DIGITAL CORRESPONDENCE: RECREATING PRIVACY PARADIGMS

Maria Helena Barrera & Jason Montague Okai[1]

> "Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court… Can it be that the Constitution affords no protection against such invasions of individual security?" [2]

INTRODUCTION

To be in cyberspace is to be recorded. Digital activities and objects are nothing but an ensemble of traces and records. Each electronic action in cyberspace implies the creation of tread marks; digitalization involves the generation of representations, more or less permanent. Those digital footprints can be, by nature, reconstituted, recreated and saved indefinitely. Where a vast number of activities in traditional space are inherently non-traceable, cyberspace actions are the traces themselves.

The prophetic scenario conceived of by Justice Brandeis in *Olmstead v. U.S.* have become a banal cyberspace reality. Theoretically an environment made of records, under non-orthodox control blueprints, is the perfect Orwellian space, a context where, in a technical point of view, privacy could not survive. That conclusion however must be vigorously tested against the value that democratic society attaches to privacy as a part of the concept of freedom.[3] In that light,

---

[1] Maria Helena Barrera, JD Central University, Ecuador. LL.M. Computer Law, Montpellier I University, France. LL.M. Industrial Property Law, Grenoble II University, France. LL.M. Intellectual Property, Franklin Pierce Law Center. Jason Montague Okai, JD Candidate, MIP Candidate, Franklin Pierce Law Center. The authors wish to express their gratitude to the following individuals for their support, understanding and patience: Professor Hugh Gibbons, Professor Richard Hesse, Cynthia Lewis, M.S.L.I.S., Ron Neary, Esq.

[2] *Olmstead v. U.S.* 277 U.S. 438, 473 (1928), Justice Brandeis, dissenting.

[3] *See* Alan F. Westin. Privacy and Freedom. Atheneum, 1966. At 24, "Just as social balance favoring disclosure and surveillance over privacy is a functional necessity for totalitarian systems, so a balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies."

privacy is a notion independent of the nature of the space where human activities are developed and unconstrained by the material tools involved in those activities.[4] Having freedom in mind, the question becomes if society could not afford to create a proper structure for privacy protection in a digital environment. If cyberspace is not an ideal setting of privacy, then it is necessary to transform it in order to preserve freedom.

The emergence of cyberspace has stretched privacy in personal digital communications to a breaking point. The laws attempting to contain it have outpaced the development and expansion of a global communication technology. The perception of the problem has become a digital paradox; the concept of privacy as an unwavering foundation of freedom seems to be at odds with the widely held view that cyberspace is the ultimate model of freedom for all people. The most critical communications privacy precepts suffer in cyberspace: The notion of correspondence inviolability seems to vanish when such correspondence is embedded in digital form.

Privacy in correspondence was perhaps the only kind of privacy protection regarded as absolute. Such perception consecrated in the Bill of Rights and established almost immediately by statute[5] seemed immutable. Inviolability of correspondence is an expression of the age-old assumption of privacy over sealed physical mail. Their bases precede legal tradition in both civil and common law systems. This assumption has apparently been shattered with the advent of electronic correspondence. E-mail is widely perceived as deserving little, if any privacy. Considered a marginal communication method, such denial has not been taken seriously. It is evident however that by challenging privacy over digital correspondence, what is in doubt is the very essence of the entire correspondence privacy paradigm. It is only a question of time, for the vulnerability of e-mail would be replicated in relation to physical mail by the advent of technological tools, and that would probably replicate the privacy vacuum.

The Fourth Amendment guarantees the right of people to be secure in their papers. That right is not limited by the place where those papers are,[6] or the method of access used to perceive its content.[7] The issue created by cyberspace is if that right is also independent of the tangible nature of the papers. In other words, whether an electronic document is or is not worth of the same privacy than a physical one, by the sole fact of its digital character. In a broader sense, it implies a need to reevaluate the underlying equilibrium between devices designated to provide privacy, and devices created to allow access, inspection and disclosure of its contents.

From the panorama outlined, it appears that is indispensable to rethink privacy in communications, and specifically, in correspondence. A juridical shift that could outpace the technological one must be achieved. The question is what is the appropriate path to accomplish such

---

[4] "For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." 389 U.S. 347, 351, 88 S.Ct. 507, 511

[5] Act of February 20, 1792, § 17, 1 Stat. 237.

