacted in most European countries. The transnational nature of data flows that are so integral to the phenomenon of the Internet has caused concern for the members of European Union. In 1980, the Organization for Economic Co-operation and Development ("OECD") issued guidelines to govern the privacy of transborder flows of personal data.[43] The United States was among the signatories to the guidelines, but they are not binding and the United States has not acted to enforce the provisions.

In 1995, citing advances in technology and market integration, the European Union created binding and enforceable legislation to provide international individual data protection. The EC Directive, titled in full, Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,[44] is binding on the member na-

41. *See* Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998) (visited Apr. 12, 1999) <http://www.ftc.gov/reports/privacy3/toc.htm> (on file with the *Fordham International Law Journal*).

42. *See* Monahan, *supra* note 25.

43. Organization for Economic Co-operation and Dev., Recommendation of the Council Governing the Protection of Privacy and Transborder Flows of Personal Data, Sept. 23, 1980, O.E.C.D. Doc. C(80)58 Final (1980), *reprinted in* 20 I.L.M. 422 (1981).

44. Directive, *supra* note 5, O.J. L 281/31 (1995).

tions, and each country must enact its own implementing legislation. The EC Directive took effect in October 1998 with the various nations meeting the EC Directive objectives independently.

Following a seventy-two point list of recitals, the EC Directive sets out its objectives, general rules, judicial sanctions, codes of conduct, supervisory authority, implementation measures, and conditions for transfer of data to third countries.[45] It is thorough in its approach to protecting the individual's right to privacy in personal information by harmonizing the data protection laws of its members and ensuring that the data protection survives transborder data flows to countries outside of the European Union.

The scope of the EC Directive is very broad, including the processing of all personal data. "Processing" is defined as "any operation or set of operations which is performed on personal data, whether or not by automatic means," and "personal data" is defined as "any information relating to an identified or identifiable natural person."[46] Article 6 of the EC Directive sets out the principles relating to data quality. It provides that personal data may be collected for specific, explicit, and legitimate purposes and not further processed.

The data controller, or "controller," which is defined as the natural or legal person that "determines the purposes and means of processing of personal data,"[47] must inform the data subject of the purpose for the personal information record and the information must be kept accurate and up-to-date. Data subjects are guaranteed access to review personal information, and they must be given the right to refuse to have their personal data transferred to a third party.

The most significant provisions of the EC Directive to individuals and businesses in the United States are provided in Chapter IV, Transfer of Personal Data to Third Countries. The EC Directive requires that any member that wishes to transfer data to a non-member country must provide an "adequate level of protection."[48] A workable definition of the standard of adequacy has not yet emerged in the European Union. There are

45. *Id.*

46. *Id.* art. 2(a)-(b), O.J. L 281/31, at 38 (1995).

47. *Id.* art. 2(d), O.J. L 281/31, at 38 (1995).

48. *Id.* art. 25(1), O.J. L 281/31, at 45 (1995).

exceptions to the prohibition against transferring information to third countries that lack adequate protection. Generally, they cover situations where the data subject has given his unambiguous consent to the transfer, the transfer is necessary for the performance or conclusion of a contract to which the data subject is a party, the transfer is necessary to protect the vital interests of the data subject, or the transfer is required for reasons of important public interest.[49]

Industry experts and legal scholars agree that the EC Directive has focused the world's attention on the need for privacy on the Internet. While Internet users in the United States have some protections against privacy abuse, historically Americans have not recognized that the processing of data itself may be wrongful[50] and can provide the basis for privacy violations. Electronic commerce is international, and a global response to the EC Directive is forthcoming. The U.S. and Japanese governments have made public their efforts to comply with the EC Directive.[51]

The majority of the literature in the United States that analyzes the EC Directive focuses on the provisions of Articles 25 and 26, which address the data transfer to third countries and the derogation from those restrictions.[52] Less attention has been given to Article 7, The Criteria for Making Data Processing Legitimate. It is helpful to see that the derogations in Article 26 follow the terms of Article 7, describing the methods for lawful data processing. For example, under Article 26, a transfer of personal data to a third country that lacks adequate levels of protection may take place on the condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

---

49. *Id.* art. 26, O.J. L 281/31, at 46 (1995).

50. *See* PETER P. SWINE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS ELECTRONIC COMMERCE AND THE EUROPEAN PRIVACY DIRECTIVE (1998).

51. Japan's Ministry of International Trade and Industry has established a new Japanese Industrial Standard JISQ1500 to create data private protection. According Michael Power, Assistant Director, Policy Treasury Board of Canada, Japan's regulations are in part in response to the EC Directive. The U.S. Department of Commerce has issued for comment *International Safe Harbor Privacy Principles*, which are designed to avoid a trade war with the European Union rising from the EC Directive.

