

E-mail, terrorism, and the right to privacy

Stephen Coleman

School of Humanities and Social Sciences, UNSW@ADFA, Canberra 2600, Australia

E-mail: scoleman@csu.edu.au

Abstract. This paper discusses privacy and the monitoring of e-mail in the context of the international nature of the modern world. Its three main aims are: (1) to highlight the problems involved in discussing an essentially philosophical question within a legal framework, and thus to show that providing purely legal answers to an ethical question is an inadequate approach to the problem of privacy on the Internet; (2) to discuss and define what privacy in the medium of the Internet actually is; and (3) to apply a globally acceptable ethical approach of international human rights to the problem of privacy on the Internet, and thus to answer the question of what is and is not morally permissible in this area, especially in light of recent heightened concerns about terrorist activities. It concludes that the monitoring of e-mail is, at least in the vast majority of cases, an unjustified infringement of the right to privacy, even if this monitoring is only aimed at preventing the commission of acts of terrorism.

Key words: E-mail, International Bill of Rights, Justified Infringement of Rights, law enforcement, right to privacy, terrorism, Universal Declaration of Human Rights

Introduction

The rapid growth of the Internet as a tool of trade, research, and entertainment has led to a good deal of discussion about the impact of this widespread use of computers on people's privacy. Governmental responses to recent acts of terrorism in Western democracies, particularly responses that seem to limit or impose on the rights of citizens of these countries, have only served to intensify that discussion. Much of the discussion of privacy on the Internet has focussed on legal conceptions of what the right to privacy might entail, and thus deals primarily with the issue of what legal protection users of the Internet (particularly American users of the Internet) might be entitled to.

Such an approach seems to me to be somewhat wrong-headed, and so in this paper I want to look at this problem in a different way. I hope to achieve three main aims: (1) to highlight the problems involved in discussing an essentially philosophical question within a legal framework, and thus to show that providing purely legal answers to an ethical question is an inadequate approach to the problem of privacy on the Internet; (2) to discuss what privacy in the medium of the Internet actually is; and finally (3) to attempt to

apply a globally acceptable ethical approach to the problem of privacy on the Internet, and thus to answer the question of what is and is not morally permissible in this area.

I should make it clear from the start that the entire issue of privacy on the Internet is a broad one, and so I expect the points that I make in this discussion will apply to a wide range of Internet practices. However, in this discussion I wish to pay special attention to the ways in which the right to privacy may be infringed during the transmission of e-mail; most notably through the monitoring of email by employers, and through the interception of e-mail by law enforcement agencies, particularly as a response to threats of terrorism.

The legal approach to privacy on the Internet

In investigating the issue of privacy on the Internet, one common approach has been to focus on legal principles that apply in certain situations in the real world, and then to attempt to apply these same principles to the virtual world. While some of these discussions have focussed purely on legal issues that may arise out of apparent breaches of privacy on the

Internet, others have attempted to draw ethical conclusions out of the legal principles that are examined.

An example of this is the work of Robert McArthur, who has taken the concept of “reasonable expectation of privacy” from the real world, and then used this principle to examine two forms of Internet activity; browsing the World Wide Web, and sending and receiving e-mail.¹ McArthur suggests that there are two essential principles against which any apparent breach of privacy in the real world must be judged, and if either one of these two principles apply, then there has been no *legal* breach of privacy. McArthur calls these the “Mischance Principle” and the “Voluntary Principle”.

The Mischance Principle – we cannot reasonably expect to maintain privacy over that which another person could discover, overhear, or come to know without concerted effort on his/her part to obtain this information.²

The Voluntary Principle – If I choose to decrease the relative amount of privacy for myself and information under my control by exposing it to view, I thereby decrease the reasonableness of any expectation that this privacy will be observed.³

In his discussion of browsing the World Wide Web, McArthur suggests that since it is now widely known that the one’s web browsing history can be tracked through the use of cookies and other software, browsing the World Wide Web is essentially a public activity, and thus falls foul of the Voluntary Principle. Unless I take specific measures to conceal my identity or to block the tracking software, then I have chosen to reveal this information about myself. Thus it is, according to McArthur, unreasonable to expect privacy in this domain and it is not a breach of my privacy for someone to collect this click-stream data.

In his discussion of sending and receiving e-mail, McArthur suggests that it is common knowledge that this medium of communication is not secure. As evidence of this he points to the fact that many major companies have put in place programs to monitor their employees’ e-mail,⁴ that many e-mail messages are erroneously intercepted by the technology that is

employed by law enforcement agencies to intercept the e-mail of suspected criminals,⁵ that backup tapes that may contain e-mails are not securely stored, and so on. McArthur again draws on the Voluntary Principle to assert that it is unreasonable to expect privacy in e-mail; if I entrust material to an e-mail while knowing that the global e-mail system is not secure, then I have chosen to reveal this information, and my privacy has not been breached if the material in that e-mail becomes public.