[6] *Ex parte Jackson*, 96 U.S. 727, 6 Otto 727, 733, (U.S.N.Y. Oct Term 1877)

[7] *Katz v. U.S.*, 389 U.S. 347, 88 S.Ct. 507.

transformation. As Professor Lessig has stated, privacy paradigms were initially object of a translation when the necessity of adaptation of constitutional principles was raised by technological shifts.[8] Such translation however could have harmful results if its limits are broken.[9] Our objective in this article is: First, to apply translation to the structures of privacy in digital correspondence by identifying a common abstract pattern underlying its fundaments. This goal implies a search for points where to attach expectations of privacy in digital environments. Second, to go beyond translation and from the identification of the fundaments of message protection, to propose a paradigm independent of the nature of the communication tools, unconstrained by the eventual physical framework of a communications system.

The first part of this article will examine the reasons of the legislative and judicial confusion, in a pure policy translation approach. The second part will propose arguments in favor of a new paradigm for digital correspondence privacy issues.

I. Privacy beyond material bedrock

Since the creation of the postal paradigm there has been only a fragile material boundary between people's messages and the world, a sheath made first of clay, late of parchment or paper.[10] Its efficacy is obviously not physical but intangible and linked with social and legal values. Beyond the inherent weakness of such evolving barrier, the existence of envelopes implies a concrete manifestation of volition of privacy. The efficacy of frail containers is, in that light, directly proportional to the worth of its symbolism.

Society has recognized that beyond the physical limits of envelopes, a will for privacy exists and conveys respect. It has been an inherent mean of inviolability, the weakness of which never constituted source of doubts about the strength of its implication. That barrier was complemented by another element where to locate privacy significance. The trust in the symbol represented by boundaries is adjoined to the trust presumed in regard of a public or private dedicated postal system, a structure recognizable, identifiable and within a clear legal structure.

Digital correspondence apparently lacks trace of both points where to ground the analysis of traditional privacy protection. There are no longer physical boundaries where recognition of

---

[8] Lawrence Lessig. Reading the Constitution in Cyberspace. 45 Emory L.J. 869, 871. Professor Lessig identify as translation the method used by Justice Brandeis in his dissenting opinion in *Olmstead*: "Brandeis first identifies values from the original Fourth Amendment, and then translated these values into the context of cyberspace. He read beyond the specific applications that the Framers had in mind, to find the meaning they intended to constitutionalize."

[9] Id. at 874. "Even the most careful translators must at some stage concede there is not enough left from the framing regime to guide anymore. Translation may well have its limits, and these limits will be of great, and I fear, of terrible significance for us today."

[10] Carl H. Scheele. A short history of the mail service. Smithsonian Institute Press. 1970. Envelopes of clay, were Assyrian, where "[t]he tablets -cushion shaped paths nearly 3 inches square – where enclosed in clay envelopes bearing addresses.", at 8.

concrete signals of privacy volition exists. Dedicated and unique postal systems by which their use could imply volition of privacy no longer exist. Digital messages are intangible messages, bounded by immaterial limits, conveyed by an amorphous conglomerate of privately controlled electronic paths.

The absence of a concrete barrier represented by material envelopes has been seen as justification for an absence of volition of privacy on e-mails. Although the non-existence of postal systems has not been recognized as equally disturbing, both have been an underlying source of trouble. The reason is simple: The non-conventional nature of e-mail has reopened discussion about the validity of old-age assumptions linking privacy to the message material bedrock. Without that bedrock, the question is reverted to what is the essence of privacy over messages.

Privacy over messages could be seen as the capacity to exclude others from the perception of a content. Taken in its literal meaning, that capacity is nothing but a right to maintain a specific content secret using personal resourcefulness, ingenious and/or force. Taken in a juridical point of view, such capacity is one not only recognized as valid by the law, but also supported by an ensemble of legally enforced conventions. Such conventions are expressed in the inviolability of frail tools of concealment, as envelopes, and the legal framework of its conveyors, postal services. Those conventions are the points where to ground privacy analysis.

