



## Spyware – the ethics of covert software

Mathias Klang\*

*Department of Informatics, University of Göteborg, Box 620, 405 30 Göteborg, Sweden*  
*E-mail: klang@informatik.gu.se*

**Abstract.** Many computer users are happy to be oblivious of the workings within the machine and yet on some level it is important to know what is occurring therein. This paper discusses an unusual type of surveillance software which may be installed in many computers. The strange aspect of this software is that it has often been downloaded and installed by the user, but without her knowledge. The software is mainly designed to collect information about the user of the computer and relay this information back to the software manufacturer. The download, installation, data collection and data transfer all take place within the users own computer but very seldom with the users knowledge. It is the intention of this paper to describe the technology involved and thereafter discuss how this new technology is affecting the online privacy debate. The paper continues to discuss the basis for legitimacy of technology and also the current level of technological deterrents available. The paper concludes with a comparison of two approaches at resolving the current problem, via legislation or the market approach.

**Key words:** contract, freeware, integrity, internet marketing, law, privacy, spyware, surveillance

### Technology of spyware

Spyware can be defined as an agent technology or software, which is bundled into another piece of software. Spyware is most commonly bundled together with freeware which the user downloads and installs.<sup>1</sup> The main purpose of the spyware is to collect information, and send it to the information gatherer.

This paper takes a more limited view of spyware, focusing on the types of spyware which most users find objectionable. The reason for this is that most users would prefer, had they known what was happening, not to have spyware on their computers. This becomes an interesting ethical discussion since the spyware manufacturers tend to claim that the users have agreed to the spyware installed in their computers.

Since there is a difference of opinion as to whether or not the spyware has been installed with or without the users consent the actual installation becomes a critical issue. What is interesting to note is the fact

that spyware can be included with the users consent but without her knowledge. This is done by including spyware clauses in the end user licence agreement (EULA) which is displayed when the user begins installing the software and requires the user to agree to the terms before the software can be installed and used. The importance of contract law and the EULA will be discussed further below.

The discussion on spyware is made more complex due to the lack of an agreed upon definition; this flaw seems to stem from a lack of adequate consensus with which to reach a definition. The name alone is not universal, spyware is sometime known as scumware, parasite-ware, stealware or theftware and occasionally mixed up with computer trojans, viruses and worms. This paper uses the name spyware since it is the name, which is rapidly becoming the most accepted when describing the phenomenon.

Despite the lack of name consensus one can see certain attributes which ensure that a piece of software runs the risk of being accused of being spyware

1. The installation occurs without the explicit consent or knowledge of the user. Uniformed consent may be obtained via the EULA and the spyware is installed together with another piece of software which the user intentionally installs.
2. At a minimum the software collects personal data about the user or aids the collection of personal data about the user by creating a unique identifier.

---

\* Lecturer, University of Göteborg, Sweden. E-mail: klang@informatik.gu.se. With thanks to Andrew Murray, two anonymous reviewers and my Computer Ethics students. All errors remain my own.

<sup>1</sup> Spyware is not limited to free software, however it occurs there more often and this paper will focus on spyware in connection to free software.

3. The software uses the users Internet connection to send information to the information collector.

#### *Five examples of spyware*

Instead of attempting to describe the many different categories of software which is considered to be spyware, the paper will give five examples of such software. The purpose of these examples is not to provide an exhaustive list, nor is it to point a finger at manufacturers or software as being extreme in any way. These examples were chosen since they are reasonably well documented and therefore serve to give the reader an example of what the software and their manufacturers are attempting to do.

*Example 1.* Comet Systems Inc is the maker of Comet Cursor.<sup>2</sup> The software allows the user to change the colour and shape of the computer cursor. The shape can change into alternative shapes such as company logos when the user visits websites connected with the service. However the software also installs a GUID (global unique identifier) and is able to follow the users online browsing habits (Oakes, 1999). The effect of installing a GUID is that a computer can be identified by this number and this is the first stage in building a database of the computer users habits since the user is no longer anonymous.

*Example 2.* Sharman Networks, the creators of Kazaa Media Desktop bundled in software that connected the users to a secondary private network called Altnet which was operated by an affiliated company called Brilliant Digital<sup>3</sup> (Rojas, 2002). This system works in the same way as a distributed computing project<sup>4</sup> and takes advantage of the unused processing power in computers where it has been downloaded. According to the company the processing power is used to process the data gathered by the advertisers and to render video and 3-D animated advertisements. However, the network, using the software of unsuspecting Kazaa Media Desktop users without their knowledge could also be used to process large amounts of user profiles. A network such as this steals resources, and abuses the property of the

unsuspecting. It also raises security concerns since it allows additional access to the user's computer.