McArthur’s assertions about what is and is not legal in regard to privacy in the use of computers can be criticised on several grounds. Take, for example, McArthur’s suggestion that it is common knowledge that e-mail is not a secure medium of communication. While it may be the case that some (perhaps even many) people who communicate by e-mail are aware that this medium of communication is not fully secure, one might question whether this really counts as ‘common knowledge’. It could also be argued that many methods of communication are not fully secure; mail can be intercepted and opened, telephones can be tapped, conversations can be monitored with listening devices, and so on. It is usually the case that any interception of such communications is considered to be a breach of privacy, and requires legal justification. If intercepting and reading someone’s mail is considered to be a breach of privacy, then there would seem to be at least *prima facie* reason to believe that intercepting and reading someone’s e-mail would also be a breach of privacy.

McArthur’s claims about the lack of privacy in e-mail also seem to ignore one of the principles that he himself quotes. The Mischance Principle suggests that my privacy has not been breached if another person could come to know that information without concerted effort on their part. Yet intercepting and reading e-mail seems to be something that does actually require concerted effort, especially in the case of law enforcement agencies attempting to intercept the e-mails of suspected criminals. If it is only as a result of concerted effort that another person comes to read the information contained in e-mails that I have sent, and if it is only this type of effort that, unbeknownst to me, makes this medium less than secure, then neither the Mischance Principle nor the Voluntary Principle seem to apply.

However, the biggest problem with a discussion like McArthur’s is that it is based on what is actually true at the present time; on what is the case. While it is of some interest to know what the law does and

¹ Robert McArthur. “Reasonable Expectations of Privacy”. *Ethics and Information Technology*, 3:123–128, 2001.

² Ibid. p. 124. McArthur attributes the original discussion of this principle to Mark Tunik, *Practices and Principles*. pp. 161–190, Princeton University, Princeton, 1998.

³ Ibid. pp. 124–125.

⁴ Ibid. p. 127 – drawing on a report from the American Manufacturing Association, <http://www.amanet.org/press/research/checkemail>.

⁵ Ibid. McArthur quotes *Electronic Privacy Information Center Alert* 7.15, August 3, 2000 (http://www.epic.org/alert/EPIC_ALERT_7.15.html).

does not allow, in discussions such as this we are generally far more interested in what *ought* to be the case, rather than what *is* the case. And discussions of law are almost invariably discussion about what is, rather than about what ought to be. In discussing the transfer of child pornography through the Internet, for example, while it may be of interest to know what laws would apply to those engaged in the practice, the main reason that this is of interest is because of an already formed a moral judgement; that engaging in the trade of child pornography is wrong, and thus the interest in what laws might apply is actually an interest in preventing the trade of child pornography through the Internet. If it was to turn out that there were no laws that applied to the trade of this material, then it is likely that there would be a call for laws to be passed that would ban the trade of child pornography on the Internet. Criminal laws that apply to the dealings on the Internet have their base in moral principles, as in fact do all criminal laws. It is because of a prior moral judgement, that engaging in a particular action is wrong, that criminal laws are established in the first place.

Thus in examining the issue of privacy in the use of computers, and privacy on the Internet, the primary interest is always likely to be in a moral issue, about what is the right and wrong thing to do, rather than in a legal issue, about what is legal and illegal. So while it may be true that e-mail, for example, is not a fully secure communication medium, that is a statement about what is the case, and not about what ought to be the case. McArthur points out that many companies monitor the e-mail of their employees, and that law enforcement agencies may intercept innocent e-mails while attempting to intercept the e-mail of criminals. This may well be true, but it does not even attempt to answer the question of whether companies *ought* to monitor employees' e-mail, or whether law enforcement agencies *ought* to try to intercept e-mail sent by suspected criminals. Similarly, the fact that one's Internet browsing habits may be recorded by software placed on websites and downloaded on to the browser's computer, does not answer the question of whether such software *ought* to be placed on websites.

While there are some extremely worthwhile points raised in discussions of the legal issues of privacy, I hope that this discussion has shown that a legally based discussion cannot answer the fundamental ethical questions raised by the issue of privacy and the Internet. To attempt to answer such questions it is necessary to determine what ought to be the case, rather than what is the case. In order to answer that question, it will be necessary to examine the concept of privacy, and to attempt to come to some under-

standing of why privacy is an ethically important concept, and thus how questions of privacy on the Internet ought to be addressed.

What is privacy?

