

Spyware: Paying for Software with our Privacy

MATHIAS KLANG

ABSTRACT This paper deals with the privacy issues related to the computer software that has come to be known as spyware. The privacy concerns have begun to be debated online and in trade media. Unfortunately, as we shall see, the concerns of the legislators and courts have not been focused on the privacy concerns of the individual but rather upon the economic interests connected with online assets and marketing. This paper will begin with the issue of defining spyware, and then move on to look at the manner in which privacy legislation can be circumvented by contract. This is followed by a brief look at the type of court activity taking place. The paper will then look at the basis for any claim to privacy and how it can be related to spyware. This is followed by a look at the weak attempts of legislation and a concluding discussion.

Introduction to Spyware

Spyware has been used in most cases for gathering information and also for providing new marketing channels. However, while this may seem to be a harmless activity, spyware has also been used to change the shape of the users' computer cursor,¹ and to install global unique identifiers (GUID)² for the purpose of making the tracking of an individual's online behaviour more efficient. Spyware has also been used to install software to make the afflicted computers part of a distributed computing network.³

One of the most crucial aspects of spyware is its lack of proper definition. There seems to be a lack of adequate consensus 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 viruses and worms. This paper uses the name spyware since it is the name most commonly used to describe the phenomenon.

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

Correspondence: Mathias Klang, Dept of Informatics, University of Göteborg, Box 620, 405 30 Göteborg, Sweden E-mail: klang@informatik.gu.se.

- 1 The installation occurs without the explicit knowledge or consent of the user. Uniformed consent may be obtained via the EULA and the spyware is installed together with another piece of software that 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.
- 3 The software uses the user's Internet connection to send the gathered information to an information database.
- 4 The information is most commonly used for marketing purposes.

Obviously point 1 is the most important point in this list. There are other software programs that rely heavily on user information and marketing for their success (often referred to as adware) but the main difference lies in the information given to the computer user prior to the software's installation and use. The origins of spyware and the name itself are in some dispute but according to the more established Internet beliefs the phenomenon was discovered, reported and achieved popular discussion in 1999–2000 when users became aware of software, that they had not installed, was silently attempting to use their Internet connection to transfer data.

An important additional aspect of spyware is the difficulty connected with its removal. Spyware rarely appears in the computers uninstall list and even if it can be located removal of parts of the software can sometimes affect the more traditional workings of the computer. Other complaints connected with the removal of spyware have been the issue that if not totally removed the spyware has an ability to re-install itself.

The Spy Software

It is important for software manufacturers to spread their software and also to obtain financing for their work. There is, however, 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 economies⁴ since there is a tendency to help, share and barter with intellectual property.

Popular free software can create channels of revenue by offering themselves as carriers of bundled software.⁵ The spyware (or indeed any other software) that travels with the free software pays a minimal fee per download for the service. This has been called the parasite economy.⁶ 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.

There are several types of software that may be used openly or covertly to spy upon computer users. Software that is capable of recording keystrokes, surf habits and screen images is common enough and marketed openly. However this paper intends to focus on a small specific group of software that is also used to record the habits of computer users but in a more hidden manner. This software has come to be called spyware. To be classed as spyware the software must usually fulfil two requirements. First, it must be able to either aid in, or be responsible for, the surveillance of the computer user and, second, it must be installed into the computer without openly declaring its purposes. Spyware is most

commonly bundled together with freeware that the user downloads and installs. The main purpose of the spyware is to collect information and send it to the information gatherer.

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.

Legitimacy through Contract

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. An important issue to discuss therefore is what position software such as this has in the legal system. There are valid claims being made that this is all legal and above board. Those making the claims can be found in both camps of the pro and contra spyware battle. 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.

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 upon 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 law⁷ 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 scenario A offers B the latest widget in technology for the price of €10.00. 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 fantastical ceremony of handshakes, nods or scribbling names on paper. This ceremonial aspect is an important issue in producing evidence and creating moral commitment to the agreement.

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.⁸ 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 that 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 clickwrap⁹ and is an evolution of the shrinkwrap and has the power to regulate the contract that 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.

Unfortunately it is about here that the law professor's myth gets into serious trouble. The contract is concluded in the store and in most cases a contract cannot be altered, without agreement, after it has been concluded. This is considered to be unfair. Despite this the papers that fall out of the box are in some way magically transformed to being part of the contract. The text that B does not read while clicking at the 'I Agree' button is actually binding. So any terms within these documents have the ability to limit B's use of the software.

Contract Theory Revisited

Naturally the myth 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 the myth is flawed or even completely fails. 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.