*Example 3.* The Napster like software called Audio Galaxy<sup>5</sup> also included the spyware program from a company called VX2<sup>6</sup>. The software recorded the user's movements and sent the data back to the database which was used for advertising purposes. The interesting issue about the Audio Galaxy case is that it also illustrates the temporary relationships and shifting loyalties of the different companies involved. These temporary relationships can be seen by the fact that Audio Galaxy bundled the VX2 software for a period of 34 days but no longer does so (Benner, 2002). These types of relationships will be discussed further below.

*Example 4.* Gator Corporation<sup>7</sup> is, according to their own website, a leader in online behavioural marketing. They create, maintain and distribute software called "Gator" which acts as a digital wallet. Gator also offers users the ability to store personal data and other information which is used to fill in online forms. The advantage to the user is that they no longer need to retype all the information when presented with an online form. This software is bundled with another, called "OfferCompanion". OfferCompanion has also been bundled with peer-to-peer software such as Kazaa<sup>8</sup>. The spyware, OfferCompanion, launches automatically when the user launches the browser program and when the user visits certain web sites the Gator Corporation transmit advertising pop-ups which appear on the screen in front of the desired page. The pop-ups prevent the legitimate page from being viewed in a manner which it was intended since the page is marred by advertising messages.

*Example 5.* An interesting case is the so-called self installing toolbar, this can be seen as a variation on the Comet Cursor. The Xupiter is an Internet Explorer toolbar program registered to a Hungarian company called Tempo Internet but has been traced to two Internet businessmen in California (Delio, 2003A). Some users have even claimed that it installs itself onto the computer after only visiting certain websites. The software changes the user's startup page to xupiter.com and redirects searches on Internet search engines to xupiter.com and changes security settings. This is important since changing security setting allows more information to be gathered about the computer user. The program attempts to download updates and in certain cases downloads and

<sup>2</sup> The software has been downloaded 152 million times according to information available on their website <http://www.cometsystems.com/>

<sup>3</sup> <http://www.brilliantdigital.com/>

<sup>4</sup> For examples of distributed computing see: Seti@home (<http://setiathome.ssl.berkeley.edu/>) which is working on the search for extra terrestrial intelligence or Drug Design Optimization Lab (<http://www.d2ol.com/>) which is the Rothberg Institute's attempt to use distributed computing to find cures for rare childhood diseases.

<sup>5</sup> <http://www.audiogalaxy.com/>

<sup>6</sup> <http://www.vx2.cc/>

<sup>7</sup> <http://www.gator.com/>

<sup>8</sup> <http://www.kazaa.com/>

launches other programs such as gambling games and causes pop-up advertising windows (Delio, 2003B).

Since many users are aware that spyware has been installed onto their computers they are not aware that they should uninstall the software. However, if the user is aware that software she installed included spyware it is seldom straightforward removing the spyware. Even if the software which carried the spyware onto the computer is removed it does not follow that the spyware is removed.

### Legality

The right to privacy is a fundamental right protected both in international conventions<sup>9</sup>, European Union directive<sup>10</sup> and national legislation<sup>11</sup>. As shown above, these types of software are capable of sophisticated surveillance and they have not been introduced into the computer in an open manner. The computer user is unaware of the surveillance and therefore continues to behave in an open uninhibited manner. Despite legal measures, the legal position of spyware is not clear and there are legal grounds for claiming that the software is legal. Therefore the paper will take its starting point in the examination of this claim since an accurate understanding of the legal position is beneficial to the total discussion of the software and its effects.

#### *How can this be legal?*

Since those who claim that the software is legal all tend to focus upon the EULA as a “silver bullet” in resolving the conflict then it is in the re-examination of contracts which we must base this first stage of the discussion. This paper will give a very brief review of the end user licence agreement and its place within contract law.

Contract law (cf. Furmston, 1996) is taught to most law students in the form of a simplified mythical situation where two people meet, lets call them A and B. In the meeting, A makes B an offer. In our sce-

nario A offers B the latest widget in technology for the price of 10 €. B, after careful thought, agrees to the offer and the contract is formed. Formation means that legally enforceable obligations have been created. The point of formation is usually symbolically celebrated by some ceremony of, e.g., handshakes, nods or scribbling names on paper. This ceremonial aspect is an important issue in producing evidence that a contract actually has been formed but binding obligations can be formed without the ceremonial aspect. The whole basis of liberal contract theory is the meeting and agreement of the wills of competent individuals. Depending upon the rules in the particular jurisdiction legally enforceable obligations are created within this meeting of wills. The efficiency of contract as a legal fiction explaining the creation of binding obligations has often led to the search for the competent wills in situations, such as, when B enters a bus, or wanders around the supermarket placing items into a shopping cart. However adequately everyday transactions can be explained by the simplification of contract theory the practice of buying software has created an interesting challenge to basic contract theory.