As the first part of this paper shows, the discussion over e-mail privacy has not attained such levels of constructive abstraction. Disperse legal approaches have been incoherent because they imply basic, expeditious analogies, ignoring the characteristics of digital messages and its context of conveyance. The question have not been whether or not an intangible fence made of bits could be equivalent to paper envelopes, or whether non-orthodox patterns of transmission could be constituted in valid conveyors. The discussion has been concentrated on an endless search of identity with traditional mail. E-mail has been approached as some sort of amorphous clone of mail, not an emerging phenomenon but a poor simulacrum of established communications.

a) Testing analogies: Digital correspondence as a new communication archetype.

Bare analogy is not the way to shift an adequate transition for correspondence protection. Analogies stress the vast differences between electronic mail and traditional mail without creating the fundaments of an appropriate analysis. Identification under translation is a better instrument. It is not an end, but an instrument. Under analogy, the panorama presented could be interpreted as a fundament of denial of privacy, or creation of an attenuate version for electronic mail. Under translation approaches, the gap is a tool, the absence of similitude suggests other implications: E-mail is a unique communication archetype with specific, exceptional characteristics. The distinction between e-mail and traditional mail is one between paths of communication and not between different versions of the same communication way.

aa) Dissecting the analogy approach: Traditional mail in the Procrustean Bed

Since the advent of e-mail, the question of privacy has been subject to the nearest available analogy: physical mail. That analogy, natural and evident as it is, has dominated even unconsciously all normative efforts, especially those directed to determine what kind of digital content is worth of protection face to government intervention. When difficulties with this approach were made obvious, the telephonic conversation analogy surged, as complementary and/or substitutive of that of physical mail. Both analogies remain until today indispensable referents.

If similar analogy omnipresence is applied in other Information Age issues, its characteristics in the e-mail field are highly unusual. Generally, analogies have been used as a Procrustean Bed.[11] That point of view implies the necessity to treating e-mail as a traditional communication method,[12] without recognizing its uniqueness. An equivalent of material bedrock has franticly been searched; the absence of materiality has been used as proof of absence of protection fundament. This implies to doubt about the privacy of the message based on its tangible –or intangible- bedrock, not on the characteristics of the message itself.

Under the Procrustean approach, e-mail shall for example mach the characteristics of traditional mail, even if such perfect equivalence is nothing but a mirage, a denaturalization that prevents an adequate legal consideration. To demonstrate the consequences of this path, it is interesting to inverse the Procrustean Bed pattern, and to try to mach traditional mail into the e-mail configuration, to analyze traditional mail as if it was the perfect counterpart of e-mail.

The first characteristic of e-mail would be necessary to reproduce is its multiplicity. A digital message is not a unique document: Since its creation, it implies the existence of two or more duplicates. In order to fit that characteristic, physical mail should never be maintained in a single exemplar: a duplicate or multiple duplicates would exist always.

The multiplicity character has in itself the source of other phenomena, the ubiquity of e-mail. From the moment that the user hits the send key, there is not only multiple copies of the message, but those copies have been created in computer memories potentially all around the world. If physical mail could be disseminated in the same manner, from the moment that somebody put a letter in a mailbox there could be copies of it not only in possession of the postal service, but also in those of a potentially infinite number of individuals around the globe.

Digital possession is of course unrelated to physical possession. Each of the persons in possession of an electronic copy is potentially in the position to make duplicates of the elec-

---

[11] Professor Le Stanc in France has used the simile before concerning a digital age problem. He advocates for a non-orthodox approach to digital age issues, in order to preserve sanctioned structures of protection into the limits of rational analogies. See, Christian Le Stanc, La proprieté intellectuelle dans le lit de Procuste. Observations sur la proposition de loi du 30 juin 1992 relative à la protection des "créations réservées". Dalloz 1993, Cahier 4.

[12] *E.g.* Ian C. Ballon. The emerging law of the Internet. "What Mode of Communication Does Email Replace?" 507 PLI/Pat 1163, 1263

tronic message, and to disseminate it. If physical mail should fit this characteristic, the single exemplar could to be duplicable *ab infinitum* by an indeterminate number of people at the same time.

The duplicates issue is not exhausted however, until there is not analysis of the user perception in regard to some kinds of those copies. An average user could not even be aware of the temporary files created at the time of the message redaction. From the moment of sending, the different classes of duplicates that would be possibly generated become a speculation field, with some certainties. One of those certainties is the creation of backup files.

