BILETA

14th BILETA Conference: "CYBERSPACE 1999: Crime, Criminal Justice and the Internet".

Monday, March 29th & Tuesday, March 30th, 1999.
College of Ripon & York St. John, York, England.

The Need For Regulating Anonymous Remailers

Michael M. Mostyn

"Look, then, into the heart, and write!"
Henry W. Longfellow 1807-1882

- Voices of the Night. Prelude. From the edition of 1886.

Introduction:

History has taught that free speech often requires some form of anonymous or pseudonymous authorship. Too many examples of repression for unpopular opinions plague our brief legacy.

The advent of the Internet has taken anonymous speech to heights never imagined. This is especially so now, during the recent remailer revolution. Although anonymous communication in the technology age is not otherwise unknown, anonymous remailers have the potential to allow anyone with a computer access to anonymous e-mail at anytime. While this is championed by civil libertarians, it has also been used to threaten, infringe copyright, and cloak traders of child pornography.

Lawrence Lessig advocates the use of the common law, a prolonged legal system, to build up case law before any rash legislative decisions are made toward a technology not fully explored. He argues this because new modes of technology facilitate new modes of criminal conduct that existing laws are not equipped to deal with. Anonymous remailers are the exception that proves the rule. The speed with which criminals are abusing this particular technology, and the anonymity it provides, necessarily make it harder for authorities to identify perpetrators. This will seriously impede potential case law appearing before the courts, as evidenced by the little case law that currently exists regarding remailers. It is therefore unlikely that the common law can be used to develop a legal policy towards remailers anytime soon. By the time it does catch up, remailers will undoubtably be leapfrogged by some new technology, and the damage will already have been done.

Anonymous remailers cannot be contained by any one government, and therefore an international convention is required to effectively provide any regulation. Such an agreement must properly balance anonymity rights with accountability. At the same time, remailer user rights to the privacy and confidentiality of e-mail communication must be expanded to protect legitimate users from tyrannous governments.

The first part of this essay will begin with a look at anonymity and its place in other legal contexts. The second part will explore how remailers work, their brief history, and the benefits and dangers of this technology. The third part will then look at how others have examined this issue, with the recommendation for a swift wake up call to regulate remailers, before disaster

strikes. However, the protection of the remailer user's confidentiality must not be sacrificed to this end.

Part I: Anonymity:

An anonymous message has been defined as a message providing the recipient with no information concerning the identity of the message originator. But this is rarely, if ever, true. An author may tend to give away his identity merely by the style of writing or the use of an unusual metaphor that the reader has known the author to use before in a similar context. There may also be third parties who have access to the author's identity, such as a remailer operator, or an access provider. Therefore the level of anonymity in e-mail is often a matter of degree, depending on how difficult it is to obtain additional information about the author. In other words, online anonymity is subject to traceability, including a remailer operator's duty (or lack thereof) to disclose user names.

Similarly, a pseudonymous message is one that is both anonymous and, "contains some information about the identity of some cognizable entity that is the originator of the message".

So a series of e-mails from a certain anonymous source may in this way build up some reputational capital, although the true identity of the author remains unknown. Richard Bachman was known to write great short stories, but who could have guessed he would later write under the name of Stephen King. Under these definitions, any ban on electric anonymity may have the unfortunate effect of banning pseudonymity as well.

The privilege relationship1. The communications must originate in confidence; 2. Confidentiality must be essential for an acceptable preservation of the parties relationship; 3. The relationship must be one the community deems worthy of such protection; and, 4. Injury to the relation through disclosure must be greater than any benefit gained. See John H. Wigmore, Evidence in Trials at Common Law (McNaughton rev. ed., 1961). has been upheld in the courts time and again in order to protect anonymity and pseudonymity in a variety of relationships that society has deemed worthy of confidence. For example, a solicitor is not compellable to reveal a client name, unless acting with him or her in furtherance of a fraud or wrongful act. The government informant and journalist/source relationships have also been protected, as they encourage the reporting of crimes and other important matters. While none of these privileges are absolute, dependant as they are on a balancing of the circumstances, they do indicate a firm desire to protect anonymity when to do otherwise may lead to a chilling effect on worthy behaviour.