#### *Shrinkwrap and clickwrap*

If B wishes to buy some software from her local computer store the contract is completed when she hands over her money and receives the box, containing the disk, containing the software. However, an interesting thing occurs when B gets home and tears open the *shrinkwrap*, opens the box and begins to install the software. Out of the box spills lots of pieces of paper with small text in unfriendly complex language. These amendments and additions to the contract are known as *shrinkwrap* contracts (Rowland and McDonald, 2000). B does not need these to install the software so she proceeds to enter the disk into her computer. On the screen she receives many options all of which she must decide whether or not to agree to. One such text which usually appears in the beginning of the installation demands that she agree to a larger text to be able to continue. This is known as a *clickwrap* (Arne and Bosse, 2003) and is an evolution of the *shrinkwrap* and has the power to regulate the contract which B has already entered into. Usually the *clickwrap* is seen to be more binding than the *shrinkwrap* since it requires positive actions from the user. Naturally since she is used to computers and software she quickly clicks her way through the options without reading all the text – she wants to use the software not read about it. It was the same when she bought her car, she did not read the manual before she started to drive.

<sup>9</sup> See for example Article 12 of the Universal Declaration of Human Rights, Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948, or Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

<sup>10</sup> Most importantly Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

<sup>11</sup> For example the United Kingdom Data Protection Act of 1998.

Contract theory has seen a need for the use of standard terms and has adopted the concept of contract d'adhesion which allows contract terms, written by one contracting party, to be included into the contract even if the other contracting party has little or no possibility to affect the contract terms. This is usually done in the form of standard contract clauses. The contract is concluded in the shop and while in most cases a contract cannot be altered without agreement after it has been concluded the contract d'adhesion is part of the contract despite that the purchaser may not be aware of the terms until the papers that fall out of the box. The text which B does not read while clicking at the "I Agree" button is binding under the same principle. So any terms within these documents have the ability to limit B's use of the software.

The situation is the same if B had chosen to download free software from the Internet. Supposing B had downloaded Kazaa to be able to share music files with all her friends. The text that precedes the installation of the program is binding. The fact that she does not read it, or if she does read it but cannot understand it does not alter the fact that it is binding. So if Kazaa has written that they intend to collect data and send it to the company for marketing purposes B cannot do anything about that – except not install the program.

### *Contract theory revisited*

Naturally the theory of contracts is a simplification used in education to teach students about the basics of law. It is not intended to be the solution or total description of reality. Nor are the challenges created by technology the only situations where flaws in the simplified model of contract theory become more evident. In any large business process there may always be difficulties in discerning when a contract was entered into and what the content of the contract was. To solve this dilemma the myth has been amended with the theories of the *shrinkwrap* and *clickwrap* licences as described briefly above. The courts have understood the necessity of these licenses and have reinforced their legality and power over the users.

At first glance the courts acceptance of these licences may seem unduly harsh. The writer of the contract is at an advantage since they have the time to create a contract which best suits their needs. Additionally the advantage is enhanced by the situation that most consumers are not legally trained and, should they read the contract, may not see the disadvantages the contract places them in. However, this situation is true of many contractual situations. Few of us bother to read the contractual terms when renting a video film or a car. There is a great deal of

trust placed in the fairness of the overall system, additionally we see many other people renting cars and video films without problem and therefore we assume the same will be true for us. The courts acceptance of the standard licence is based upon the needs of commerce; the courts acceptance of the contract d'adhesion contract is based upon the knowledge that most consumers are not going to read the contractual terms which underpin every train or airplane ticket. In most cases the contracts are not unduly harsh since they have developed over time to suit the contractual situation and the courts acceptance of them is based upon commercial necessity.

It is however, important to note that this is not the same as saying that the *shrink/clickwrap* licence is enforceable in all situations. There are contract situations where the contracts are not enforced by the courts. In Scandinavian contract law the courts have the power to amend contracts which are unduly harsh on one of the contracting parties. This situation typically occurs when the drafter of the contract has used techniques, such as language and layout, to obfuscate the terms of the contract. Under common law the question may be one of misrepresentation since the spyware is most commonly bundled into another software product and it is not the intention of the user to download the spyware.

