



**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.

Computer-Mediated Communications and Criminal Evidence

Louise Ellison & Mary Childs
Faculty of Law
University of Manchester

Introduction

Two recent criminal prosecutions in the United States have drawn attention to the relatively novel phenomenon of CMCs being offered as evidence in criminal prosecutions. The trial of Oliver Jovanovic for kidnapping and sexual assault and the prosecution of Larry Froistad for murder both involved claims that CMCs were relevant to the determination of guilt or innocence. In Froistad's case the evidence consisted of a confession allegedly showing the guilt of the accused, while in Jovanovic's case the CMC was to him from his victim, and it was the defence who attempted to introduce it to support his claim that the activity in question was consensual.

It seems inevitable that CMCs will be tendered as evidence in criminal cases throughout the world. Their most obvious relevance is to crimes committed using computers, such as distribution of child pornography or other prohibited materials. But the Froistad and Jovanovic cases show that such communications may have relevance to the full range of criminal offences. In the United Kingdom, law enforcement authorities are attempting to develop a "memorandum of understanding" about police access to e-mail messages, as well as to the identities of those users. It has been alleged that the police are using the Data Protection Act to persuade ISPs to pass over private information about their customers and their messages.

In this working paper we aim to raise a number of questions relating to the technological and psychological nature of CMC and consider whether the current English law of criminal evidence presents any problems of application to such types of communications.

CMC

Although the nature of CMC and its societal and behavioural effects have been the subject of much research it is, as Walther notes, "still debated, tested, and not very well understood when one examines the literature on the subject." It has, however, been suggested that CMC differs in many ways from traditional communication technologies. These possible differences are discussed below.

One striking and highly valued feature of CMC is its general potential for pseudonymity. In CMC the gender, race, age and physical appearance of others is not immediately evident. It is for the user to decide what information she or he will or will not reveal in Internet communications. This gives

users greater control over self-representation. Researchers of human behaviour on CMC systems observe that identity manipulation is commonplace in CMC as a result. Users often create alternative personae for their on-line interactions with others that bear little resemblance to their real life identities. It is reported that gender-switching is, for example, commonplace on the Internet especially in chatrooms where the majority of female-presenting participants may, in fact, be men. Howard Rheingold, a popular theorist on community in cyberspace, notes:

"The grammar of CMC media involves a syntax of identity play: new identities, false identities, multiple identities, exploratory identities, are available in different manifestations of the medium."

Identity deception appears to be generally accepted as an inescapable feature of CMC. Some have highlighted the positive sides of selective self-representation; the opportunity it gives users to play with social roles and conventions. Others have focused on the negative aspects; how it is abused by confidence tricksters and con men.

CMC is also said to differ from other forms of communication in that CMC users tend to be less inhibited in their interactions with others. It is commonly asserted that people will write, or more accurately type, things in electronic communications that they would not ordinarily say or write in "real life". CMC users will make frank and candid revelations, it is claimed, to relative strangers on-line. This is often attributed to the enhanced anonymity of CMC. Anonymity is said to promote disinhibition among users. Frequently, this aspect of CMC is portrayed in a negative light. Anonymous CMC, it is claimed, encourages increased hostility and aggression. On-line behaviour such as "flaming" is offered as evidence that people can be more insulting in CMC. However, others claim that the safety of anonymity encourages an intimacy between CMC participants and creates an environment in which people are more willing to discuss sensitive and difficult issues and in which meaningful relationships are formed.

Disinhibition among CMC users has also been attributed to a lack of regulating feedback in electronic communications. There is no body language, no change in tone of voice or facial expression in CMC. There are only letters, numbers and symbols. Reid claims that this lack of social context cues obscures the boundaries that would generally separate acceptable and unacceptable forms of behaviour.

"Protected by the anonymity of the computer medium, and with few social cues to indicate 'proper' ways to behave, users are able to express and experiment with aspects of their personality that social inhibition would generally encourage them to suppress."

According to Reid, this can lead to extremes of behaviour on-line. Users in IRC will express love, hate, anger and intimacy and engage in relationships that would in other circumstances be deemed unacceptable in relating to strangers. Reid notes that in IRC users "feel free to act out their fantasies, to challenge the social norms, and exercise aspects of their personality that would under normal interactive circumstances be inhibited." This extends to sexual behaviour on-line. There are many sexually orientated chatrooms on IRC where users engage in open, frank and sexually explicit exchanges.