If physical mail should fit e-mail backup standards, then the post office would need and be authorized to keep a copy of each message handled in each point by where the message is transferred, including permanent official copies in the send and receipt points. The initial and the final copy, kept by the sender and the receiver, are in that light minimal appearance of the real volume of duplicates. Without forgetting that any receiver (authorized or not) at any time, could reinitiate the chain of duplicate creation, by copying or forwarding the message. And, the most bizarre corollary, by using computers other than personal equipment to access e-mail accounts, the user is creating local copies of each message accessed, not only in system backup files, but also in current browser and temporary files.[13]

In that panorama, there should be an underlying element to eliminate in the analysis: The notion of a unique, official, centralized controlled postal service. In cyberspace, there is nothing comparable to traditional postal services or even with private carriers. Each node, each server, each computer that is used as transport element in the net has a proportional responsibility in the handling and delivering of e-mail. Applying this characteristic to traditional mail would result in the effacement of any trace of postal service structure: Any person would be able and even expected to take part on the manipulation, control and delivering of postal objects.

Finally, is necessary to establish that the panorama traced includes only possible behavior that could be considered legitimate. Unlawful interventions such as non-authorized access, screening, interception, duplication, forgery, modification, effacement, etc, have not been take in account.

bb) The backup paradox: Dominion notions in cyberspace.

There are fields where analogy has not been used extensively, specifically referencing dominion concepts. E-mail, unlike traditional mail and phone, imply two phases where privacy issues emerge: First, the transmission and actual conveyance of the message in the cyberspace.

[13] Royal Van Horn. Electronic gadgets never forget. "Even those previous users who had properly signed off from their e-mail servers had failed to clear out all the other computer memory locations: the Web browser's "Go: Last" memory, the Web browser's bookmark memory, the computer's scrapbook memory, and so on. *The previous users had left the computer equivalent of a paper trail leading to everything they had just done.* It was a little scary and surrealistic. 26 WTR Hum. Rts. 26, 27 (emphasis added)

Second, the storage produced in successive phases from the creation to the reception of the e-mail, while the transmission is made. The complexity of the legal regulation of the late has for source its unusual characteristics that call doubts upon traditional notions of dominion in regard of messages.

The impossible existence of a centralized controlled postal service is not the only paradox proper to e-mail. Perhaps the more disturbing of its characteristics is a de facto dissolution of the traditional dominion rationale upon which privacy theories are linked in physical environments.[14] Although dominion does not necessarily imply authority, such a shift is unprecedented and important.[15] E-mail not only exists in naturally multiple copies, but as a ubiquitous document transmitted in an absolute heterogeneous private automatic system. It is a kind of communication that demands the intervention of private third parties in its management and control. E-mail transmission and storage imply the intervention of a service provider, and most precisely, a systems operator.

The very nature of the systems operator's job implies handling, manipulating and routing messages. This description seems to fit that of postal service employees, and it does so to a certain magnitude, because it excludes other characteristics completely unusual.[16] Beyond its manifest heterodox nature, a system operator has specific endowments: She can access and monitor, in a word control electronic messages, and keep backup copies of it and of its subsequent modifications and manipulations.[17] The broadness of its management activities does possess an express legal basis, but even a minimal analysis will confirm its existence.[18]

Where access to the content of messages is sometimes allowed to postal employees, such allowance is possible only under extraordinary circumstances. For systems operators, it could be a normal, daily necessity.[19] Monitoring is a more delicate matter, whose nearest analogy could be

---

[14] David J. Loundy. E-LAW 4: Computer information systems law and system operator liability. "Unlike the U.S. mail, electronic mail is almost always examinable by someone other than the sender and the receiver of the message." 21 Seattle U. L. Rev. 1075, 1080

[15] *See e.g.,* Daniel B. Yeager, Search, Seizure and the Positive Law: Expectations of Privacy outside the Fourth Amendment. 84 J. Crim. L. & Criminology 249, 304

[16] Internet providers and BBS have been analogized to broadcasters (Doe v. America Online, Inc., 25 Med. L. Rptr. 2112 (Fl. Cir. Ct. 1997)), publishers (Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 139 (S.D.N.Y. 1991)), bookstore owners (Stratton Oakmont, Inc. v. Prodigy Services Co., 23 Med. L. Rptr. 1794, 1796 (N.Y. Sup. Ct. 1995)). The analogy with postal service systems seems however not to have be exploited…