Analogizing to a related technology, many feared that Caller ID might dissuade some from contacting certain organizations, such as an abuse hotline, for fear of having their identity revealed. Courts subsequently found Caller ID not to be in the public interest unless free call blocking was also offered. Critics of this view attempt to differentiate between anonymity and privacy, suggesting there should not be a right to hide on a public telephone network. The same reasoning ought to apply to the Internet, a public worldwide interconnection of computers. Such authors raise these concerns not to rid society of anonymity, which has many legitimate and important purposes, but rather to bring a greater sense of accountability to those who abuse the technology. This is a valid concern, as will later be discussed under the dangers of anonymous remailers. Nonetheless, society must be steadfastly vigilant in protecting the freedom of speech, which in times of darkness may only be facilitated through anonymity. And in an age of increasing Internet surveillance and personal profiling, anonymity may be the only tool to help even the odds.

Part II: Anonymous Remailers:

A. Anonymous e-mail:

The Internet has brought the same conflict between accountability and anonymity to a new level with the introduction of e-mail communication. There are generally five methods of anonymity available when composing an e-mail. One may send an e-mail from another's valid account, but this also requires their often difficult to acquire password. A second method is by altering one's Internet browser's preferences. By altering the SMTP server, name, and e-mail address, it can appear that the message is coming from anyone's name at any imaginary address. However, this is also easily traceable by any computer user with even the slightest sophistication, as one's IP address is also sent. The third method is to telnet to a server's mail port, a security hole that is rarely closed. This method is similar to altering the browser, but much more difficult to trace. This method's weakness is that responses cannot be received. A fourth method has similar benefits and limitations as using the mail port, although by much more complex means. This is accomplished by telneting to a news port on a host machine. The fifth method of composing anonymous e-mail is potentially the most expedient approach to anonymous communication over the Internet. This is through the use of anonymous remailers.

B. How Remailers Work:

Remailers are servers designed to strip all identification marks from any e-mail messages sent to it. The e-mail is then forwarded to the intended destination, with new identification marks placed onto the message, denoting the remailer as the message originator. Responses to the message can then be sent to the remailer which will forward it to the original author. This can create what is referred to as "double blind" communication, where two people can converse without knowing the identity of the other, due to the remailer's intermediary role. When several remailers are combined into a chain, located in various jurisdictions around the globe, together with the use of encryption software easily available on the Internet, the traceability or interception of such a message is highly unlikely.

Even this method does not offer absolute anonymity. The anonymous remailer operator must hold a list of sources and corresponding numbers in order to forward the mail to the anonymous account. This operator will always act as the weak link. PC industry pundit John Dvorak has stated that some remailers may already be fronts for government intelligence agencies. But word spreads like wildfire on the Internet, and any operator violating a user's anonymity by releasing their names to others without justification would quickly have her remailer fall into disuse. Nonetheless, remailers further down the chain will only know which immediately preceding remailer the message came from. The message can also be free from prying eyes as each resending of the message encrypts another layer over the e-mail using the latest Mixmaster technology.

Not all remailers keep lists of users, especially those which do not facilitate returnable messages, and anyone can make their own remailer with minimal effort. Coupled with the fact that most remailers do not run constantly, an e-mail sent by this method can be incredibly difficult to trace, no doubt a strong reason why there is such little litigation in this area.

C: A Brief History:

The first remailer was created in one day, from conception to finish. The original intention was to use it to encourage open discussion among victims of child abuse or AIDS. It quickly evolved into something much more.

The best known anonymous remailer controversy involves the anon.penet.fi remailer in Finland. It forwarded more than 8,000 messages daily, and held more than 50,000 active accounts. Finland was an ideal location to host a remailer because of its powerful privacy laws

and the fact that it lead the world in Internet connection *per capita*. The remailer operator was Johan Helsingus, who ran the service as a matter of principle, being a staunch civil libertarian.

