International Journal of Information & Network Security (IJINS)
Vol.1, No.4, October 2012, pp. 330~335
ISSN: 2089-3299

Legal, Ethical & Social Issues in the case of an Intrusive Remote Monitoring Software

Shaun McBrearty*, Nigel McKelvey*, Kevin Curran**
* Institute of Technology, Letterkenny, Co. Donegal, Ireland
** School of Computing and Intelligent Systems, University of Ulster, Derry, Northern Ireland

Article Info

Article history:

Received Sept 05th, 2012
Accepted Sept 15th, 2012

Keyword:

Legal
Ethical
Intrusion
Remote
Monitoring

ABSTRACT

In 2008, a laptop was stolen from a high school student in the USA. The laptop was being monitored by remote recovery software. The thief sold the laptop in question to another student who in turn sold it to a teacher. The software continued to monitor the private daily life of this teacher. This paper provides an overview of the resultant lawsuit. We examine the ethical, privacy and legal dilemmas highlighted by this case.

Copyright @ 2012 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Second Author,
Computing Department of the Letterkenny Institute of Technology
Email: Nigel.McKelvey@lyit.ie

1. INTRODUCTION

In 2008, the Clark County School District had a laptop stolen from one of its students in a library (Schwartz, 2011). Upon discovering this, the school district reported the theft to Absolute Software who began monitoring the laptop (Keegan, 2011; Zetter, 2011). The thief reportedly a student (Zetter, 2011) then sold the laptop in question to a student attending Kiefer Alternative School. The student suspected the laptop of being stolen and decided to sell it to Mrs Susan Clements-Jeffrey, a long-term substitute teacher at the school they attended (Zetter, 2011). Mrs Clements-Jeffrey agreed to purchase the laptop, which was now in a non-operational state, provided one of her work colleagues would be able to fix it, which they ultimately did (Keegan, 2011). Unbeknownst to Clements-Jeffrey the laptop was under supervision by Absolute Software.

LoJack for Laptops is remote-recovery software developed by Absolute Software (Schwartz, 2011). The software comes pre-installed on several new laptops to assist in the recovery of stolen laptop computers. The software must first be activated before the functionality is enabled. In the event of a laptop being stolen and the software has been activated, the laptop owner simply informs Absolute Software of the theft and they then monitor the stolen laptop (Absolute Software, 2011a). The software allows users to monitor the last known location of where their laptop was connected to the internet, to remove files stored on the computer and even freeze the laptop to prevent it from being used until the laptop is recovered. Absolute Software assigns a theft officer to the case and they then gather information on the stolen laptop and present it to the relevant authorities to recover it (Absolute Software, 2011b). Under normal circumstances Absolute Software forward the IP address obtained from the stolen laptop to local police who then obtain the name and address of the person currently in possession of the laptop, but in the following case the company went beyond their usual course of action and invaded the privacy of the laptop user, who was unaware of the fact she was in possession of a stolen computer (Zetter, 2011).

In this particular case the theft officer in charge of monitoring the laptop, Kyle Magnus took extreme measures and spied on communications between Clements-Jeffrey and her partner, Carlton Smith, several of which were of a sexual nature. Magnus also logged Clements-Jeffreys' keystrokes and internet browsing habits, and perhaps most shockingly of all, captured nude images of her from the laptops webcam (Zetter, 2011). Upon reporting the case to local police, Magnus handed over all information he had gathered on Clements-Jeffrey, including the nude images (Schwartz, 2011; Zetter, 2011). The police then approached Clements-Jeffrey with the intention of arresting her for being in possession of stolen goods, but rather than presenting her with an arrest warrant, they instead brandished the nude images and messages that Magnus had captured and intercepted while monitoring her. Obviously Mrs Clements-Jeffrey was not aware she was in possession of a stolen computer and the charges against her were dropped a week later (Keegan, 2011; Schwartz, 2011; Zetter, 2011).

Mrs Clements-Jeffrey in turn sued Absolute Software, theft officer Kyle Magnus and the Springfield, Ohio Police (Keegan, 2011; Zetter, 2011). Absolute Software settled out of court with Mrs Clements-Jeffrey when the judge in the case stated that the company had breached Clements-Jeffreys' privacy because she was unaware that the laptop was stolen property. The theft officer involved in the case went above and beyond normal protocol. In doing so, he violated both the Electronics Communications Privacy Act (ECPA) and the Stored Communications Act (Keegan, 2011; Zetter, 2011). In their defense Absolute Software claimed that Clements-Jeffrey should have known that the laptop was stolen because of the price she purchased the laptop for, and that because the laptop was stolen, Clements-Jeffrey had no right to privacy (Zetter, 2011; Schwartz, 2011). Absolute Software asked for the case to be dismissed but the judge declined this due to the fact that he believed a jury could find the company guilty of breaking several laws and denying the human rights of both Clements-Jeffrey and Smith (Keegan, 2011; Zetter, 2011; Schwartz, 2011). The judge added that tracking the IP address of a stolen laptop was an acceptable method for trying to recover it, but accessing the communications of the person using the laptop was not tolerable (Schwartz, 2011; Zetter, 2011).