[17] *See* Barry Fraser. Rules of the road for navigating the information superhighway. "[Y]our e-mail message may be handled by several different online services during delivery. The sysop of each of these systems may view e-mail under the above exceptions to the ECPA. Additionally, the message may be intercepted if either the sender or recipient consents. So, *even if you do not consent yourself, the person you sent the e-mail to may have consented to the disclosure of the message.*" 26 WTR Hum. Rts. 17, 18 (emphasis added)

[18] *E.g.,* Nicole A. Wong. Responding to subpoenas: a Sysop's primer for protecting user privacy under the ECPA. 2 No. 10 GLCYLAW 3

[19] 26 Cap. U. L. Rev. 347, 352 "[R]eading the E-mail message may be a legitimate, and even necessary, function of a sysop monitoring the traffic load on the network to ensure proper functionality."

only found in real time communications as telephonic calls. Maintenance and management of backup copies are without doubt matters out of any analogy panorama, and as so alien have not be the object of attempts of a comprehensive normative.

Some scholars have stated that there is an identity between current e-mail and backup e-mail content.[20] Such identity does not exist. The two categories of stored information seem to be clearly distinct. In ordinary circumstances, for example, users can only access current content that they have not deleted from their account. Backup files include messages that were never opened by the user, or about the existence of what the user never was aware, as misaddress e-mails returned automatically. It also includes messages that have been voluntarily discarded from the current e-mail account, after having been opened or not. Those opened and deleted could be analogized to letters voluntary send to the trash, and therefore in a legal limbo. The question here is whether or not the voluntary discarding could be seen as a renouncement of privacy.

All backup content, including current messages voluntarily discarded are beyond access, impossible to reach by standard procedures covered by a user's password. Had a user sought to recover a copy of a deleted message, she must ask the Systems Operator for the inaccessible message that requires a time and money consuming procedure; backup files are out of user possession and control, commonly with the user contractual acquiescence. Such acquiescence could be formal, without any real knowledge of its implications. The Systems Operator had control and possession of the backup files.

If Systems Operators have possession over backup files, they also have responsibilities over the content, responsibilities that are determined by the society. Those responsibilities go beyond the mere technical area. In the first years of the information age, where no analogies could fit perfectly, society has placed a burden upon the persons that control electronic communication systems. That burden is one of diligence and alertness. This burden does not go to a virtual sovereignty over the contents of the e-mail, but up to a similar pattern that those created for private mail systems and private carriers. It is a subjective area, because for the moment, there is not a legal framework for it.

The subsequent question, what kind of privacy society could recognize as a reasonable undertaking over the content of backup files, has a very concrete outcome. What seems a rhetoric issue implies in reality a directly proportionality between the reasonable control that society recognize as the responsibility of the Systems Operator, and the natural limits that personal and social privacy values impose. There is however a nearly total absence of legal rules at that respect. Systems Operator and Internet Provider responsibilities and rights in regard to the privacy of e-mail users are open issues. How important are those issues will be analyzed later.

---

[20] *See e.g.*, Randolph S. Sergent, Note, A Fourth Amendment Model for Computer Networks and Data Privacy, 81 Va. L. Rev. 1181, 1226 (1995)

II. Digital correspondence privacy: Devising protection paradigms.

In order to create a coherent privacy norm for e-mail, translation must be performed and addressed to abstractions of where privacy is attached in communications, taking in account the differences in order to adapt the general principles to a new reality. The question is not how different is e-mail from traditional mail, but what are the legal substrates that make traditional mail, as other communications paths, worthy of privacy.

a) Privacy principles in cyberspace communications

What are the common attachments where to ground privacy protection, independently of communication methods? The only stable element is the message and its connotations. That implies apparently a search as to the content and context of the message, but such inquiry is too subjective for to be useful. What is necessary to the creation of a norm is to understand what external manifestations of volition of privacy must be found in regard of the message and of the medium. To this day the search for privacy norms has been directed to the physical way of manipulation and delivering; That search must be transformed in an examination of the intangible measures that assure the conveyance of the message only to its intended recipient, measures founded in legal basis.

A message sent without some kind of protection that prevents a general, non-restrictive communications has no ground upon which to attach expectations of privacy. Complementarily, even if the message is concealed in a steel case, there is clearly not ground where to attach a privacy expectation if it is confided to the first stranger passing by the street in order to be conveyed.