"Norms of etiquette are obscured by the lack of social cues, and the safety given by anonymity and distance allow users to ignore otherwise strict codes regarding sexual behaviour."

It is also suggested that people attach less significance and weight to their electronic correspondence. Electronic messages are regarded as casual and transitory and are less reflective as a result. This is in part due to the fact that people assume that their one-to-one messages are private and will be seen only by the recipient; they are, as a result, lulled into a false sense of security. A user may include

extremely personal information in an e-mail believing it to be the equivalent of sending a letter when, in fact, e-mail messages may be more accurately compared to a postcard in terms of privacy. In addition, people are also often unaware that most e-mail systems can create a complete record of a communication. As well as the text of a message, information regarding the transmission and receipt of the message will also be stored. This may include the names of the sender and recipient(s), the date and time that messages were sent and received, and an acknowledgement that the e-mail was retrieved. Many people also wrongly assume that once a file or e-mail message is deleted it is gone. In fact, e-mail messages and deleted files may remain hidden in a computer's storage areas long after they have been erased from the screen. Some computer applications create back-up files in unlikely places to reduce the chance of data being inadvertently erased. With the help of a relatively simple undelete programme deleted files may be easily recovered

Oliver Jovanovic

In April 1998, Oliver Jovanovic, a thirty-year-old student at Columbia University, was convicted of the kidnapping and sexual assault of a woman he met in an Internet chatroom. Jovanovic, who used the pseudonym Oliver Gray on-line, and the victim, 22-year-old philosophy student, corresponded in chat rooms and by electronic mail for several months. The two arranged to meet for dinner and afterwards the young woman agreed to accompany Jovanovic to his apartment. It was here that the woman alleged that she was subjected to a 20-hour ordeal during which Jovanovic tied her up, threatened to kill her, burned her with candle wax and beat her with a baton. The electronic communications that the two had exchanged before and after the alleged attack were to become the focus of the trial. In these messages both Jovanovic and the woman discussed a range of subjects including violent films, sado-masochism and the occult. A central argument in the case was whether the electronic mail messages should be presented to the jury in their entirety. The defence argued that they should be presented in full while the prosecution argued that a number of the e-mails should be excluded under New York's rape shield laws. The Manhattan Supreme Court ruled in favour of the prosecution. The defence had argued that the excluded messages revealed the victim's interest in sado-masochism and supported the defence's claim that what took place was consensual. Jovanovic was sentenced to 15 years to life imprisonment. The defence plan to appeal.

Larry Froistad

In March 1998, Larry Froistad, a computer programmer from San Diego, posted an Internet message to members of Moderation Management, a self-help group dealing with alcohol problems, in which he confessed to killing his daughter by setting fire to their home. At the time the fire had been ruled an accident. Three members of the support group faxed printouts of the confession to the police and Froistad was arrested and charged with murder. In the confession Froistad stated:

"I got wickedly drunk, set our house on fire, went to bed, listened to her scream twice, climbed out of the window and set about putting on a show of shock, surprise and grief to remove culpability from myself."

Froistad initially claimed that the confession was an expression of grief and guilt and untrue. In an e-mail sent two days after his on-line confession Froistad wrote:

"I'm so confused, I keep remembering what must be dreams as reality."

Froistad has since pleaded guilty to murder; he was sentenced to 30 years imprisonment and an additional 10 years for child pornography offences, with no chance of parole for 25 years..

Evidence - General Principles

Where emails or other forms of CMC are adduced as evidence of facts stated in them, they must fall within a statutory or common-law exception to the rule against hearsay. How would these rules have applied to the Froistad and Jovanovic cases were they tried under English law?

Confessions

Froistad's statement is a confession. One of the most important exceptions to the hearsay rule is that allowing the admission of confession evidence. The traditional justification for admission of confessions lies partly in the belief that they are more likely to be reliable than other hearsay statements, as nobody would confess to a crime without good reason. The maker of the statement would know that it was against his or her interest to utter the incriminating words, and would not do so lightly. History has taught that people will confess for many reasons, but this notion of enhanced reliability still underpins this exception to the hearsay rule. Could it be argued that this rationale has even less validity with respect to CMC confessions than with respect to confessions made face-to-face? If Larry Froistad typed his confession believing that the message could not be traced back to him or if the faceless, seemingly private nature of CMC induced Froistad to make a confession that under different conditions he would never have made should this affect the admissibility of the confession?