A former Church of Scientology minister, Dennis Erlich, posted some of the Church's sacred texts to the Usenet through this remailer. Scientology claimed copyright in the text and filed a complaint with Interpol. Under a cloud of mistrust, due to false newspaper accusations that the remailer had been used to distribute child pornography in Sweden, a Finnish search warrant was obtained. Helsingus was offered the choice of revealing the infringer's identity, or having his computer confiscated, which carried the source addresses of the 200,000 using his service. Choosing the latter option, he shut down his operation because of the uncertainty of his future liability. Finnish police, later realizing they were misled into believing a crime had occurred in Finland, the only way to obtain a valid search warrant, vowed to be more guarded about piercing such anonymity in the future.

Helsingus is not alone in his concern over potential liability. Recently, some commercial remailer services have entered the scene, contrary to some skeptics predictions. But at the present time, the majority of remailers are still operated by civil libertarians, who offer a gratuitous service for the promotion of free speech. The majority of operators consequently do not have deep pockets to pay for costly litigation in an area of legal uncertainty. This has not deterred them from taking the risk nonetheless, because of their unwavering belief in the value of anonymous remailers.

D. The Benefits of Remailers:

Anonymous remailers have tremendous potential to benefit our society. Anonymous remailers have been used by political dissidents in Singapore to criticize their government, without fear of incarceration. More recently, a Chinese dissident may have evaded State detection had he made use of such a remailer. There are Usenet discussion groups which encourage corporate whistleblowing for employees that would otherwise be unable to do so. Public health is enhanced by allowing people to discuss delicate issues without fear of being identified. Celebrities may talk as they did before discovering their fame. Those currently employed can search discretely for new career opportunities. There is also the real possibility that by eliminating gender, race, nationality, and age from a two-way communication, for the first time in our collective history there may be an encouragement of speech based on its merits and not the supposed attributes of the speaker.

E. The Dangers of Remailers:

Unfortunately, it is widely speculated that the majority of remailer users are not employing them for such enlightened purposes. Online defamation can be spread with the click of a button, perhaps indelibly posted because of the reproduction and storage capabilities of the world's computers. Anonymous remailers can be used for destroying valuable trade secrets with impunity, spamming, and spoofing. One well known spoof distributed by a remailer in 1994 as an AP news release, claimed that Microsoft had acquired the Roman Catholic Church for an unspecified number of common shares. The possibility of an assassin for hire system across the Internet has been imagined, while the existence of a shady corner of cyberspace called BlackNet, which deals in the purchase of information ranging from nanotechnology and chemical manufacturing to children's toys, is unknown. Perhaps the costliest illegality on the Net facilitated by anonymous remailers is copyright infringement. And its most perverted use may be in the realm of child pornography, where the traceability can be negligible compared to the use of pseudonyms on a network like AOL.

Part III: The Great Debate:

Academic opinions on what to do regarding anonymous remailers have often been based on their hope (or despair) that regulation is possible. Most attempt to reach some middle ground between the defence of anonymity and the need for online accountability in an age where terror may strike from greater distances daily.

Specifically citing copyright concerns, Trotter Hardy advocates the legislative prohibition of anonymous remailers as the only solution. He states that this could be accomplished by attaching strict liability to remailer operators for the crimes of those that use their services. An international ban such as this could only be enforced through international cooperation, he suggests. Hardy's reasoning has been attacked by those such as Noah Levine as raising constitutional issues and for presupposing the ineffectiveness of less absolute solutions. A chilling effect would result for the legitimate uses of remailers. Furthermore, Hardy infers that a ban on remailers is possible, which could be the subject of some debate. Arguably, with today's technology, it is not. The imposing of strict liability upon remailer operators may merely push them into foreign jurisdictions where any one, or set, of countries' laws will be unable to reach them. What Hardy does recognize is the fact that the problem of anonymous remailers is an international one, and cannot be dealt with in nationalistic isolation.