It is however, important to note that this is not the same as saying that the shrink/click-wrap 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 that 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 UK law, in the case of *Spurling v Bradshaw*,¹⁰ Lord Denning stated that the use of sweeping exclusion clauses was necessary and, in order 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 that could not be missed. Arguments such as these show that the existence of a contract is not enough to legitimize any and all content. The red hand argument can be extended and 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.¹¹ 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 the actions of the courts in attempting to decide upon these issues.

Spyware in Court

The courts have already been made aware of spyware, however the issues that have been raised have not been concerned with the privacy aspects of the software and are therefore not helpful to understanding where the legal reasoning should be developing within this field. However, it is interesting to note that the development of spyware related case law is moving ahead in relation to trademark and copyright infringement. While this is helpful for companies hoping to maintain control over their online assets the connection of spyware to trademark and copyright tends to relegate the importance of privacy concerns to a lesser place.

Gator Corporation is, according to its 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 that 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. 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 in which it was intended since the page is marred by advertising messages. Removing OfferCompanion is no straightforward affair, the removal of the programs with which it was delivered does not remove the spyware.

The Gator spyware prompted 16 online news-publishing organizations to file a lawsuit¹² against Gator claiming trademark and copyright infringement, and unfair enrichment by freeloading on the reputation of the established sites. The court granted a preliminary injunction in July 2002 preventing Gator from causing pop-up advertising on the Plaintiffs websites. In February 2003 the case was settled out of court but unfortunately for the development of jurisprudence in this area the settlement is covered by confidentiality.

The courts have, however, not been consistent. In June 2003 the court¹³ granted WhenU's motion to dismiss charges of trademark infringement, unfair competition and copyright infringement. With this the company U-Haul could not prevent WhenU.com from delivering competitors' ads to visitors to U-Haul's site.

There are more cases pending, both against Gator Corporation and others. The cases revolve around the presentation of websites and the right of corporations to be able to protect their intellectual assets and not have their users be bothered by pop-up advertising. Unfortunately these types of case are not concerned with the privacy concerns of the individual user and therefore the courts have not been asked to develop legal arguments within the privacy field.

The Privacy Dimension

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. 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 Bobbio¹⁴ 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, ie where do the limits of privacy stand?

In Europe this question has received considerable help in recent years because of the growth of the European Union, which requires the incorporation of the European human rights convention.¹⁵ Prior to the 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 and has always stood in relation to the level of technology of the day. The seminal Brandies and Warren article¹⁶ on privacy was very much a result of the technology of the time. They feared the continued development of the small portable camera that could be handled by the amateur.¹⁷ 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.

For a long time now the computer privacy debate has been trapped in the 'Panopticon'. The metaphor of Bentham's Panopticon has travelled via Foucault¹⁸ into the foundations of the computer privacy discussion. For Bentham¹⁹ the Panopticon was both a business proposal and the ideal prison where the prisoners were kept in control by the knowledge that they were being watched at any time. As such, privacy was never available. 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 that is incompatible with the concept of human freedom. Foucault²⁰ used Bentham's prison as a metaphor. Those under the eye of the Panopticon internalized their own regulation and behaved accordingly. The theory is that the knowledge, suspicion or fear of being watched changes the behaviour of the person being watched. This change is non-voluntary and therefore it is an exercise of power on the part of the watcher. Herein lies a weakness with the Panopticon metaphor. What happens when the behavioural change is voluntary? Can the Panopticon be acceptable if it is a part of an agreement, or better still, a contract? If this is so then privacy is a right that may be bargained with.

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.²¹ 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 are 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 missing in the case of spyware where 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'.²² 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 are tempted to fall back upon a familiar pattern of discussion centred on contract law and this leaves the user in a weaker position.

Despite its established position, the right of privacy has not been actively defended and reinforced by political and economic initiatives. Unfortunately, it is rarely enough to create or establish a right by law or international convention. Without the political and economic will to protect the right it will be unable to establish itself at a level that the public can rely. Without a clearer political and economic will the regulation of privacy will continue to be symbolically valuable but not strong enough to create awareness among the afflicted that there is recourse in the law. As it stands today the right to privacy is often discussed but cannot be effectively used by individuals, with the aid of the state, to ensure that their rights are protected above the economic interests of Internet marketers.

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 that 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 Directive²³ (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 that can be inferred from that information. This includes any and all actions that the software can record from the web and the conclusions that can be drawn from this data. This non-sensitive data can be collected, processed and sold without the data subject's 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 that pertain 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 criminalize the actions of spyware since the Act requires that the consent of the user be 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 caused in part by the fact that the techniques required to monitor and enforce are beyond the power of single states, or groups of states.

