subsequently, how tenuous a finding for legal liability for defamation can be. His Honour duplicates the defendant's contested statement by stating

> "*It is common experience that ugly people have satisfactory social lives – Boris Karloff is not known to have been a recluse...*"

He goes on to conclude

> "*if I have appeared to treat Mr Berkoff's claim with an unjudicial levity it is because I find it impossible to take seriously.*"

This is a serious contrast to Niall LJ's finding that the statements were

> "*capable of lowering his standing in the estimation of the public and of making him an object of ridicule*".

When the court cannot agree on the reaction to a statement, the subjectivity of meaning and variety of legitimate reactions to a text is demonstrated highlighting problems with the objective test.

CONCLUSION

Defamation law addresses the painful co-existence of freedom of speech and the "*interest all individuals have in safeguarding or vindicating their reputation*"[14]. Postmodern literary theory could make a valuable contribution to the law by encouraging claims to objectivity in meaning to be disregarded and the policy justification for erring on one side or the other to be made explicit. This would result in a clearer understanding of the uses of defamation law in society.

1 Andrew Kenyon, Media Law 2004: The Australian Plaintiff's Case, Melbourne University Course Material, 50.

2 Ibid.

3 See Terry Eagleton, *Literary Theory: An Introduction* (1983) 66.

4 *Sim v Strech* [1936] (Lord Atkin).

5 See Eric Barendt, 'What is the point of libel law?' (1999) 52 *Current Legal Problems* 110, 111-117.

6 *Sim v Strech* [1936] (Lord Atkin).

7 *Chakravarti v Advertiser Newspapers* [1998] (Kirby J).

8 *Bond Corp Holding v ABC* (1989) (Kirby J)

9 *Boyd v Mirror Newspapers* [1980] (Hunt J)

10 *Sim v Strech* (Lord Atkin)

11 See Lyrissa Barnett Lidsky, *Defamation, Reputation and the Myth of Community, Washington Law Review* (1996) 9.

12 See Ibid.

13 *Morgan v Lingen* (1863), *Yousoupoff v MGM* (1934).

14 Barendt, above n 5, 112.

University student Sarah Krasnostein received a Highly Commended Award in the 2004 CAMLA Essay Prize Competition.

Invasion of Electronic Communication Privacy

Yi-Jen Chen, highly commended in the 2004 CAMLA Essay Prize, considers the impacts of the recent decision of the United States Court of Appeals for the First Circuit in *United States of America v Branford C. Councilman*

With the rapid development of computer technology, individuals are becoming increasingly dependent on the Internet to communicate and conduct their every-day business activities. While the Internet has promoted greater access to public and private services, it has raised new concerns regarding personal privacy and security. Online users' communications, for example, may now be exposed to the wider public. Any person who has superior computer knowledge, or who employs particular software, could easily monitor other users' activities on the Internet. The legality of employers' and internet service providers ("**ISP**") monitoring online users' electronic communications, such as the use of electronic mail, instant messaging, forums and bulletin boars, has been discussed vigorously. On 29 June 2004, the ruling made by the United States Court of Appeals for the First Circuit in *United States of America v Branford C. Councilman*1 focused significant attention on the issue of electronic communication privacy. According to this decision, ISPs have the right to read and copy the inbound email of their clients.

THE COUNCILMAN DECISION

In the *Councilman* decision, the defendant was the Vice President of Interloc, Inc. ("**Interloc**"). Interloc is an ISP, which provides an online rare and out-of-print book listing service and email service for its clients. The defendant was accused of directing Interloc employees to write computer codes (procmail.rc or "the **promail**") to intercept and copy all incoming emails from Amazon.com before they were delivered to the clients. The employees were also instructed to read these emails to gain commercial advantage. The defendant's action allegedly violated sections 2511 (1)(a), (c) and 2511 (3)(a)2 of the *Electronic Communications Privacy Act* ("***Wiretap Act***"3). The violation included intentionally intercepting electronic communications, disclosing the contents of the intercepted communications, and causing a person to divulge the contents of the communications while in transmission to persons other than the addressee of the communication4.