Under U.K. law, in the case of *Spurling v Bradshaw*<sup>12</sup>, Lord Denning stated that the use of sweeping exclusion clauses it was necessary to draw the contracting parties' attention to such cases it required something startling. Denning suggested printing in red ink with a red hand pointing to it or something similarly striking which could not be missed. Argument such as this show that the existence of contract is not enough to legitimize any and all content. The red hand argument can be extended to be used against the bundling of spyware, especially since the spyware interferes with the peaceful enjoyment of the users' property vis-à-vis the browser and the personal computer.

Today we tend to follow what is often referred to as the liberal contract theory and see contract law as an instrument for enforcing promises (cf. Gordley, 1991). This view is tempered with the fact that the contract is seen as an agreement where the wills of the contracting parties are in accord. If we are to view contract law as an enforcement mechanism then the law tends to be weighted in favour of the EULA since this is, at first glance, the contract. However, it is important to remember that the contract should represent an agreement and as such the question of what the parties knew they were agreeing to is vital to

<sup>12</sup> *Spurling (J) Ltd v Bradshaw* (1956), CA.

the actions of the courts in attempting to decide upon these issues.

### **Spyware business model**

It is important for software manufacturers to spread their software and also to obtain financing for their work. There is a culture of not paying for goods and services online. Many, if not most, users have come to expect and demand that information, software and services are available at no cost. The traditions of no cost software have been compared with tribal gift economies (cf. Barbook, 1998) since there is a tendency to help, share and barter with intellectual property.

The tradition of no cost software and information has developed into the copyright conflicts taking place today. Entertainment files are being transferred over peer-to-peer networks despite the fact that they are copyrighted. The entertainment industry is attempting to regain control over their traditional marketplaces by persecuting those who aid copyright infringement via technical means. This situation has led many users to attempt to legitimise their infringing actions and call for the demise or radical change of copyright legislation. In discussing the legitimacy of infringing software copyright Nissenbaum (1995) argues both with consequential and deontological arguments that there are some specific cases where infringement is morally permissible. However, whether or not the action of copyright infringement can be justified or not the situation is such that many do not feel that they are doing anything wrong in violating another's copyright or at least they are not deterred by any such emotion.

This desire for free software has led to a loss of revenue and a need for software manufacturers to find alternative incomes. Enter the parasite economy (Cave, 2001). To obtain income for their products the popular software can act as a host for other software, carrying it into the computers of users, see Example 3. Popular free software can create channels of revenue by offering themselves as carriers of bundled software. The spyware (or indeed any other software) which travels with the free software pays a minimal fee per download for the service. The total cost paid therefore naturally depends upon the popularity of the downloaded software.

The creators of the downloaded software claim that their actions are both legal and driven from economic necessity. Users demand free software, software manufacturers need funding to create more competitive software and marketers need to reach potential customers. Since the users obtain free software, software houses obtain a new source of income

and the marketers increase their reach, then one might argue that there should not be any discussion on the evils of spyware. This is, however, an oversimplification of the situation.

### **Privacy theory**

Despite the fundamentals of contract law and despite the legality of the business models there appears a level of discontent among those afflicted by the technology. These users are not pacified by the legality of the scheme. They do not agree with the implementation of technology in this clandestine manner for the purposes of invasion of their experienced integrity. In this we can see a connection to the arguments of Habermas (1989) on the relationship between technology and power. This relationship exists in a state of constant evolution and the important issue to be discussed is one of legitimacy. The problem of legitimacy arises when the technology is driven forward in such a way as to exclude a number of users from the socio-legal discourse. Since it can be claimed that it is one of the many roles of law to legitimise actions and create a level of understanding between the citizens and those in power it is important that those who are affected by the technology, and the infrastructure it creates, have the opportunity to partake in an open discussion. When the law is used in such a manner as to silence debate by legitimising actions which are unwelcome to the users then one can claim that the law has been used as a pacifier and alienated the users from partaking in the debate.

Those who are discontented and wish to argue from another point of view tend to evoke the arguments of the privacy and integrity debate. Lacking the international consensus of contract law these users have to argue from a rights based position which, as Bobbio (2001) states is a position of weakness since they first have to prove the existence of their position and then argue that theirs is the position more worthy of concern. Online privacy has been discussed for a long time and in many different ways. The most common legal discussion tends to be whether or not there is, or there should be, a right to privacy. If this can be answered in the affirmative the question then becomes one of degree i.e., where do the limits of privacy stand?