David Post advocates that a better alternative to regulating anonymous speech is in the creation of the e-person, the recognition of a new corporate identity in cyberspace, with the accompanying limited liability. This creative suggestion has the potential to increase privacy for anonymous users of the Internet, but it is a nebulous one. Whether it is actually a viable possibility has yet to be explored. It also violates Occam's Razor, the principle that the simplest explanation is usually the correct one. Why attempt to create limited liability for criminals that had they not been using a computer would face the full extent of the law? After all, though the crimes may be, the perpetrators are not virtual.

Anne Wells Branscomb has put forward the thought that what is being sought may not be privacy, but merely anonymity, free from accountability. Nonetheless, Branscomb advises that anonymous remailers should not be banned, due to their benefits to society. At the same time, there should be some accountability for abusive behaviour by the anonymous and pseudonymous. She implies that the users of the net may be able to impose their own solutions to this dilemma. This concept of "self government" is dismissed by Jonathan Edelstein and Levine as unworkable at the present time. This was concluded because there is no single Internet community that could agree on some variety of legislature, the inability of an Internet jurisdiction to carry appropriate remedies, and the fact that the problem of tracing an anonymous message violating national law from its source would not be solved.

Noah Levine advocates an increase in the legal liability of remailer administrators for their irresponsibility as the primary method by which to balance anonymity concerns with personal accountability. He proposes to accomplish this by imposing liability on the remailer operator for constructive knowledge of the illegal acts of the remailer users, the creation of a record keeping regulation, and a safe harbour exemption for administrators who voluntarily reveal the identity of culpable users while acting in good faith. Levine further indicates that although foreign remailers exist, this should not be viewed as a reason for inaction, and predicts that such regulations will not push American remailers into foreign jurisdictions. There are several deficiencies in Levine's proposal. First of all, a constructive knowledge standard will in most cases be identical to a strict liability standard because of an operator's inability to read most messages due to encryption and Mixmaster technology. Secondly, Levine's safe harbour exemption has no concern for the anonymous user's of the remailer service right to confidentiality. It is not enough to have good faith in voluntarily releasing the identities of those who may be prosecuted abroad as political dissidents. Stricter guidelines must be

developed for when it may be appropriate to release such sensitive material. Lastly, Levine predicts that these recommendations would not push remailers into foreign jurisdictions. This assertion is likely false. If remailer operators begin to be prosecuted in a given jurisdiction, less people will serve as operators in that area. This would especially be true of administrators that operate remailers out of a sense of liberty, without payment from users or the deep pockets necessary to fight their sins in court. If there is truly a demand for remailers in the cyber-community (and there appears to be), and operators at home are too scared to operate them, they will inevitably pop up elsewhere. This time they will have been pushed to exist free of these harsh regulations in some "cyber-crime friendly" jurisdiction.

It is the abusive user of anonymous remailers that must be punished, not the administrator. Levine's required record keeping proposal is essential to this extent. Presently, some administrators do not keep such records, especially those that operate remailers which cannot receive replies. Records are necessary to allow the proper authorities to find the culpable user.

Conversely, George P. Long III advocates a decrease in remailer operator's liability. Instead, he encourages the use of the wire tap standard to give authorities the power to request user identities. Due to the technology of the Internet, Long argues that the physical evidence can be examined by the magistrate (ie. on the public Usenet) to find probable cause before the issue is ordered. He declares that this is an even better method than currently used, as presently magistrates decide solely on the word of law enforcement officers. While this solution may provide greater privacy for anonymous users living in Western democracies, it ignores the international magnitude of anonymous remailers. Many oppressive regimes do not take kindly to internal criticism, and can easily find probable cause when prosecuting free speech crimes.