The Member States of the European Union have a strong level of privacy legislation that 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 concepts of spyware, and user consent, are vague, especially in light of the licence agreements that have been incorporated into the original contract. There may also exist another argument against the use of the licence agreement as a method of legitimizing 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 are 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 that is limited to nation states in an environment that 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 who is behind the software and which corporate entities or private citizens are to be considered to be responsible for the software.

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 that 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 legitimizing factor for unfair 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 not 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 that is very hard to achieve, implement and enforce. Until this can be achieved legislation will continue to be unclear in its effect and therefore be more important as a symbolic gesture on the part of the national legislator.

The disruptive effects of technology upon a social balance created over time can have the subtle effect of changing that 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 affected 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.

Attempting a regulatory approach takes time and a great deal of concerted effort. Habermas²⁴ argues that societies are the base for a multitude of pluralistic opinions but where only a few ever come to the forefront of the public debate. In ensuring that the debate is maintained in an open forum and that the rules are created in a transparent method it is important that the basis for rules are discussed by those who are affected by them. It is also important, however, to note in this context that all rules should be held under constant debate.²⁵ 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.

An additional reason for the need for more public debate amongst those concerned is that they are themselves responsible for achieving 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.

Notes and References

- 1 The software has been downloaded 152 million times according to information available on their website <http://www.cometsystems.com/>.
- 2 C Oakes 'Mouse pointer records clicks' *Wired News* 30 November 1999. <http://www.wired.com/news/technology/0,1282,32788,00.html>.
- 3 P Rojas 'Kazaa Lite no spyware aftertaste' *Wired News* 18 April 2002. <http://www.wired.com/news/mp3/0,1285,51916,00.html>. 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 attempts to use the D2OL distributed computing platform to search for cures for rare childhood diseases.
- 4 For example R Barbrook 'The hi-tech gift economy' *First Monday* 3 (12), 7 December 1998. (http://www.firstmonday.dk/issues/issue3_12/barbrook/).
- 5 J Benner 'Spyware in a galaxy near you' *Wired News* 24 January 2002. <http://www.wired.com/news/technology/0,1282,49960,00.html>.

- 6 D Cave 'The parasite economy' 2 August 2001, Salon.com http://archive.salon.com/tech/feature/2001/08/02/parasite_capital/.
- 7 M P Furmston *Cheshire, Fifoot & Furmston's Law of Contract* Butterworths, London, 1996.
- 8 D Rowland & E McDonald *Information Technology Law* 2nd edn, Cavendish, London, 2000.
- 9 P H Arne and M M Bosse 'Overview of clickwrap agreements' *Practising Law Institute*, January—March 2003.
- 10 *Spurling (J) Ltd v Bradshaw* (1956), CA.
- 11 P Gordley *The Philosophical Origins of the Modern Contract Doctrine* Clarendon Press, Oxford, 1991.
- 12 *Washington Post, Newsweek Interactive Co., LLC., et al. v The Gator Corporation*, Civil Action 02-909-A, U.S. District Court (EDVa).
- 13 B Tedeschi 'Pop-up ads provoke a turf battle over Web rights' *International Herald Tribune*, Tuesday 8 July 2003, p 15. The court was the Eastern District Court of Virginia.
- 14 N Bobbio *Rättigheternas Epok* transl. W Fovet (translated from original *L'età dei diritti*) Daidalos, Zoetermeer, The Netherlands, 2001.
- 15 *Convention for the Protection of Human Rights and Fundamental Freedoms*—Rome 1950.
- 16 S Warren and L D Brandeis 'The right to privacy' *Harvard Law Review* 4 (5), pp 193-220, 15 December 1890.
- 17 S Kern *The Culture of Time and Space 1880-1918* Harvard University Press, Cambridge, MA, 1983.
- 18 M Foucault in C Gordon (ed) *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977* The Harvester Press, New York, 1980.
- 19 J Bentham in M Bozovic (ed) *The Panopticon Writings* Verso Books, London, 1995.
- 20 Foucault, op cit, Ref 18.
- 21 See for example, D G Johnson *Computer Ethics* 3rd edn, Prentice-Hall, Paramus, NJ, 2000.
- 22 R L McArthur 'Reasonable expectations of privacy' *Ethics and Information Technology* 3, pp 123-128, 2001.
- 23 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.
- 24 J Habermas *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* transl. B Thomas, MIT Press, Cambridge, MA, 1989.
- 25 J McCormick 'Habermas's discourse theory of law: bridging Anglo-American and continental legal traditions' *The Modern Law Review* 60, pp 734-743, 1997.