In Europe this question has received considerable help in recent years due to the growth of the European Union which requires the incorporation of the European human rights convention.<sup>13</sup> Prior to the

<sup>13</sup> Convention for the Protection of Human Rights and Fundamental Freedoms – Rome 1950.

incorporation of the convention into the national legislation of the member states the discussion centred on the creation of a right as opposed to a discussion of positive law. After the incorporation the main thrust of the legal discussion became a positivistic discussion on what should be included in a right to privacy.

The debate on privacy has developed over time<sup>14</sup> and has always stood in relation to the level of technology of the day. The seminal Brandeis and Warren (1890) article on privacy was very much a result of the technology of the time. They feared the continued development of the small portable camera which could be handled by the amateur (Kern, 1983). The concept of privacy can only be placed in relation to the ability of that privacy to be invaded.

Unfortunately the discussions have for a long time focused on either the voluntary submission of data or the use of cookies. Software such as spyware has not been discussed and its appearance and proliferation requires urgent action on the part of the users, software manufacturers and legislators.

In the modern privacy debate an influential work is Foucault's (1979) interpretation of Bentham's (cf. 1995) Panopticon. The Panopticon was a prison in which the prisoners could never be sure whether or not they were being observed at any given time. Since there was always the risk that they were being observed the prisoners were forced to behave as if they were being watched. This, according to Foucault, was the internalisation of supervision. The entailed exercise of self-supervision due to the fact that there always was the risk of being caught. As such, privacy was never available. The awareness of this type of constant supervision, or even the threat of this type of constant supervision leads the subject to behave differently. The subject must behave in a manner consistent to the fact that she may be observed at any time. This knowledge has the effect of changing the behaviour of the subject in a manner which is incompatible with the concept of human freedom.

Technological advances have brought about the change in the concept of privacy and many would claim that the new technology represents a panopticon of sorts (cf. Johnson, 2001). While there may be certain elements of truth in this type of discussion this is not the case with spyware. This is due to the fact that the user is unaware that she may be watched and this causes her to behave in a natural and uninhibited

manner. This means that tools of supervision installed in the computer through bundled software is more serious than the panopticon metaphor. In the panopticon the user is aware that she is being watched and has the choice to behave accordingly but this crucial difference is, in the case of spyware, that the user has no knowledge that her actions may be observed.

Leaving the panopticon metaphor leaves us more able to understand the need for an increased discussion in the privacy debate. This new technology represents a new challenge to the level of privacy we can expect. The amount of privacy we can reasonably expect is "...a function of the practices and laws of our society and underlying normative principles." (McArthur, 2001). Unfortunately the open public debate on the integrity depriving aspects of spyware has not yet developed enough which has the effect of depriving the law from a worthy basis of discussion and not developing the underlying principles to be able to meet this new challenge. In the face of this vacuum courts may be tempted to fall back upon a familiar pattern of discussion centred on contract law and this leaves the user in a lesser position.

### The market approach

While attempting to remove the nefarious software may be a complex affair there are software programs which may be useful. Software such as Ad-aware created by Lavasoft<sup>15</sup> and Spybot created by PepiMK Software<sup>16</sup> both can be downloaded free and be used to find and remove the unwanted software.

These programs have however given rise to an interesting dilemma. They are not all too open about their methods in defining what spyware is and as such have a large amount of political power in their ability to blacklist programs. Comet Systems Inc claim that they have been unfairly targeted by Lavasoft and their business has suffered because of it (Miles, 2002). The potential of anti-spyware companies to damage the legitimate business interests is a serious threat. Marketing companies claim that they have a right to market their products, software companies need revenues from marketers to be able to provide free software. The whole process is legitimised by contract law. The question therefore may be to what extent the anti-spyware companies are, or should be, liable for their activities.

It is therefore important for the creators of anti-spyware programs to be open about their methodol-

<sup>14</sup> For a good overview of the developments of law and Privacy see Wong, R. (2004) "Privacy: Charting its Developments & Prospects" in Klang and Murray (eds) *Human Rights in the Digital Age*, Cavendish Publishing.

<sup>15</sup> <http://www.lavasoft.de/>

<sup>16</sup> <http://spybot.eon.net.au/>

ogy and their choice of programs which their software removes. The most popular anti-spyware program is reputedly overly covert and silent about their business practice which makes any discussion on openness difficult.

For those who are technically adept the whole problem of spyware is an issue of lesser importance but the majority of technology users are happily unaware of how their technology works or how to correct it if it fails to work. This is the group which needs anti-spyware software. This group is usually unaware of the choices made by the programmers of which software to define as spyware and which not to include in this category.