Jonathan Edelstein proposes that an international convention is necessary to regulate anonymous remailers effectively. Signatory nations might disclose the source of messages sent by anonymous remailer upon a prima facie showing that a crime had been committed in the requesting nation, as well as a strictly defined list of torts. Like Long, he does not advocate remailer administrator liability, and suggests it be limited to situations where remailer operators do not follow the international guidelines. Edelstein counsels that any such convention should contain a political exemption clause. He later states that the size of messages that anonymous remailers carry should be limited, so as to eliminate their use as facilitators of child pornography pictures, which are necessarily larger files than purely textual ones. Unfortunately, due to the fact that one e-mail message may travel as several small data packets and reassemble on delivery, this is unlikely to work. A larger file could be sent in several parts and reassembled later. Furthermore, technology is constantly providing greater file compaction capabilities.

Conclusions:

After surveying various proposals regarding the future of anonymous remailers, this paper advocates the necessity of regulation. With all the current media attention over the possession of child pornography, it is unfortunate that the question "where is it coming from?" has not been asked.(visited January 20, 1999). One major reason for its recent proliferation is the increased use of anonymous remailers by users who know their identity is safe, for the time being.

An international convention is required to properly enforce any meaningful regulation upon anonymous remailers. This may be advanced through the adoption of bilateral and multilateral agreements between nations until a truly worldwide agreement is conceivable. Remailer operators should have their liability limited to not following the international agreement in order to gain their assistance in apprehending the true perpetrators. Required record keeping must be included in any agreement to easily identify those that abuse the

privileges of anonymity.

While the wiretap standard may provide a good basis as to when authorities should have access to anonymous remailer user names, especially emphasizing the minimization of any such intrusion, more is required. If any international agreement is attempted it must contain certain provisions to guarantee the privacy and confidentiality of legitimate anonymous remailer users. This could be roughly based upon privacy legislation enacted in several Canadian provinces, creating a tort, "actionable without proof of damage, for a person, wilfully and without claim of right, to violate the privacy of another". These privacy statutes do not define privacy, and no general right of privacy is known to Canadian law. But so long as they are modified to ensure their effectiveness in an online environment, such an extension to any international agreement could act to legally protect the privacy of an anonymous remailer user from the eyes of both remailer operator and State, even those where such protection is not normally safeguarded. The nature and degree of privacy to which a person is entitled must be that which is reasonable under the circumstances, and is not violated by a peace officer acting in the course of his or her duties while acting proportionately to the gravity of a crime or subject of investigation, not committed in the course of trespass. A political and religious speech exemption clause would also be required, to prevent oppressive regimes from making such "crimes" legitimate reasons for requesting user names.

Such privacy provisions are necessary for any international agreement to be effective for two reasons. First, anyone can convert their home computer into a remailer in a matter of hours. If strong regulations are passed that vicariously threaten the remailer operators for the actions of remailer users, then operators may begin setting up shop elsewhere. It would not be difficult for them to so. This would result in futile regulations that effectively regulate nothing. Secondly, it is the user of the remailer that commits the crimes. Therefore any regulations enacted must focus on maintaining proper user conduct, and punishing those that actually commit the illegal offence. By espousing a regulatory process which balances the privacy concerns of remailer operators and users with the need for authorities to identify and apprehend criminal suspects, a win-win situation materializes. The proper authorities will be allowed access to the accused's names, if the remailer operator resides in a jurisdiction which is party to the proposed convention, as a matter of process similar to outside cyberspace, with all the same safeguards intact. At the same time, remailer operators need not fear that they may be held accountable for user activity they have no control over, and likely no knowledge of. Remailer operators could then also rest assured that they need not reveal user names to authorities unless it accords with due process of the law, allowing those who abuse the system to be punished. Lastly, remailer users will know that they no longer hold absolute anonymity in cyberspace through the use of anonymous remailers. This will act to deter users who carry criminal motives, while simultaneously reassuring legitimate remailer users that their identities will never be arbitrarily revealed. If their name ever is revealed without due process, then the user will hold a remedy under the proposed convention against those who did him/her wrong.

Only through the diligent protection of anonymous remailer user's confidentiality would an international agreement properly balance the rift between accountability and anonymity.