PACE defines a confession as any statement wholly or partly adverse to the accused; for such a statement to be admitted it must pass the tests set out in s.76 of PACE. That section says the confession will be excluded if the prosecution does not disprove beyond reasonable doubt any claims that the confession was either obtained by oppression of the person who made it or "in consequence of anything said or done which was likely, in the circumstances existing at the time, to render unreliable any confession which might be made by [the defendant] in consequence thereof".

The judicial interpretation of "oppression" has been quite narrow, and it seems unlikely that its application to CMCs will present any serious issues. The "unreliability" head of exclusion, however, might be more problematic. If there are psychological differences between CMC and other forms of communication could defence counsel seek to rely upon these differences in their arguments about the potential unreliability of Internet confessions? For example, could it be argued that the anonymity and fantasy-friendly nature of cyberspace might increase the likelihood of any particular confession being unreliable?

Case law interpreting this ground of exclusion has established that the thing "said or done" which forms basis of the unreliability claim must be something external to the accused - thus a heroin addict was unable to argue that his confession should be excluded as unreliable because he made it while suffering withdrawal symptoms in order to obtain his release so he could seek drugs. The addiction and its unpleasant consequences were 'internal' and therefore could not support a claim for exclusion based upon the potential unreliability of the confession. There must be a causal link between the confession and something said or done by someone other than the accused. If the accused is more prone to make unreliable statements in CMC than in face-to-face communication, it is likely that this factor would be found not to constitute something external to the accused, so the causal nexus would be absent. This does not mean, however, that the mental state of the accused and the posited psychological peculiarities of CMC would be irrelevant to the question of unreliability. If there is something said or done which leads the accused to make a confession, then a wide range of other factors may be taken into account when assessing the risk of unreliability, due to the inclusion

in the section of the words "in the circumstances existing at the time". Those circumstances may well include the psychological state of the accused. Thus in a case like Froistad's defence counsel might argue that the comments or questions of others in his group induced Froistad to confess, but that the confession was potentially unreliable because of the nature of the forum, an argument they might seek to support by pointing to the number of group members who apparently felt the confession was untrue.

An example of the courts taking a broad approach to the range of surrounding circumstances is *McGovern*, in which the background circumstances relevant to the assessment of likely unreliability included the fact that the defendant was said to be of a peculiarly vulnerable disposition, was pregnant, and had been vomiting in her cell.

This approach was used to consider the emotional and psychological background in the trial level decision of *Hall (Keith)*. Hall became besotted with an undercover policewoman, who secretly recorded their conversations. After some time without any admission of guilt by Hall, the officer responded to his marriage proposal by saying that she feared his wife might return. He responded by saying that he had killed his wife and disposed of the body. His confession was excluded as unreliable, because in the circumstances he would be under great pressure to appease the woman he loved.

Exclusion if Improperly Obtained

If the confession was not excluded under s.76, it might still be argued that the court should exclude it under s.78, on the grounds that "having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect upon the fairness of the proceedings that the court ought not to admit it". In *Sang*, it was held that unfairness would be found where the prejudicial effect of the evidence outweighed its probative value, or where it was obtained by improper or unfair means. In practice this discretion has been used principally to exclude evidence obtained as a result of some sort of police illegality or impropriety. It is possible, of course, that a CMC confession like Froistad's might be thought more prejudicial than probative and therefore excluded under s.78, but there is no reported case of exclusion on these grounds due to psychological factors absent some police wrongdoing. There seems little chance that s.78 could be the basis of a successful application to exclude in a case like Froistad's unless the CMC was obtained in an unlawful or improper way. That might be the case if it had been obtained by some violation of the Data Protection Act or the Interception of Communications Act, but not where, as in Froistad's case, the relevant email was passed on to the police by one of its intended recipients. Of course, if a police officer had joined the email discussion group and actively induced Froistad to confess, the argument for exclusion under s.78 might be stronger.