Anti-spyware software, once established, creates for itself the role of gatekeeper since it has the ability to choose which software is to remain on the users computers and which is not. For software developers therefore, the anti-spyware software becomes another barrier which must be respected. Some software developers have attempted to open discussions on the powerful position attained by anti-spyware companies in relation to deciding which advertising is allowed and which is not (McWilliams, 2002). Another interesting reaction can be seen in the attempts of the software companies to fight back against the anti-spyware programs. The Radlight<sup>17</sup> video playing software, once installed, attempted to remove or disable the Lavasofts Ad-aware program. This action was legitimised in the EULA

“...You are not allowed to use any third party program (e.g. Ad-aware) to uninstall application bundled with RadLight. Such programs will be removed. If you want to uninstall them, you may do so via Add/Remove in Windows’ Control Panel.”

The EULA text has since been amended with a text describing which types of third party software is bundled into the program and also the fact that it will create a GUID for the computer. It no longer claims the right to remove software installed in the computer. It does however openly explain that the software will be used for marketing purposes. In a text few of their customers will ever read.

### The legislative approach

The concerned citizen therefore turns to the legislator for solutions and it is heartening to note that while this is a new phenomenon the legislators have been active even on this issue. This activity is an important

starting point in a long process for the development of an equitable legislation which has the needs of all the actors in mind.

### *The American legal reaction*

The “Spyware Control and Privacy Protection Act of 2001” (hereafter The Act) intends to control spyware. The Act requires that manufacturers notify consumers when a product includes this capability, what types of information could be collected, and how to disable it. More importantly The Act makes it illegal for the programs to transmit user information back to the manufacturers unless the user enables this function and the user has given the collector access to the information. There are exceptions for validating authorized software users, providing technical support, or legal monitoring of computer activity by employers.

However, The Act has been attacked for not being consumer friendly since despite its good intentions it does not go far enough in controlling the actions of the spyware producers. The Act follows the ideas set out in the European Data Protection Directive<sup>18</sup> (hereafter The Directive) in that it divides personal data into two categories: sensitive and non-sensitive. Sensitive data concerns personal data surrounding the data subject’s finances, medical history, sexual orientation, lifestyle, political affiliation and race. This data cannot be collected or used without the data subjects consent.

The non-sensitive data, however, is everything else and all information which can be inferred from that information. This includes any and all actions which the software can record from the web and the conclusions which can be drawn from this data. This non-sensitive data can be collected, processed and sold without the data subjects consent. While at first glance this seems to be a reasonable starting point, there is one major drawback. If you collect or record much, or all, of the information a user obtains via the Internet you can make several inferences about the users which pertains to her sensitive data and therefore the division of sensitive and non-sensitive division is no longer useful.

### *The European legal reaction*

The Directive has been enacted in all member states and can be used to criminalise the actions spyware since the Act requires that the consent of the user be

<sup>17</sup> <http://www.radlight.net>

<sup>18</sup> Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

obtained prior to collection of personal data. While these legislative tools are effective they have been unable to deal with the Internet based privacy invasions due in part to the fact that the techniques required to monitor and enforce are beyond the power of single, or groups, of states.

The member states of the European Union have a strong level of privacy legislation which enables a level of control of the companies dealing with personal data in their businesses. Unfortunately those dealing in personal data collection through spyware are notoriously difficult to locate and tend to shy away from establishing themselves in states where there is a strong privacy enhancing legislation.

Another problem with all legislation is that the concept of spyware, and user consent, are vague, especially in light of the licence agreements which have been incorporated into the original contract. There may also exist another argument against the use of the licence agreement as a method of legitimising the actions of spyware and this is the Convention for the Protection of Human Rights and Fundamental Freedoms which has been incorporated into the legislation of the member states. This convention and the legislation is concerned with the defence of privacy and as such can be used against the manufacturers of spyware.

The weakness of the legislative approach is that it must struggle to obtain a balance of the needs and wants of the different groups in society. After this balanced approach there is the difficulty of enforcing legislation which is limited to nation states in an environment which no longer considers these boundaries to be relevant. It is not that the courts do not have the competence or jurisdiction to rule in a case but rather the question as to whom is behind the software and which corporate entities or private citizens are to be considered to be responsible for the software.