Defining privacy is, unfortunately, not an easy task. There are innumerable definitions of privacy as a philosophical concept, and while most will capture some important aspects of the issue, it is virtually impossible to arrive at a definition that is not flawed in some way. Privacy as a concept is most commonly discussed as a right possessed by persons, and it is definitions of the right to privacy that are generally considered to be the most philosophically important. For example, an early, and extremely influential definition of the right to privacy was formulated by Warren and Brandeis,⁶ who suggested that the right to privacy was "the right to be left alone",⁷ to protect the privacy of one's thoughts and emotions. Warren and Brandeis saw this as one important aspect of a broader interest in being left alone to pursue one's own projects; in other words, they derived a right to privacy from a broader right to liberty. One problem with such a definition is the fact that a person's privacy can be invaded without any direct infringement of their liberty.⁸ Another problem is that conceiving of a right to privacy in this way makes the right too broad, and gives no clues as to when such a right might be justifiably overridden.⁹

Another way of defining the right to privacy is in terms of a right to control access to one's personal information.¹⁰ Seeing privacy in this way makes it akin to a property right, in that it can be dealt with in any way that the owner wishes. However, it is questionable whether it is appropriate to link privacy and control in this way, since this definition is open to a counter-example. A person who freely discloses intimate information about themselves to a wide range of people has suffered a loss of privacy, but since the disclosure of that information was entirely voluntary, there has been no loss of control. It seems clear that some sense of control of personal information is an

⁶ Samuel Warren and Louis Brandeis, "The Right to Privacy" *Harvard Law Review* (1890) cited in Lisa Austin "Privacy and the Question of Technology". *Law and Philosophy* 22 (2003) 119–166. pp. 121–123.

⁷ Warren and Brandeis, quoted in Austin. *Ibid.*

⁸ See Darren Charters "Electronic Monitoring and Privacy Issues in Business-Marketing: The Ethics of the DoubleClick Experience" *Journal of Business Ethics* 35 (2002) 243–254. pp. 246–247.

⁹ *Ibid.*

¹⁰ *Ibid.* Charters draws heavily on the work of H. McCloskey "Privacy and the Right to Privacy" *Philosophy* 55 (1980) 17–38.

important aspect of privacy, but it cannot constitute privacy in and of itself.

A third way to define privacy is to make reference to the notion of public and private spheres of life. The private sphere is that part of life concerned with familial, personal, and intimate relations, while the public sphere is the part of life concerned with action in the community. This is the way that the terms are used in business, for example when discussing public sector and private sector enterprises. If privacy is taken as referring to the private realm, then a right to privacy is simply a right to ensure that one's life is not subject to undue interference from the government. While defining privacy in this way does capture some important ideas, it falls far short of an adequate definition of privacy generally, for such a definition would suggest that it is only the government and its agencies that can infringe upon a person's privacy, which is clearly not the case.

While there are clearly problems with the main definitions of privacy, it is also the case that these influential definitions each manage to delineate some important aspect of privacy. Warren and Brandeis highlight the necessity of privacy in order to allow a person to pursue their own life goals and projects.¹¹ Accounts that link privacy to control over the release of personal information, draw attention to the fact that a right to privacy is necessary (at least in some cases) in order to prevent a person from being harmed. For example, if a person's sexual preferences were considered to be socially unacceptable, then that person might be harmed if that information was to become widespread. Thus a right to control the release of this personal information is necessary to prevent harm to that person. Accounts of privacy that draw a distinction between the public and the private aspects of a person's life serve as a reminder of the importance of this distinction, for if there is excessive interference of the government into the private domain, then certain public roles become impossible to fulfil. An example of this is the necessity for secret ballots in elections; if a person's voting preferences are known to the government, then it becomes difficult (if not impossible) for that person to properly fulfil their public role as a voter. Thus it can be seen that while it may not be easy to arrive at a precise definition of privacy, it is possible to sketch out the main features of a right to privacy.

What aspects or features of life must a right to privacy protect? Three things have already been mentioned. A right to privacy must be, in at least some sense, a right to be left alone, and a right to exclude others, which would include a right to not be

subject to unjustified surveillance. A right to privacy must also allow a person to control, at least to some extent, the release of personal information about them. A right to privacy must also protect a person from unjustified interference by the government, lest one's public roles be undermined.

The extent to which a right to privacy can limit these sorts of infringements of privacy is also a source of some debate. For example, the question of the control of the release of personal information has been debated at some length. Some people have argued that virtually all information about a person is public information, which thus makes that information available for publication and dissemination. Others suggest that even information about a person that has been collected publicly ought to be subject to privacy limitations. This has given rise to a debate about the issue of 'privacy in public'; a debate that is unfortunately beyond the scope of this paper to discuss.

The International Bill of Rights

The biggest problem with discussion of moral issues that arise in a medium like the Internet, is that there is little agreement about what moral theories ought to be applied to such a discussion. One scholar might wish to discuss these issues in purely utilitarian terms, but such a discussion is unlikely to be well-received by another scholar who wishes to discuss that same issue in Kantian terms, and both are likely to disagree with yet another scholar who wishes to discuss the same issue in terms of an ethic of care. Such problems are only magnified by the global nature of the Internet; in order to come to any satisfactory answer to these problems, it is necessary to rely on some global, or near-global, theory of ethics.