Mrs Clements-Jeffrey sued the Springfield, Ohio police force for wrongful arrest, divulging sexually explicit photographs of her and for violating her Fourth Amendment rights (Keegan, 2011; Zetter, 2011). The arresting officers involved in the case admitted to having little or no knowledge about 'wiretapping' laws and that they assumed the images used during the arrest were obtained legally (Schwartz, 2011). The case bears a striking resemblance to a 2010 case involving a Pennsylvania school district spying on students using school distributed laptops when they were in use outside of school hours (Matyszczyk, 2010; Keizer, 2010).

2. PRIVACY ISSUES

A major issue in this case is privacy. The victim, Susan Clements-Jeffrey had her privacy violated and her communications illegally intercepted (Matyszczyk, 2011; Keegan, 2011; Schwartz, 2011; Zetter, 2011). The Clark County School District reported the theft of their laptop to Absolute Software who in turned carried out their investigation. The district did nothing wrong in their actions because they were unaware that Absolute Software could/would intercept the communications of the people involved. Undoubtedly the school district and the student who had the laptop stolen benefited from this action because the computer was returned. Clearly Susan Clements-Jeffrey was hurt by this action because her laptop was seized as she was unwittingly in possession of stolen goods.

Absolute Software are the developers of the software used to track the stolen laptop, LoJack for Laptops. Obviously, Absolute Software and the Clark County School District benefited from the retrieval of the stolen laptop. On the other hand, the company was harmed by its own actions for facilitating its employees to break laws and denying people their human rights by illegally surveilling them. Susan Clements-Jeffrey and her partner, Carlton Smith were clearly harmed by the company's actions by having their laptop confiscated. They also had their privacy violated; explicit images of themselves released and suffered the embarrassment of having details of their relationship and personal lives being made available to the public in the proceeding court case. It could also be argued that the reputation of the Clark County School District may have been damaged due to their association with the case.

Kyle Magnus was the theft officer involved in surveilling Susan Clements- Jeffrey with the intention of retrieving the stolen laptop she unknowingly had in her possession. Evidently Kyle Magnus benefited from his own actions by eventually retrieving the stolen laptop. The Clark County School District also benefited by getting their stolen property back as did Absolute Software themselves. Conversely Magnus' actions harmed himself, his employer, and Susan Clements-Jeffrey and her partner Carlton Smith. Magnus harmed his own reputation and left himself open for prosecution by undertaking illegal activities as part of his job that were above and beyond his required duties. Absolute Software had its reputation damaged by being associated with Magnus. Magnus' actions left the organisation open to investigation due to the serious nature of the case. Susan Clements-Jeffrey and Carlton Smith had to suffer the embarrassment of the details of their

relationship and personal lives being made public due to the case they took (although this could also be argued that it was an effect of their own actions). The couple also had their privacy breached and Mrs Clements-Jeffrey had her laptop seized. It could also be argued that the Springfield, Ohio police were harmed by Magnus' actions because they used the evidence that he had gathered under the impression that it was legally obtained.

The Springfield, Ohio police wrongfully arrested Susan Clements-Jeffrey for being in possession of stolen goods. They seized her laptop and returned it to its rightful owner but in the process used illegally obtained evidence and arrested Clements-Jeffrey without an arrest warrant. At that time the police benefited from their own actions by arresting, what the believed to be, a thief. The Clark County School District and their student benefited because they got their stolen laptop back in their possession. It could also be argued that Absolute Software and Kyle Magnus benefited because they were successful in their attempts to recover the stolen laptop. On the opposite side of things though, the Springfield, Ohio police harmed themselves by their own actions. They arrested an innocent woman without an arrest warrant and they used inadmissible evidence as their basis for arresting her. Susan Clements-Jeffrey was harmed by these actions in that she was wrongfully arrested and she had the embarrassment of intimately revealing photographs and messages involving herself and Carlton Smith being brandished about. It could also be argued that Absolute Software were harmed by these actions due to the police force displaying the images they captured, had they not done so then Clements- Jeffrey would not have known that her privacy was invaded and therefore may not have taken legal action against the company.