### **The ethics of spyware**

The ethical viewpoint of the spyware maker can be summarised by the Friedman's (1970) controversial view of the duty of the corporation to maximise profits and benefit the shareholder. This deontological approach however is opposed by the other rule based imperative not to spy upon or cause harm to others. The question of how to resolve this conflict of ethical rules by applying the Kantian humanity principle of not treating people as a means to an end but rather as ends in themselves. If we were to apply this final Kantian principle we can arrive at the conclusion that spyware constitutes a breach of ethical conduct. However if we were to attempt to apply

a utilitarian analysis of the situation the ethics of the actors becomes less clear. The inclusion of spyware in free software could be viewed as a necessary evil and the creation and supply of free software creates more happiness or utility than the evil generated. This argument is effectively reinforced by the fact that there is software which can be used to protect the individual from the harms of software. However, for this argument to be effective the person downloading spyware must be aware both of the consequences of her actions and the availability of counter-measures.

Since it is difficult to clearly state that spyware is inherently immoral, the position of other actors who provide the infrastructure with which the software is spread (for example those who bundle spyware with other software) is even more difficult to ascertain. Despite the difficulties it is possible to state that spyware is often an unwelcome addition to the computer and from the growing popularity anti-spyware software it is possible to surmise that many computer users believe spyware to be wrong.

### **Market vs. legislation solutions**

One interesting question which the spyware problem opens up is the question of which is the best method for combating these types of issues. The problem of spyware is relatively new and relatively unknown outside technical forums or privacy forums. While many of these forums may agree that the problem is growing, it remains difficult to see which solutions should be applied to the problem.

The use of anti-spyware software is at best a market solution which requires from the users knowledge of the problem and, at least, a working knowledge of where to find the solutions and how to install and use them. The level of information required by the market is therefore reasonably high, especially considering the fact that most Internet users have never even heard of spyware and, even if they had, may not realise the importance of defending their privacy. If the users are aware of the problem, and want to resolve it, a new question arises and this is one of understanding which software is the best for their problems. This stage is crucial since the users can download inadequate anti-spyware software or, in the worst case scenario, even more spyware.

Attempting a regulatory approach takes time and a great deal of concerted effort. Habermas argues (1984, 1989) that societies are the base for a multitude of pluralistic opinions but only a few ever come to the forefront of the public debate. In ensuring that the debate is maintained in an open and that the rules are created in a transparent method it is important that

the basis for rules are discussed by those who are effected by them. It is also important however to note in this context that all rules should be held under constant debate (McCormick, 1997). Rules should not exist in a closed space but must exist in the open under public scrutiny to avoid the creation of a representative elite whose interpretations of societies needs, or an illusion of public good, control what is developed as a social balance.

The user is left therefore with problems on all sides and must therefore attempt a pragmatic approach to the problem. Not using information technology is not a viable option but what is important is that an effort is made by the users to keep up to date with the state of privacy, both technical and legislative. The user must be prepared to use both technical means to protect her own data while participating in a public discourse on the importance of better data legislation. As has already been shown the nation state is not capable of meeting all the ills on the Internet and protecting its citizens from them but it is important that the nation state creates an environment where the individual has the ability to find information, make informed decisions concerning her privacy and, if so desired, implement technical countermeasures to protect the level of privacy required.

## Conclusion

Privacy has once again become the price computer users pay for their use of the information technology infrastructure. This time the threat comes from software bundled into free software, the problem is that the price the user pays is not one which is discussed or declared openly. The user is therefore not able to enter into an agreement on equal grounds or attempt to negotiate to achieve a better bargain. Contract law is in this scenario pushed to the limits and used as a legitimising factor for unethical business practices.

There are alternatives for the user. She can naturally choose not to use free software but this choice requires knowledge of the integrity threatening software within the free software. Also the choice no to use free software has economic effects and may create barriers to active participation in the information technology infrastructure. There are also possibilities for the user to attempt to eradicate the unwanted software installed into the computer. These types of solution require an awareness of the problem and a certain level of knowledge on how to find, download, install and run the necessary software. An important issue with these market based solutions is that their fairness and objectivity have been marred by accusations of injustice and unfair treatment.

On the legislative side we once again see an example of legislation struggling to enforce local ideas under fire from a global (or a-national) infrastructure. This is becoming a familiar pattern when the national or regional legislation attempts to deal with Internet based technology. There is no solution to this aspect of the problem other than international legal consensus which is very hard to achieve, implement and enforce.

The disruptive effects of technology upon a social balance created over time can have the subtle effect of changing that balance which was created at a prior technological balance. Technological advance demands a renewed discussion on its effects upon the users in society and on the gradual effects of technology on society. This is especially true since a market approach to resolving the issue requires that more information is made available to those who are effected by the problem. Without this information they will be unable to take a stand on whether they desire to protect themselves, and if so, in which manner.