There is really only one moral standard in the world today that fits with the global nature of the Internet, and that is the International Bill of Rights. Assented to by the General Assembly of the United Nations,¹² the International Bill of Rights consists of three documents: the Universal Declaration of Human Rights (UDHR), the International Covenant on Economic, Social and Cultural Rights (CESCR) and the International Covenant on Civil and Political Rights (CCPR). The International Bill of Rights was reaffirmed by 171 countries of the world at the World Conference on Human Rights, held in Vienna in June

¹¹ Warren and Brandeis "The Right to Privacy".

¹² In fact, recognition and promotion of human rights is central to the mission of the United Nations, being mentioned in Article 1 of the United Nations Charter.

1993. As of November 2, 2003, the United Nations consisted of 189 member states, so the reaffirmation of the UDHR by 171 nations represents the overwhelming majority of the nations (and peoples) of the world. Such international agreement to a common moral standard makes these human rights instruments an excellent tool for assessing the issues raised in the use of an international medium such as computing, and the Internet.

Both the UDHR and the CCPR assert that people have a right to privacy. Article 12 of the UDHR states that:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 17 of the CCPR is virtually identical:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

The biggest difference between these two documents is that the UDHR is merely an aspirational document, whereas the CCPR is an international treaty, legally binding upon its signatories, who are thus committed to taking steps to ensure that the rights enumerated in the CCPR are incorporated into domestic law. As of November 2003, 151 nations had ratified this treaty, thus agreeing to be bound by its standards. Such international agreement gives good grounds for asserting that there is a widely recognized right to privacy, and suggests that an attempt to deal with the issue of privacy and the Internet ought to utilize the notion of such a right. I would also suggest that given its widespread international acceptance, any attempt to deal with practical problems of privacy on the Internet also ought to give due recognition to the International Bill of Rights, and its to interpretation, to which so many nations have agreed to be bound.

In examining the International Bill of Rights, and its relation to the issue of privacy on the Internet, the published comments of the Office of the High Commissioner for Human Rights (OHCHR) regarding the interpretation of article 17 of the CCPR are extremely important, since in agreeing to the CCPR, nations are binding themselves to the interpretation provided by the OHCHR.

There are eleven particular points raised in the OHCHR comment on article 17 of the CCPR. Of these, several are particularly relevant to the issue of privacy and the Internet. Point 3 notes that when the article prohibits “unlawful interference” with privacy, that this means that no interference with privacy can take place except for cases specifically authorised by law, and that the law itself must also comply with the provisions of the covenant. Point 4 emphasises this even further, by noting that arbitrary interference is also prohibited by the covenant, and this may well include interference that is provided for under law. Any legal interference with privacy should be reasonable in the particular circumstances.

Point 8 deals specifically with correspondence, and notes that:

Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed *de jure* and *de facto*. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.

Point 8 also notes that where authorised interference with correspondence is contemplated, that such interference may only be made by the authority designated under the law, and that the decision to engage in such interference must be made on a case-by-case basis. Point 9 notes that state parties are also under an obligation not to engage in interference with correspondence that is inconsistent with article 17 of the covenant.

Justified Infringement of Rights – The use of harmful methods

The International Bill of Rights certainly does not propose an absolute right to privacy. Rather these declarations of rights are intended to protect persons against “arbitrary” interference with their privacy. So what does this actually mean? The Shorter Oxford Dictionary defines arbitrary as “Unrestrained in the exercise of will or authority; despotic, tyrannical.”¹³ Thus an arbitrary infringement of privacy would be an infringement that was based on an unrestrained exercise of authority, and a non-arbitrary infringement of privacy would be an infringement that was justified according to recognisable and objectively

¹³ Brown, Lesley (Ed.) *The New Shorter Oxford English Dictionary*, 3rd Edn. (Oxford: Clarendon, 1993).

defined standards. In fact, many countries have recognised the need to establish clear standards that make it possible to clearly differentiate between justified and unjustified infringements of privacy, laying down in legislation the specific conditions that must be met in order for an infringement of the right to privacy to be legal. The bases of these laws, as with most criminal laws, are ethical principles – so the laws themselves reveal the ethical principles that are considered to be important.

In order to determine when it might be justified to infringe upon a particular person's right to privacy, it is necessary to have some understanding of when it is going to be generally justifiable to infringe upon a right. The area of police ethics has been an important source of discussion in this area, since the infringement of rights is an everyday occurrence in police-work. The basic principle in that area is that a police officer will only be justified in infringing upon a person's moral rights if the following rules are met:

- (1) The police officer is aiming to achieve a good end.
- (2) The infringement of rights is necessary – i.e. there are no other means that could be used to achieve this end.
- (3) The good that is being aimed at by infringing upon this right, outweighs the evil that will follow from infringing upon the right – i.e. the infringement of rights is proportional to the end that is being aimed at.