What is required in cyberspace is nothing less that unearthing a basic structure underlying the privacy of messages. First, this structure must define the existence of a message with has been provided with some kind of boundary, a capsule that protect it against general perception of the contents. Second, the message must be conveyed by a system socially recognized as a trusted carrier of messages. Boundaries and carriers are conventions supported in the existing law about privacy. Those concepts will provide a framework applicable to developing a privacy system for digital correspondence. Whether or not an effective attachment of privacy has taken effect is an issue that must be considered in each individual case. But a general framework must be determined before these cases move into the courts.

The question here is where to objectively establish the existence of such measures. Electronic mail has obliterated old-age perspectives. Mail has two physical elements to which attach a privacy scrutiny: The message *corpus mechanicum*, and the envelope. Without envelope, or equivalent form of boundary, privacy vanished, as for example with postcards. Electronic mail has no physical elements, there are not habitual, tangible barriers in which to built a privacy approach. The only standard restraint associated with e-mail is the password-protected mailbox. That implies that maybe for the first time in history, it is indispensable to scrutinize message

protection as the intangible phenomenon itself. An emerging process directed to absolute intangible elements.

b) Legal structures for old-age/digital questions.

From a limited, elitist communications path, electronic messages are evolving in prevalent standard. In due time, e-mail will not continue to be another alternative of interchange, but the basic and preferred way of communication.[21] Such standard cannot continue to carry a stigma of lack of privacy protection due to its non-orthodox nature.[22] If a general free exchange risk shall be avoided,[23] it is in the interest of society to assure a privacy paradigm for electronic messages, beyond its apparent vulnerability.

Congress has attempted to address digital correspondence issues without success. The Circuit Courts have failed to find a common ground for communications privacy in either the congressional enactments or in the technology itself. A possibly fruitful approach is to apply this dual principle create by the U.S. Supreme Court: "[F]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable.'"[24] What this rule means in physical space has been subject to controversy, and the rule by itself vastly criticized.[25] Its rationale is however compatible with a constitutive analysis of correspondence privacy.

The U.S. Supreme Court rule has two parts that seem to correspond with two basic message privacy elements. The exhibition of a subjective expectation of privacy implies a manifestation of privacy volition; individuals must make evident in some way a will of privacy. In regard to correspondence, that manifestation is the use of a boundary that protects the message from unrestricted knowledge. The subjective expectation must be also one that society recognizes, a manifestation that is objectively reasonable. It is objectively reasonable to expect privacy over

---

[21] C. Edward Good. An e-mail education. What You Don't Know About E-Mail Can, and Will, Hurt You

"By the year 2001, the number of Americans using e-mail will total 135 million, according to one estimate. The will send 500 million messages each day." 35-FEB Trial 28, 29

[22] Jeffrey H. Reiman.Driving to the panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future. "The very fact of general visibility - being see able more than being seen - - will be enough to produce effective social control. [FN4] Indeed, awareness of being visible makes people the agents of their own subjection." 11 Santa Clara Computer & High Tech. L.J. 27, 28

[23] Cyberights. Defending free speech in the digital age. Random House. 1998. "It's well understood that freedom of speech means the right to say almost anything you choose; it is less commonly recognized that freedom of speech also means freedom to choose *how* you communicate what you want to say." at 133.

[24] *Katz v. U.S.*, 389 U.S. 347, 361, 88 S.Ct. 507, 516 (Justice Harlan concurring).

[25] For a comprehensive list of critics, *see* Thomas K. Clancy. What does the Fourth Amendment protect: Property, privacy, or security? 33 Wake Forest L. Rev. 307, 369, Fn. 234.

encapsulated message conveyed by a private or public postal system; society has recognized it for centuries.

There has always existed means by which an individual could manifest their intent to retain privacy in a physical communication, even when these manifestations have always been admitted as inherent to the nature of the communications system being employed. That inherence must be abandoned, if the sound rule would be applied pertaining to technological advances. In order to apply the basic privacy framework implied in the Supreme Court benchmark to cyberspace, a level of abstraction is required. An abstraction that eradicates assumptions proper to pure physical systems of communication.

aa) Recreating symbolic boundaries: Envelope related solutions.

In order to neutralize e-mail vulnerability, methods have been suggested in attempt to create some kind of tangible digital boundaries. Those boundaries must have the characteristics of envelopes in physical mail: they would be signs of privacy volition, tools for encapsulation and memory devices. A digital plus is of course present: In a space made of records, the boundary represents the limits between private records and the environment.