An additional reason for the need for more public debate amongst those concerned is that they are themselves responsible for achieve a re-balancing of the socio-technical regulation. Without information and debate the process of establishing a balance between the effects of technology and the needs of society will cease to be forceful and any meaningful effects such a debate can create will be lost.

## References

- P.H. Arne and M.M. Bosse. Overview of Clickwrap Agreements, *Practising Law Institute*, January–March, 2003.
- R. Barbook. The Hi-Tech Gift Economy, *First Monday*, Volume 3 Number 12–December 7th. 1998, [http://www.firstmonday.dk/issues/issue3\\_12/barbrook/](http://www.firstmonday.dk/issues/issue3_12/barbrook/)
- J. Benner. Spyware in a Galaxy Near You. *Wired News* 24 January, 2002, <http://www.wired.com/news/technology/0,1282,49960,00.html>
- J. Bentham. *The Panopticon Writings*. M. Bozovic. editor Verso Books, 1995.
- N. Bobbio. *Rättigheternas Epok*. Fovet W. (translator from original L'età dei diritti) Daidalos Publishing, 2001.
- D. Cave. The Parasite Economy, August 02, 2001, *Salon.com* [http://archive.salon.com/tech/feature/2001/08/02/parasite\\_capital/](http://archive.salon.com/tech/feature/2001/08/02/parasite_capital/)
- M. Delio. Xupiter Mongers Deal Spam, Scams, *Wired News* 5 February, 2003A, <http://www.wired.com/news/infrastructure/0,1377,57553,00.html>
- M. Delio. Sneaky Toolbar Hijacks Browsers, *Wired News* 30 January, 2003B, <http://www.wired.com/news/infrastructure/0,1377,57467,00.html>
- M. Foucault. *Discipline & Punish: The birth of the prison*. Vintage Books, New York, 1979.

- M. Friedman, (1970) The Social Responsibility of Business Is to Increase Its Profits. New York Times Magazine (1 September 1970). Reprinted in T. Beauchamp, and N. Bowie. *Ethical Theory and Business*, Prentice-Hall, Englewood Cliffs, N.J., 1993.
- M.P. Furmston. *Cheshire, Fifoot & Furmston's Law of Contract*. Butterworths, London. 1996.
- P. Gordley. *The Philosophical Origins of the Modern Contract. Doctrine*. Clarendon Press, Oxford, 1991.
- J. Habermas. *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. B. Thomas (trans), MIT Press, Cambridge, MA, 1989.
- I. Kant. *Grounding for the Metaphysics of Morals*. H.J. Paton (trans), New York Harper Torchbooks, 1964.
- S. Kern. *The Culture of Time and Space 1880-1918*, Harvard Univ. Press, Cambridge, MA, 1983.
- R.L. McArthur. Reasonable Expectations of Privacy. *Ethics and Information Technology*, 3: 123–128, 2001.
- J. McCormick. Habermas's Discourse Theory of Law: Bridging Anglo-American and Continental Legal Traditions, *The Modern Law Review*, 60, 1997.
- B. McWilliams. Cursor Company's Conduct Cursed, *Wired News* 6 June, 2002, <http://www.wired.com/news/privacy/0,1848,52985,00.html>
- S. Miles. Ad-Aware Maker LavaSoft Frustrates Internet Advertisers, *The Wall Street Journal Online*, 2002, <http://online.wsj.com/article/0,,SB1035830...231,djm,00.html>
- H. Nissenbaum. Should I Copy My Neighbor's Software? In D. Johnson and H. Nissenbaum, editions, *Computers, Ethics, and Social Responsibility*, Prentice-Hall, pp. 201–213. NJ, 1995.
- C. Oakes. Mouse Pointer Records Clicks, *Wired News* 30 November, 1999, <http://www.wired.com/news/technology/0,1282,32788,00.html>
- P. Rojas. Kazaa Lite no Spyware aftertaste, *Wired News* 18 April, 2002, <http://www.wired.com/news/mp3/0,1285,51916,00.html>
- D. Rowland and E. McDonald. *Information Technology Law*, 2nd ed. Cavendish Publishing, 2000.
- S. Warren and L.D. Brandeis. The Right to Privacy, *Harvard Law Review*, 6(5) December 15. 1890.
- R. Wong. Privacy: Charting its Developments & Prospects. In Klang & Murray editions, *Human Rights in the Digital Age*, Cavendish Publishing, 2004.