The usual situation where a police officer will be required to infringe upon a particular person's rights, is where such an infringement is necessary in order to protect the rights of another person. In order for condition (3) to be met, the rights that the police officer is aiming to protect would have to be at least as fundamental as the right that the police officer is going to infringe upon.

A practical example that illustrates this situation is when a police officer is forced to resort to the use of deadly force. If a police officer is going to violate a person's right to life (or threaten to violate their right to life) through the use of deadly force, then this will only be considered to be proportional to the situation if the officer is using deadly force to protect the right to life of another person. One person's right to life is threatened by the police officer in order to protect the equally fundamental right of someone else. It can clearly be seen that the police officer would not be justified in using deadly force in order to prevent a theft – the right to own property is not as fundamental as the right to life, thus it would not be proportional for a police officer to threaten to violate the right to life in order to protect another person's right to own property.

The three rules that I mentioned earlier are really the only justification for any infringement of rights: in order for it to be justified for person A to infringe upon any of the moral rights of person B, the three conditions must be met. Person A must be aiming at a good end, there must be no other way of achieving that end that does not infringe upon rights, and the infringement of the rights of person B must be proportional to the end that is being aimed at – i.e. the right that is being protected by infringing upon the rights of person B must be at least as fundamental as the right of person B that is being infringed upon. (In fact, in situations where these three conditions are actually met, it will often be the case that person B is attempting to infringe upon or violate the rights of another person, and that this is the reason why it is justified to infringe upon the rights of person B.)

There is one important general consequence of the need for justification of any infringement of rights. Any time that an important moral right is being infringed upon, if that infringement of rights is to be considered justified, then the circumstances of that individual case will need to be examined. One cannot give a blanket approval for the infringement of rights; each infringement will have to be considered on a case-by-case basis to determine if that particular infringement of rights is justified.

In order for it to be justified to infringe upon any person's right to privacy, the three basic conditions must be met; good ends aimed at, privacy infringement necessary, and privacy infringement proportional to the ends aimed at. In general, it will only be justified to infringe upon a person's right to privacy where this is necessary in order to preserve the more fundamental rights of others, rights such as life, liberty, and security of person.

The need to justify any infringement upon the right to privacy has long been recognised in law. For example, if a police officer wants to infringe upon a particular person's right to privacy, such as by searching their house or by tapping their telephone, (and if the officer wishes to do this legally!) then it is necessary for the police officer to obtain a warrant. In order to get a warrant that will allow this legal invasion of privacy, the officer must provide evidence that this infringement of privacy is justified, by showing that the infringement is necessary and that there are reasonable grounds at law to allow the infringement of rights. In effect, the officer is being asked to prove to a third party (usually a judge) that this particular infringement of rights meets the three general rules for the justified infringement of moral rights.

In the terms of the International Bill of Rights, if a particular infringement of privacy meets the three

general conditions for the infringement of rights, then that infringement of the right to privacy is non-arbitrary, and invading someone's privacy in this way would not breach the right to privacy clauses of the UDHR or the CCPR.

Having discussed the arbitrary and non-arbitrary infringement of the right to privacy, it is now time to return to the final task of this paper – to see how the International Bill of Rights might apply to issues of privacy arising from the Internet, particularly with regard to e-mail. In examining this issue, there are two main cases that I wish to consider; the monitoring by employers of e-mail sent by their employees, and the monitoring and interception of e-mail by law enforcement agencies.

Privacy in the on-line workplace

It can be seen from the comments of the OHCHR, that monitoring of e-mail by employers will only be compatible with the International Bill of Rights in very specific circumstances. The CCPR requires that monitoring not be illegal or arbitrary, thus all monitoring would have to meet not only legal standards, but must also meet the required standards for the infringement of rights. That is, the infringement must be aimed at achieving good ends, it must be necessary to infringe upon rights in order to achieve those ends, and the good to be achieved by the infringement of rights must be proportional to the evil caused by the infringement. Since all infringements upon rights need to be justified on a case-by-case basis, monitoring of e-mail would also need to be justified case by case. This would seem to rule out virtually all monitoring of e-mail by employers, though there may be some exceptions to this in unusual circumstances.¹⁴ Even if the e-mails were not being read by the employer, but were rather being scanned for particular terms (which has been seen as a way of protecting company secrets without requiring mass infringement of rights), this would be a form of

arbitrary interception and interference with communication, which is also prohibited by the CCPR.

It could be suggested that the fact that it is the employer's equipment that is being used to send e-mails, means that the employer has the right to monitor the way in which that equipment is being used, and to exercise some control over the use of that equipment. While this may be true, it does not justify the practice of monitoring of e-mails sent by employees, for monitoring e-mails sent by employees will infringe upon the employee's right to privacy, and there are many other ways in which an employer might exercise control over the use of their equipment that do not involve the infringement of the rights of others. As Miller and Weckert point out,¹⁵ employers have certain rights with respect to their employees, but employers are still constrained by the human rights of their employees. An employer cannot imprison, rob, or flog an employee simply on the basis of the employer/employee relationship, since these things infringe upon the employees basic human rights. Similarly, an employer cannot simply infringe upon the right to privacy of their employees.