One of the paths proposed for the creation of boundaries is an expansion of simple Internet instruments that would make users anonymous. This could make it possible for a total disjunction between the sender and the message, making further identification impossible. Other and perhaps the more admitted way advise cryptographic tools. The anonymity method requires the availability of an intermediary server containing a program that could manage to delete any identification information from the message. In that manner, a total dissection between the first set of stored copies of the message, those bearing traces of its origin, and the second set, without any source information, could be achieved. It recreates an envelope by sealing the content in a no-proprietary, unidentifiable appearance.

The weakness of this solution is dual. First, the remailer server is always source of limitation, as an intervention on its content could rebuilt the chain of identification, recreating the link between the two phases of the transmission. Second and most substantial, it is impossible to equalize in a legal point of view anonymity and privacy. If anonymity could be see as a part of the scope of privacy, to convert privacy in a mere anonymity issue is illogic and dangerous.

Encryption is apparently the better possible answer to electronic mail concerns. It allows anonymity and impenetrability or mere impenetrability of the content of the messages.[26] Beyond

[26] Joel C. Mandelman. Lest we walk into the well: Guarding the keys encrypting the constitution. To Speak, Search & Seize in Cyberspace.. "No one has a constitutionally protected right to send anonymous e-mail ... No one has asserted that these prohibitions are interfering with the free flow of political debate and there is no reason to think that limits on the use of a brand new technology, the past absence of which has not in any way inhibited the most vigorous debate of all issues in this country, will suddenly cause that debate to be stifled." 8 Alb. L.J. Sci. & Tech. 227

the endless debate about legal availability and use of cryptography,[27] there is a paradoxical danger. The obvious question, that encryption could nullify de facto any law enforcement intent,[28] is controversial but not relevant to the essential matter. In order to have a legitimate container, the method used could be weak, not strong cryptography, because for privacy purposes what matters is its existence, not its impenetrability.

The double-edge of cryptography resides in to attribute to encryption tools the role of only and supreme solution to privacy concerns. Advised as unique answer, cryptography is not only relative – there are new decrypt tools available almost each day, for free download in the Internet - but also a notably precarious, denaturalizing basis for privacy. By allowing encryption as universal indicator of privacy expectation, we are relinquishing our privacy to the bare efficacy of far-related simile of physical boundaries, a de facto poor substitute.

Privacy over messages is not directly proportional to the strength of its container. The presence of a container is important – it has been from the nineteenth century BC - as a symbolic manifestation of privacy volition. Is that manifestation what is fundamental, not the invulnerability of the envelope. A manifestation that is complemented by another necessary element: a safe postal environment conformed of a standard normative governing ISPs postal activity.

bb) ISP / System Operator normative: from postal service to postal environment.

Issues pertaining responsibilities and limits to ISP and System Operators activities have not been substantially addressed in the area of privacy.[29] How detrimental is this absence could be weighed by examining the consequences of the vacuum. In the lack of a clear normative, the nebulous limits that ISP and System Operators activities are used as a dual tool undermining privacy over electronic mail. First, it opens the door to a contractual delimitation of privacy for e-mail subscribers, broad or narrow as determined by each ISP. Second and most important, it inhibits the emergence of a structured and stable electronic postal environment.

When the user signs a contract for e-mail service, he is accepting a set of contractual dispositions that, in most of the cases, are very restrictive of privacy. In general, users are not aware of such limitations until a problem appears. How constitutional is such kind of renounce

---

[27] *See,* Daniel R. Rua. Comment: Cryptobabble: How Encryption Export Disputes Are Shaping Free Speech for the New Millennium . 24 N.C.J. Int'l Law & Com. Reg. 125. In a non-orthodox light, a valuable panorama about cryptography is offered by accessing the homepage of The CryptoRights Organization. "Security for Human Rights and human rights for Cryptographers." Available at http://www.cryptorights.org

[28] *Cf.* Robert Reilly. Mapping legal metaphors in cyberspace: Evolving the underlying paradigm. Citing Attorney General Janet Reno: "Encryption can frustrate completely our ability to lawfully search and seize evidence and to conduct electronic surveillance, two of the most effective tools that the law and the people of this country have given to law enforcement to do its work…" 16 J. Marshall J. Computer & Info. L. 579, 588

[29] The ECPA being an incidental legislation, not directed to clarify user privacy. The limits that it impose over System Operators could not be considered as a appropriate structure, neither in scope, nor in deepness.

to privacy is difficult to analyze, because of the non-settled main question of e-mail privacy protection.