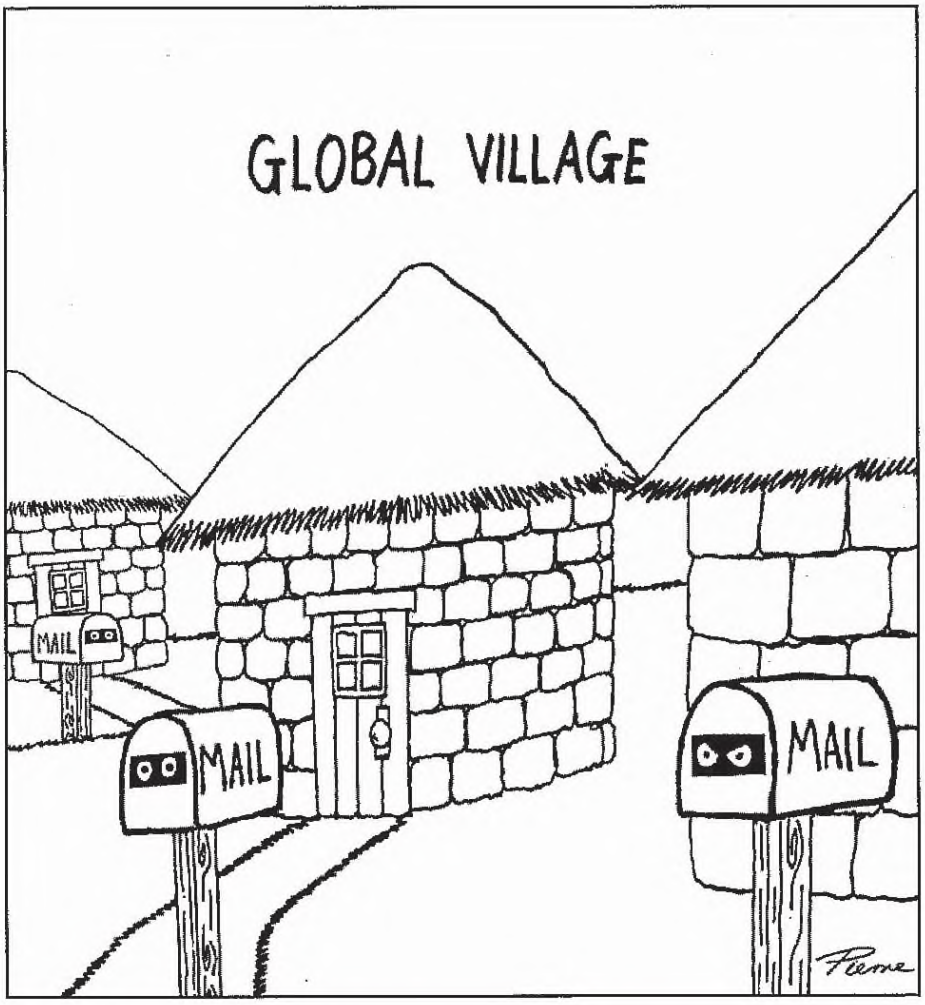
The issue was whether there was an "intercept" of a communications within the meaning of the *Wiretap Act*5. In the email transfer protocol, an email message is locally stored, formatted and forwarded by mail transfer agent ("**MTA**") through the Internet from one MTA to another until it reaches the recipient's mail

server. Once the message reaches the recipient's mail server, a mail delivery agent ("**MDA**"), which in the *Councilman* case was a program called "promail", will retrieve the message from the MTA, determine which user should receive the email and place the message in the user's mailbox. In the process of retrieving and placing, the message is temporarily stored in the random access memory ("**RAM**") or on hard disk within the ISPs computer system. In other words, an email is stored contemporaneously with it transmission.

Accordingly, the defendant argued that the email interception in this case was defined in the *Stored Communications Act*6. It was in a form of "electronic storage" and could not be intercepted in violation of the *Wiretap Act*. The defendant's submission was favoured by the United States District Court for Massachusetts and upheld by the Court of Appeals.

In dismissing of the indictments, the *Councilman* court focused on the differing definitions of "wire communications" and "electronic communication" in the *Wiretap Act*. According to the Court, the definition of "electronic communications" in section 2510 (12) of the *Wiretap Act*7 fails to provide for any "electronic storage". In contrast, "wire communication" included "any electronic storage of such communication" in its definition8. The omission of "electronic storage: in "electronic communications" was intentionally excluded by the Congress from applying "intercept" to "electronic communications" when those communications are in electronic storage. In order to find an offence against the intercept provisions of the *Wiretap Act*, interception must take place,

> "*when the message is... 'in transit' or 'in process of delivery'. No interception can occur while the emails are in electronic storage and therefore, without the requisite interception, the Wiretap Act could not be violated.*" 9



Since the electronic communications in this case were in a form of electronic storage, the Court of Appeal affirmed that no interception occurred and the case was dismissed. Accordingly, the *Councilman* decision indirectly indicated that email providers can copy and read the email of their clients.

COUNCILMAN AND THE WIRETAP ACT

Applying the *Councilman* approach, the *Wiretap Act's* prohibitions against "intercepting" electronic communication would be virtually invalid for the following reason.