There are other obvious examples that can be presented to demonstrate that mere ownership of equipment does not justify infringing the privacy of those using that equipment. Consider the example of the telephone. The mere fact that someone is using a telephone that I own, does not give me the right to listen in on their conversation. In the same way, the fact that an employee is using their employer's telephone does not give the employer the right to monitor the employee's telephone calls. Similarly, the fact that one owns the cables through which telephonic communications are being sent does not give one the right to monitor those communications. As is the case with computer equipment, ownership of the telephonic equipment does give one the right to exercise some control over the use of that equipment, but there are many ways in which control can be exercised without monitoring calls. Employees could be informed that the business telephone is not to be used for personal calls without the approval of the employee's manager for example. Or the use of the telephone system could be limited in certain ways, such as by blocking particular telephone extensions from making long distance phone calls. So in the case of computing equipment, an employer may control the use of that equipment in certain ways, such as by insisting that the equipment only be used for work related purposes, or by restricting access to particular

¹⁴ If, for example, there was genuine evidence that suggested that a particular employee was using the company's e-mail facilities for illegal purposes, then monitoring of that employee's e-mail *may* be justified. In most circumstances of this type however, I would suggest that there would be justification for relevant law enforcement authorities to monitor the employee's e-mail, rather than for the employer to monitor the employee's e-mail. Even in these circumstances, it is likely that those law enforcement authorities would only be justified in monitoring e-mail sent to or received from particular e-mail addresses, rather than in monitoring all e-mail sent by the employee.

¹⁵ Seumas Miller and John Weckert "Privacy, the Workplace and the Internet" *Journal of Business Ethics* 28 (2000) 255–265. p. 258.

computing functions,¹⁶ and the employer can exercise that control without resorting to infringing upon the basic human rights of their employees.

Perhaps the biggest difference between monitoring employee's telephone calls, and monitoring employee's e-mail, is that it is technically feasible to monitor e-mail, in particular to scan e-mail for certain terms of special interest, in a way that it is not currently possible to do with telephone calls. As I hope I have made clear in the early parts of this paper, the mere fact that it is technically possible to do something does not mean that it ought to be done. Thus the difference between the technical feasibility of monitoring e-mail and the technical feasibility of monitoring telephone calls is not a moral difference.

E-mail, privacy, law enforcement, and terrorism

The final issue that I wish to examine in this paper is the issue of the monitoring and interception of e-mail by law enforcement agencies. Such activity falls into two distinct categories, which can be differentiated by the form of justification offered as a basis for this infringement of privacy; attempts by agencies such as the FBI to intercept the e-mail of those suspected of what might be termed 'ordinary' criminal offences, and attempts to intercept the e-mails of those suspected of involvement in terrorism. Intercepting the e-mail sent by those suspected of criminal offences is an activity which relies upon the protection of the rights of victims of crime for its justification, while intercepting the e-mail sent by those suspected of terrorism is usually justified by an appeal to national security.

Monitoring and intercepting the e-mail of those suspected of criminal offences, if it is to be justified, will need to meet the usual conditions for the infringement of rights. That is, the law enforcement officers who are infringing upon the right to privacy of these suspected criminals (and of any other people whose e-mail is also inadvertently intercepted) must be aiming at a good end, there must be no other way of achieving that end that does not infringe upon the right to privacy of those whose email is intercepted, and the right (or rights) being protected by this infringement of privacy must be at least as fundamental as the right to privacy. These are, of course,

exactly the same conditions that are required to be met in order for it to be justified to infringe upon a person's privacy by intercepting other forms of communication, such as telephone calls or ordinary postal mail.

It is interesting that the legal arguments of McArthur ignore this similarity; nowhere does he discuss the requirements for justified infringement of privacy in other forms of communication, yet these moral standards required for justified infringement of privacy in communications such as telephone calls or postal mail have, at least in most Western jurisdictions, been more or less directly transformed into legal requirements for justified infringement of privacy. Consistency would seem to demand that if certain legal privacy standards apply to other similar forms of communication, then these same standards ought to apply to communication by e-mail as well, unless it can be demonstrated that there are significant and morally relevant differences between the forms of communication. As I noted earlier, McArthur's focus on what actually occurs in this medium, rather than on what *ought* to occur, means that he is blind to the lack of such morally relevant differences between e-mail and other forms of communication.