As evidenced in this paper by the Procrustean inverse pattern, it could be impossible to create a structure remotely similar to a postal system in the cyberspace. That impossibility, however, must not be see as an insurmountable impediment to the creation of a reasonable commensurate, a configuration that we would like to call a safe and stable electronic postal environment. Such environment would permit the emergence of the sense of trust that prevails in physical mail private and public carriers. If there could not be a unique, centrally controlled entity, then the rules by which the heterogeneous multiple ISPs control nodes behave in regard of e-mail privacy need to be identical.

Although privacy policies have been created and adopted by ISPs,[30] such efforts have a disparity that could be seen as pernicious, because of the sense of mistrust that it create, and furthermore, lacking focus and strength in e-mail privacy areas. Even between the ISPs that charge for e-mail access (AOL, Prodigy, etc.), there are important incongruities in approaches. The situation in regard of free e-mail access providers (Yahoo, Hotbot, etc.) is far more ambiguous, the privacy allowed to users being notably limited after even a superficial analysis. It is important to stress that the voluntarily character of such limits are subject to sudden transformations. [31]

Discrepancies in ISPs privacy procedures make evident the necessity of a legitimate structure with a solid public policy background. The creation of a safe postal environment passes by the regulation of the actors in the field. That implies generation of reasonable and fair standard governing ISPs postal related activities, not only in regard of its own subscribers, but also respect to the e-mail traffic that is conveyed by its equipment.

III. Conclusion

The U.S. Supreme Court's holdings regarding determination of privacy volition is an appropriate pattern for correspondence privacy. [32] Privacy implies a will that, when mani-

---

[30] *E.g.*, AOL's Eight Principles of Privacy. Available at http://legal.web.aol.com/policy/aolpol/privpol.html (Visited May 1999).

[31] Jeremy Pomeroy Online anonymity can be illusory under current law, ISP policies. 4 No. 12 MMEDIAST 1. "In any event, whatever protections ISPs do offer by way of their "privacy policies" are typically subject to change. ISPs customarily reserve the right to revise their terms and conditions of use on notice to subscribers. Therefore, an unwary user relying on a certain level of protection might, if he or she wasn't paying attention, find that the intimate details he or she had purposely or inadvertently revealed about him or herself were suddenly available to third parties."

[32] *Minnesota v. Olson*, 495 U.S. 91, 95 (1990)

fested, society is prepared to recognize as legitimate. Construing the Court's holding in cyberspace implies a regard to two intangible elements: First, the use of a digital individual container for each message - an electronic equivalent of envelopes-, and, second, the creation of a safe electronic postal environment, essential complement of the container. Courts must find a common ground in traditional Fourth Amendment communications cases to build a legal framework that can adequately deal with advancing technologies, guarantying personal communications seclusion. That interpretation implies a notion of privacy not only independent of material bedrock, but also of the actual way of communication used. A pattern that could be transposed to new communication paradigms without inconvenience.

In order to assure privacy in messages, and particularly in digital messages, it is necessary to identify the points where to ground privacy analysis. A backdrop where to determine the existence of privacy interests through a case by case approach is indispensable. Of course these are conventions framed in the law in order to make obvious whether or not a person had a manifested volition of privacy with regard to a message. Such conventions are necessary as a reminder that privacy over correspondence could not be diminished merely because there is not more simple physical elements where to find it.

In the space made of HAL's chips, privacy is not a natural resource but a social choice. Whatever the communication system, the right of people to create a specific, restrictive interaction worth of privacy must not be diminished, because it is one of the fundaments of freedom in democracy. Respect of such right to restrictive communication is independent of technological bedrock, and therefore *absolute in itself*. It is possible and necessary to translate the principles that governs the manifestation of privacy expectations to cyberspace, in its dual structure: Digital boundaries and conveyance by a trusted carrier. A new legal paradigm must complement the translation, a paradigm that legitimate the inviolability of such boundaries, beyond its actual strength, and could assure a stable and secure postal environment.