> "*All digital transmissions must be stored in RAM or on hard drive while they are being processed by computers during transmission. Every computer that forwards the packets that comprise an email message must store those packets in memory while it reads their addresses, and every digital switch that makes up the telecommunications network through which the packets travel between computers must also store the packets while they are being routed across the network...*
>
> *Since this type of storage is a fundamental part of the transmission process, attempting to separate all storage from transmission makes no sense.*"10

Before the *Councilman* case, the U.S. District Court for the Eastern District of Pennsylvania had confronted the issue of the intersection of the *Wiretap Act* and the *Stored Communications Act* regarding the interception of email. In *Fraser* v. *Nationwide Mutual Insurance Co.*,11 the plaintiff, Fraser, was an agent of the defendant insurance companies. After the

plaintiff drafted a letter warning that agents might leave defendants over objectionable policies, the defendants searched Nationwide's electronic file server for email communication indicating whether the letter had been sent. The defendants opened the stored email of Fraser and other agents and found an exchange of emails between Fraser and an agent of Nationwide's competitor. The plaintiff alleged that the defendants' actions were in violation of the *Wiretap Act*. The plaintiff also asserted that the defendants unlawfully accessed his email from storage, in violation of the *Stored Communications Act*.'12

The Court held that,

> "*interception of a communication occurs when transmission is interrupted, or in other words when the message is acquired after it has been sent by the sender, but before it is received by the recipient.*"13

To clarify the concept of "intercepting email," the Court began with the discussion of the way email works.

> *"E-mail is stored in two different types of storage during the course of transmission - intermediate storage and back-up protec-tion storage. Retrieval of an e-mail message from either intermediate or back-up protection storage is interception; retrieval of an email message from post-transmission storage, where the message remains after transmission is complete, is not interception.*"14

In this case, the defendants acquired the plaintiffs email by retrieving it from Nationwide's electronic storage. At the time, the email had already been received by the recipient. The defendants did not retrieve the email before it was received and read by the recipient, and therefore, the Court concluded that there was no "interception."

The Government's contention in the *Councilman* case was consistent with the *Fraser* court's approach. According to the Government,

> "*an intercept is subject to the Wiretap between the time that the author presses the 'send' button and the time that the message arrives in the receipt's email box. Accordingly, the Wiretap Act should apply to message that are intercepted contemporaneously with their transmission and the Stored Communication Act would apply to messages that are accessed non-contempor-aneously with transmission.*"15

The Government's contention in *Councilman* and *Fraser* are theoretically consistent with the *Wiretap Act*. The decision in the *Councilman* case will ultimately have detrimental effects on the protection of personal privacy and security.

The most serious adverse effect of the *Councilman* case is that law enforcement officers could follow the less legal procedure with less juridical supervising for interception of electronic communications16. Under the *Wiretap Act*, only certain federal felonies are allowed to be wiretapped. To obtain a wiretap order, the officers must make a statement including a description of the offence, the location of the communications, the type of communications, and the identity of whose communications are to be intercepted. The judge may require the officers to furnish additional testimony or documentary evidence in support of the application. If necessary, the court could require reports showing the progress made toward achievement of the authorized objective and the need for continued interception.17 Most importantly, any content of communication intercepted in violation of the rules made under the *Wiretap Act* cannot be received in evidence.18 In contrast, those procedural protections under the *Wiretap Act* are not applicable to the *Stored Communications Act*. Law enforcement officers could gain access to contents of any wire or electronic communications in electronic storage simply by obtaining a search warrant.19

Pursuant to *Councilman's* narrow interpretation of the *Wiretap Act*, law enforcement officers no longer need to obtain a wiretap order to monitor email accounts. For example, the U. S. Federal Bureau of Investigation ("**FBI**") designed a system, Carnivore, to monitor the Internet communications of suspects under its surveillance. However, the system, housed on computers at Internet service providers, can also collect email messages from people who are not under its investigation.20 From the view point of the *Councilman* court, FBI agents would be free to install the system into ISPs' servers to monitor all web surfing and email that are temporarily stored in electronic routers during transmission without complying with the strict procedural provisions in the *Wiretap Act* for seeking a wiretap order.

Besides the flaw of the *Councilman* court's ruling, section 2701(a), coupled with section 2701(c)(l) of the *Stored Communications Act*21, exempt an electronic communication service provider from the prohibition against unlawful access to stored communications. Without the restrictions of the *Wiretap Act* and the *Stored Communications Act*, ISPs have the right to invade the privacy of their clients' electronic communications for any reason and at any time. Personal privacy on the Internet could be easily invaded.