As I noted earlier, an important consequence of the need for justification before rights can be infringed, is that the infringement of rights will need to be justified on a case by case basis. This means that before a law enforcement agency can be justified in infringing upon privacy by intercepting and reading the e-mail of suspected criminals, it must be possible for that law enforcement agency to specify the rights which will be protected by this infringement of privacy, and the specification would need to be in more than general terms; that is, the law enforcement agency would need to be able to nominate not only a particular right that would be protected by this infringement, but also a particular rights holder – an individual person. Thus a law enforcement agency could not argue that it was necessary to infringe upon the right to privacy by attempt to intercept and read the e-mail of a suspected criminal (C) in order to protect the rights of the community in general; in order for this law enforcement agency to be justified in infringing C's right to privacy by intercepting and reading C's e-mail, the law enforcement agency would have to be able to specify a particular member of the community (M) whose rights could only be protected by this infringement of C's right to privacy. Generally such a condition will only hold if there is evidence to suggest that C has committed a specific criminal offence (most commonly with M as a victim of that offence) and where infringing upon C's privacy by intercepting and reading C's e-mail is nec-

¹⁶ Restrictions on particular computing function are a common means of control. For example, computer users may require special access privileges in order to install programs onto the machines that they use, access to the world wide web may be constrained (such as by only allowing employees to access pages on the company's own web site), e-mail access may be restrained to allow the user to only send mail to a particular range of addresses, and so on.

essary in order to secure the legal evidence required by the courts. Again, if such a requirement were to be transformed from a moral requirement into a legal one, then this would correspond (at least in most Western jurisdictions such as the USA) with the current legal requirements for other infringements of privacy, such as the interception of postal mail or telephone calls.

The situation with regard to the infringement of privacy of those suspected in involvement in terrorist activities is somewhat different, since the infringement of privacy in such cases is usually justified by appeals to national security, rather than the protection of individual rights. Genuine concerns about national security licence the state to infringe upon rights in a much more significant manner than the protection of the rights of individual persons does, for the security of the state may be seen as a necessary condition for the existence and protection of any rights at all; social upheaval and anarchy are not conducive to the protection of rights. The more serious the threat to national security becomes, the more widely the state may be thought to be licensed to infringe upon the rights of those under its protection;¹⁷ a more serious threat to national security would thus permit the infringement of more fundamental rights than would a less serious threat, and would also license the state to infringe upon the rights of more of those persons under its protection than would a less serious threat. Even in cases where there is a direct and dire threat to national security there may still be infringements of rights that could not be justified.

Even in cases where national security is (or appears to be) threatened, rights cannot be infringed without moral justification; the infringement of rights must be necessary for the protection of rights and the good to be achieved, the protection of national security, must be proportional to the harm caused by the infringement of rights. Thus there must be a reasonable prospect that the infringement of rights in the name of protecting national security will actually achieve its object.

Therefore there are two main questions that need to be addressed before any state can claim to be justified, on the basis of an appeal to national security, in infringing the privacy of those under its protection by scanning e-mails in an attempt to intercept and read e-mail sent by terrorists. One, do these terrorist activities, actual or suspected, represent a

genuine threat to national security and two, if these activities do represent such a threat, is there a reasonable prospect of successfully preventing those activities by scanning e-mails in an attempt to intercept and read e-mail sent by terrorists?

In times past, only fairly direct military or espionage activity against a particular country was seen to be a threat to national security. However, in recent times many more activities, issues and problems have been seen to fall into this category, far more in fact, than can comfortably fit. Perhaps the main problem is that many people, especially politicians, tend to equate something not being in the national interest with it being an issue of national security. Issues of national security license the state to infringe rights, but issues that are simply not in the national interest do not, so the distinction between the two terms is particularly important in the context of this discussion.

One possible reason for the confusion between the terms is that events that occur that are not in the national interest may well involve issues of security, more narrowly defined. For example, suppose an embassy of country X, located (obviously) in a foreign country (Y), was to be the subject of an attack in the form of a suicide bombing, resulting in significant damage to the embassy and numerous casualties. While this is certainly not in the national interest of country X, it does not realistically count as a matter of national security, since the very existence of country X is in no way threatened by such an attack. Yet the attack may have only occurred because of a breach of security, such as allowing a vehicle to enter the embassy without proper authorization. Thus the bombing can correctly be termed an issue of security of one of the national buildings of country X (in this case the foreign embassy) while not actually being an issue of national security for country X.

In line with this distinction, I would argue that acts of terrorism and threatened acts of terrorism may involve security issues, but are not in fact issues of national security. While clearly extremely serious, even acts of terrorism such as those of September 11, involving the deaths of thousands of people, do not in themselves constitute a threat to the existence, as we know it, of a country such as the United States, nor would such attacks threaten the national security of a smaller and less powerful country. In order to truly count as an issue of national security, terrorist attacks would need to continue over such a long period of time, and with such intensity, that not merely the government, but the governmental system, was on the point of collapse.