The Home Office has been considering the question of how e-mails and other forms of CMC should be treated for the purposes of evidence gathering. It appears that one of the issues currently under review is whether e-mails should be subject to the same rules as ordinary mail when police wish to intercept it as part of an investigation. Police have already obtained search warrants authorising them to seize computer logs held by ISPs; an initiative proposed by the Association of Chief Police Officers would circumvent the need for such warrants. Under the proposed new scheme, ISPs would be sent electronic forms certifying that police needed the requested information for the prevention or detection of crime. These forms would be valid if signed by a senior police officer, and would permit the information obtained to be "used for any other investigation". ISPs claim that police have already been asking for information which might be illegal for ISPs to provide, such as lists of all clients living in a particular area. Police and government officials have also expressed a wish to have all outgoing e-mails recorded as a matter of routine, and to request that ISPs log all incoming emails for

selected individuals. It appears that the legality of such searches under present law is questionable at best. They are likely to be outlawed by the new EU Directive on communications privacy, until such time as regulations are in place to control such access.

Expert Evidence

Some researchers of human behaviour in CMC might suggest that Froistad was communicating in a forum whose psychological dimensions were not within the understanding of the ordinary juror and that expert opinion evidence on this matter would assist the court. In English law expert evidence is not admissible to explain aspects of human nature and behaviour within the bounds of normality. The psychological aspects of CMC, even if accepted, are highly unlikely to satisfy the requirement of abnormality and therefore expert evidence as to weight to be accorded Internet communications would be inadmissible. Suitably qualified experts have a clearer role to play in relation to the authentication and provenance of computer-derived evidence and the reliability of any computers involved. The complex techniques involved in the seizure, recovery and storage of computer evidence mean that these are matters outside the knowledge and experience of the ordinary juror and would therefore satisfy the rule in *Turner*.

If a confession like Froistad's were admitted in evidence, it would still be open to the defence counsel to argue that it should be given little or no weight due to the psychological peculiarities of CMC. In order to do so they might rely upon the testimony of the accused himself to explain his reasons for making the statement.

Documentary Hearsay

One exception to the hearsay rule is that contained in ss.23 of the Criminal Justice Act 1988. This allows documentary hearsay to be admitted in certain limited circumstances. Section 23 permits the admission of first-hand documentary hearsay subject to two conditions. The first is that the maker of the statement is unable to attend the trial for one of a number of reasons (including death or unfitness to attend due to a physical or mental condition). Unavailability might be satisfied where the maker of the statement is overseas (say, the sender of an email message) and cannot be persuaded to travel to the UK for the trial. The second condition is that leave of the court is required where the document was prepared for the purposes of criminal proceedings or a criminal investigation.

Computer –Produced Documents

If the documentary hearsay is in the form of a computer-produced document, certain additional requirements must be satisfied before it can be admitted. Section 69 of the Police and Criminal Evidence Act 1984 provides that such statements are not admissible unless it is shown that:

- there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;
- at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents; and
- any relevant conditions specified in [rules of the court] are satisfied.

This provision is based upon a model of computer-produced evidence that assumes the computer in

question is the only one involved in production of the document. It was drafted and enacted at a time before the use of CMC was common, and therefore does not easily fit the model of email or other forms of Internet communication, where many computers may be involved in the production and transmission of the evidence. How could it be shown that none of those computers were malfunctioning? The hurdle posed by s.69 means that it may prove virtually impossible to introduce emails into evidence, except in cases where the prosecution is able to gain access to the computer of the sender and to extract the contents of the message from the memory of that machine. In such cases the requirements of s.69 could be met.

Conclusion

It has been suggested that CMCs differ from other more traditional communication technologies in a number of ways. It has been claimed, for example, that electronic messages tend to be less inhibited, less reflective than other forms of communication and these peculiarities are directly attributed to the nature of CMC. Research into the behaviour of CMC users is, however, at a very early stage. It is not yet possible to judge whether these purported psychological differences are sufficiently great to warrant CMCs being treated differently by the courts. After all, courts have always been deemed capable of interpreting a range of behaviours and expressions, and it would be a significant departure from this tradition to treat CMCs as falling within an exceptional class of communications. And as CMCs become more commonly used, there may be reduced scope for arguments that such communications are outside the ordinary experience of jury members. What is clear, however, is that there are potential arguments which may be raised in connection with these issues.

The Jovanovic and Froistad prosecutions do raise interesting evidential issues that English courts have yet to confront. With the exponential rise in the use of e-mail and other forms of computer-mediated communications it is inevitable that CMCs will appear increasingly in criminal proceeding world-wide. The reliability, authenticity and verifiability of electronic communications are issues that criminal courts in all jurisdictions will have to address.