Since a privacy right is created by law, the protection should be the same regardless of the medium of communication. Letters in the postal communication, telephone conversations, and email should all receive the same level of protection from surreptitious interception by law enforcement officers or private parties. People's interest in their privacy of the emails is the same as their privacy interest in a telephone conversation and the mail.22

In *United States* v. *Maxwell*23, the U.S. Court of Appeal for the Armed Forces affirmed that a person has an objective expectation of privacy in messages stored in computers which can be retrieved through the use of an assigned password. People also have an objective expectation of privacy with regard to messages transmitted electronically to other subscribers of the service who also has individually assigned passwords24.

This personal privacy expectation has been protected and demonstrated in title 39 of U.S. Code of Federal Regulations, Postal Service:

> *"No person in the Postal Service except those employed for that purpose in dead-mail offices, may open, or inspect the content of, or permit the opening or inspection of sealed mail without a federal search warrant, even though it may contain criminal or otherwise nonmailable matter, or furnish evidence of the commission of a crime, or the violation of a postal statute."*25

In effect, email is a form of letter. It is sent and sealed by a computer until the recipient retrieves it from his or her mail server. Hence, the sender and the recipient should enjoy the same expectation of privacy in their email as they would expect with their regular mail. That is, the mail will not be inspected by anyone unless there is a search warrant. Based on the same logic, electronic communications service providers, such as ISPs, should not allow access to theft clients' stored emails except under certain circumstances permitted by laws.

EMAIL PRIVACY BILL

To address the unfavourable consequences resulting from this juridical interpretation and the associated loose stipulation of the *Stored Communication Act*, on July 22, 2004, U.S. Congress sponsored the bill for the "*E-mail Privacy Act of 2004*."26 26 According to the summary of the bill, the objective of the Act is to modify the definition of "intercept" to include the acquisition of the contents of the communication through the use of any electronic, mechanical, or other device, at any point between the point of origin and the point when it is made available to the recipient. This Act also serves to limit the service provider exception to the prohibition on unlawful access to stored communications. Once the bill is enacted, emails that are in transit or in transit with contempor-aneously storage cannot be legally monitored without a wiretap order.

1 373 F.3d 197 (1st Cir., 2004)

2 18 U.S.C. § 2511: Interception and disclosure of wire, oral, or electronic communications prohibited: (1) Except as other wise specifically provided in this chapter [18 USCS § 2510 et seq.] any person who –

(a) intentionally intercepts, endeavours to intercepted or procures any other person to intercept or endeavour to intercept, any wire, oral, or electronic communication;

(c) intentionally discloses, or endeavours to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(3) (a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

3 *Electronic Communications Privacy Act* was divided into Title I, 18 U.S.C. 2510-2522, commonly known as the *Wiretap Act*, and Title II, U.S.C. 2701-2711, commonly known as the *Stored Communications Act*.

4 Supra note 1, 200.

5 Ibid 201.

6 *The Electronic Communications Privacy Act* Title II, U.S.C. 2701-2711, commonly known as the Stored Communications Act.

7 18 USC § 2510 (12): "electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system.

8 18 USC § 2510 (1): "wire communication" means 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 furnished or operated by any person engaged in providing or operating such facilities.. .and such term includes any electronic storage of such communication. .." However, the Congress deleted the phrase "and such term includes any electronic storage of such communication" in 2001.

9 Ibid

10 Ibid

11 135 F. Supp. 2d 623 (E.D.Pa2001)

12 Ibid 633

13 Ibid 635

14 Ibid 636

15 Supra note 1, Dissenting Opinion 208-209.
16 ibid 219-220

16 Ibid 219-220

17 18 U.S.C. 2516-2518

18 18 U.S.C. 25 15

19 18 U.S.C. 2703(a)

20 Erich Luening, 'FRI takes the teeth out of Carnivore's name', CNET news.com, 9 February 2001, at: http://news.com.coml2lOO-l023-252368.html (last visited September 28, 2004)

21 18 U.S.C. 2701: (a) Offense. Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

18 U.S.C. 2701 (c) (1): "exceptions. Subsection (a) of this section does not apply with respect to

conduct authorized (1) by the person or entity providing a wire or electronic communications service."

22 Robert A. Pilcowsky, 'The need for revisions to the law of wiretapping and interception of email' (fall 2003) 10 *Michigan Telecommunication and Technology Law Review* 47

23 42 M.J. 568 (A.F. Ct. Crim. App., 1995)

24 Ibid 577

25 C.F.R. 2333 (g)(1)

26 ll.R.4956

University student Yi-Jen Chen received a Highly Commended Award in the 2004 CAMLA Essay Prize Competition. Yi-Jen Chen is a M. Phil Candidaate at the TC Beirne School of Law, University of Queensland.