While terrorist attacks in themselves may not be an issue of national security, in that acts of terrorism or

¹⁷ I use the somewhat cumbersome term 'those under the protection of the state' rather than the simpler terms 'citizens' or 'residents' since neither of these simpler terms really seem to capture the meaning that I wish to convey in this discussion.

threats of terrorism do not threaten to end the existence of the country as it currently exists, it is possible that a country's *response* to threats of terrorism might qualify as an issue of national security. If a country's response to threats of terrorist activity (or indeed to perceived threats of terrorist activity) is extreme enough, with massive infringements upon the rights of those under that country's protection in the name of terrorism prevention, then this may in itself threaten to end the existence of the country as it currently exists. For example, a liberal democracy that endorses dramatic infringements on liberty in the name of protecting the lives of those under its protection from perceived threats of terrorism may, in relatively short order, come to no longer deserve to be known as a liberal democracy.

With these points in mind, I would argue that no truly democratic state is justified, on the basis of an appeal to national security, in infringing upon the privacy of those under its protection by scanning e-mails in an attempt to intercept and reading e-mail sent by terrorists. Intercepting and reading the e-mail of those directly suspected of involvement in terrorist activities may be justified, but only under the same conditions as is necessary to justify the infringement of privacy of those involved in ordinary criminal offences.

Even if a state could claim that terrorism was a legitimate threat to national security, before that state could legitimately infringe upon the privacy of those under its protection by scanning e-mail in an attempt to intercept and read e-mail sent by terrorists, it would need to answer the question of whether such an attempt would have a reasonable prospect of successfully preventing those terrorist activities. Given the volume of e-mail sent and delivered every day, it would be impossible to actually read (or even glance over) every e-mail message sent, and so it would seem that the only reasonable method of scanning that e-mail in an attempt to intercept the e-mail sent by those engaged in terrorist activity would be to search all e-mail for specific terms likely to be used by terrorists in their communications. The chances of success in such an endeavour seem incredibly low, since once those involved in terrorist activities became aware that e-mail was being monitored (in whatever form) it seems likely that they would take the simple precaution of removing from their e-mail vocabulary terms likely to attract the attention of any e-mail scanning program designed to identify them. If the chances of success of such an e-mail scanning and interception program are low, then a government would not be justified in infringing upon the privacy of those under its protection by engaging in such activities, since the potential gain of

such government activities would not be proportional to the harm likely to be caused by this infringement of rights.

Conclusions

In discussing "reasonable expectations of privacy" in Internet transactions, Robert McArthur noted that e-mail was an insecure medium, and thus suggested that there was no right to privacy in e-mail correspondence. Among the reasons that he gave for holding this view were the fact that e-mail was commonly monitored by employers, and that innocent e-mails were often intercepted by FBI software that attempts to target the e-mails of suspected criminals. I hope that this paper has shown that McArthur's position, while plausible legally, is certainly not plausible morally. The arbitrary monitoring of employees' e-mail is an infringement of the employees' privacy, which fails to meet the three conditions necessary to justifiably infringe upon this right. The monitoring of e-mail by the FBI or other law enforcement agencies is also an infringement of the right to privacy, and is in fact specifically ruled out in the OHCHR comments regarding article 17 of the CCPR, which states that "the integrity and confidentiality of correspondence should be guaranteed". If e-mail was to be examined, then in order for this infringement of the right to privacy to be justified, a decision regarding the interference would have to be made on a case-by-case basis, which is all too clearly not the situation with current FBI monitoring of e-mail, and the infringement would have to meet the same conditions as other infringements of privacy in correspondence. Claims that threats to national security justify the scanning of e-mail in order to attempt to intercept the e-mail of those involved in terrorist activities also seem to fail to pass muster, since terrorist activities do not seem to be a genuine threat to national security, and even if they were, the chances of such a program succeeding are so small that the potential gain of such a program would be out of proportion to the harm caused by this widespread infringement of rights.

Acknowledgements

I would like to thank those who have given helpful comments on previous versions of this paper, especially John Weckert, Nikki Coleman, and an anonymous referee of this journal.

References

- L. Austin. Privacy and the Question of Technology. *Law and Philosophy*, 22(2): 119–166, 2003.
- L. Brown, (Ed). *The New Shorter Oxford English Dictionary*, 3rd edn. Clarendon Press, 1993.
- D. Charters. Electronic Monitoring and Privacy Issues in Business-Marketing: The Ethics of the DoubleClick Experience. *Journal of Business Ethics*, 35(4): 243–254, 2002.
- R. McArthur. Reasonable Expectations of Privacy. *Ethics and Information Technology*, 3(2): 123–128, 2001.
- H.J. McCloskey. Privacy and the Right to Privacy. *Philosophy*, 55(211): 17–38, 1980.
- S. Miller and J. Weckert. Privacy, the Workplace and the Internet. *Journal of Business Ethics*, 28(3): 255–265, 2000.
- M. Tunik, *Practices and Principles*. Princeton University Press, 1998.