52. *See, e.g.*, Patrick J. Murray, Comment, *The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?*, 21 FORDHAM INT'L L.J. 932 (1998); Monahan, *supra* note 25; SWINE & LITAN, *supra* note 50.

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.[53]

Article 7 states that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, expect where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).[54]

The characteristic of digital currency, which makes it useful for

53. Directive, *supra* note 5, art. 26, O.J. L 281/31, at 46 (1995).
54. *Id.* art. 7, O.J. L 281/31, at 40 (1995).

global electronic commerce, is that it crosses national borders unchanged. Digital currency is not the subject of any one sovereignty, and thus digital currency issuers would likely be subject to both Articles 7 and 25.

Digital currency issuers under any model, except the fully anonymous protocol, will be "processing personal data" as defined by the EC Directive even if it is by automatic means. The traditional transfer of personal information in a wire transfer or other international payment is generally permitted under the EC Directive because such information is needed to make the payment work. Under Article 7, the information can be processed because it is "necessary for the performance of a contract." Under Article 26, it may be transferred to a third country without adequate levels of protection because "it is necessary for the performance of a contract to which the data subject is a party." Similarly, processing of data by credit card issuers is permitted because it is a "necessary for the performance of a contract."

The previous discussion of alternative digital currency schemes demonstrates that collection of personal data is *not* necessary for a digital currency transaction to work. When a product is in the development stages, as is the case with digital currency, it is prudent to design the product to comply with the relevant laws. Therefore, if the mechanism or structure of digital currency does not require the processing of personal data, then designated digital currency, which creates a free flow of personal data, would be prohibited under Article 7 and would not fall within any of the derogations of Article 26. It would be logical for issuers of digital currency to endeavor to comply with the EC Directive. Consequently, it is likely that anonymous digital currency will emerge as the dominant player in the digital currency or electronic cash market.

In addition to the "necessary to the performance of a contract" allowance in both Articles 7 and 26, these articles also allow personal data to be processed or transferred to third countries that lack adequate protection if it is necessary for "compliance with a legal obligation" or if it is legally "required on important public interest grounds." Opponents of the anonymous digital currency model, which primarily include the national security agencies of governments, may suggest that the prevention of money laundering and other criminal activity justi-

fies the data collection of designated digital currency under these public interest provisions.[55] Current studies of the relationship between digital currencies and increases in money laundering are not conclusive.[56]

Finally, the terms of the EC Directive that allow the processing of personal data as long as the data subject gives his consent may weaken the argument that the EC Directive will drive the development of anonymous digital currency. Consumers with large "privacy premiums" may demand anonymous digital currency in which case they would not give their consent. This situation again suggests that the EC Directive and its implementing legislation will direct the development of digital currency towards products that ensure privacy.

CONCLUSION

The electronic commerce industry for information will continue to expand as economic success in society becomes more dependent upon having greater quantities and better quality information. The business of information dissemination will depend upon having an efficient means to transfer small value amounts or microtransactions. Digital currencies are uniquely designed to satisfy this demand and, thus, will eventually be commonplace on the Internet. As the "information age" evolves, consumers will continue to demand privacy protections. The concern for individual data privacy protection, which has been recognized by the implementation of the EC Directive, will likely influence the development of financial services and digital currency in particular. Privacy abuses can be eliminated by implemented technology solutions and will lead to the deployment of anonymous digital currencies.

---

55. The Financial Action Task Force ("FATF"), which includes 26 member countries, is the world's leading anti-money laundering authority. The FATF issued a paper on Money Laundering in 1996, which offered recommendations on how to stop money from freely traveling the globe, see United States Embassy, Isreal, *Financial Action Task Force Paper on Money Laundering* (visited June 9, 1999) <http://dns.usis-israel.org.il/publish/econews/1996/ecojuly/eco_701b.htm> (on file with the *Fordham International Law Journal*), and in April 1998, the FATF sought for further cooperation from the global community to stop money laundering, U.S. Information Service Israel, *Ministerial Meeting Statement on Money Laundering* (Apr. 29, 1998) (visited June 9, 1999) <http://www.usis-israel.org.il/publish/econews/1998/april/eco0429c.html> (on file with the *Fordham International Law Journal*).

56. Timothy Ehrlich, Note, *To Regulate or Not? Managing the Risks of E-Money and The Potential Application in Money Laundering Schemes*, 11 HARV. J.L. & TECH. 833 (1998).