Susan Clements-Jeffrey purchased a damaged laptop from a student in the school she taught in; unbeknownst to her the laptop was stolen. She herself benefited from this action by acquiring a laptop at a very cheap price. The child that sold her the laptop benefited financially from this. In doing so, Susan Clements-Jeffrey, unintentionally harmed the Clark County School District by taking possession of their property. In taking the matter to court, both herself and her partner, Carlton Smith, benefited from the action because they were compensated for being the victim in the case. Perhaps society also benefited from the fact that such illegal activities were exposed. Absolute Software, Kyle Magnus and the Springfield, Ohio police were all harmed by this action because they were punished for their wrong-doings. It is plausible that the reputation of the Clark County School District was also damaged due to be being associated with the case.

3. LEGAL, ETHICAL & SOCIAL IMPLICATIONS

Several legal issues arose out of this case such as Absolute Software providing its staff with a means to remotely access the electronic communications of the computers it monitors and protects. This violated several laws such as the ECPA and the Stored Communication Act. The Springfield police force violated Susan Clements-Jeffreys' Fourth Amendment rights and the Springfield police force also used inadmissible evidence for arresting Clements-Jeffrey. The Springfield police force also wrongfully arresting Clements-Jeffrey.

The ethical issues arising out of the case include whether a person using a stolen computer have privacy rights and whether an image of a person using a stolen laptop should be allowed to be remotely captured without their consent. There are also ethical issues as to whether the police should have used embarrassing photographs of Susan Clements-Jeffrey when arresting her and whether it is right that a person monitoring illegal activity are themselves, undertaking an illegal activity to do so. There are legitimate concerns over Absolute Software providing its employees with such powerful monitoring software when an IP address would suffice and over a person being in charge of monitoring peoples activities.

Social issues arising out of this case include how far someone should be allowed to go to retrieve stolen property. Dilemmas arising out of this case include the possibility of the school district eventually selling on the laptop and it still having LoJack for Laptops installed on it (Keegan, 2011).The possibility that a theft officer may be monitoring a person's laptop even though it is not stolen (Keegan, 2011) and whether Absolute Software violated the rights of people like this before and not been caught (Keegan, 2011). Due to the embarrassment involved for Clements-Jeffrey and Smith, should the context in which their communications took place have been disclosed. There is also the question of how to determine whether a person knows if they are in possession of stolen property or not.

4. RELEVANCE OF ETHICAL THEORIES

The consensus of the Divine Command Theory is that right and wrong are dictated by the holy text of whatever religion, if any, the people in question are. This ethical theory is not relevant to this case study because the religion of those involved is not disclosed. The general consensus of Kantianism is that a decision is good when there is good will behind it, even if the end result is not as good as intended. Good will is considered doing the right thing, not what the individual wants. In this case then Kyle Magnus' actions are

considered acceptable. He may have invaded Susan Clements- Jeffreys' privacy and captured nude photographs of her, but he was doing his job with good intentions.

Under Act Utilitarianism, an action is considered good if it benefits someone, whereas an action is considered bad if it harms someone. It does not consider the morality of an action, it just considers its outcome; If the positives outweigh the negatives then an action is considered good. In this case then Kyle Magnus' actions can be justified as good because the end result was that the owner had their laptop returned, Kyle Magnus was successful in his work, Absolute Software were successful in their work and so were the Springfield, Ohio police. The only person harmed by these actions was Susan Clements-Jeffrey, who had her laptop seized. Although it can also be argued that his actions were considered more harmful than good because of the trouble caused to himself, his employer and the police in the legal action that followed.

In Rule Utilitarianism, a rule is considered good if it leads to the greatest happiness. Rule Utilitarianism is different in that it analyses the outcome of an action and not the will behind it. In this case a proposed rule could be "Peoples privacy should be violated if they are using a stolen laptop". If everyone followed this rule then all people who have had their computers stolen would be better off. The Police and Absolute Software (and similar companies) would also benefit by being/becoming more successful at their jobs. The harm caused by this action would be that all people in possession of stolen computers would have their privacy violated and their computers seized and returned to their rightful owners. The good outweighs the bad in this case; therefore it is acceptable to invade a person's privacy if they are using a stolen laptop. In Social Contract Theory an action is considered right if people collectively accept it because of its benefit to people. So in this case then Kyle Magnus is considered to be in the wrong. Al people are entitled to their privacy. An obvious solution for avoiding this problem is for Absolute Software (and other similar service providers) to only provide its employees with the use of software that does not breach privacy rights.

This case is a good example for the introduction of internet regulation. The thought immediately springing to mind is that this type of remote monitoring should not be allowed over the internet, although remote camera monitoring can also encompass CCTV and speed cameras which would be counter-productive. Clearly this is a gray-area. The software that provides this illegal access is allowed to exist even though it provides such law breaking. Monitoring the persons IP address alone should be more than substantial to retrieve the stolen computer in this instance. Besides this, there are also several more reasons for the internet to be regulated. These include: the fact the internet is no different to any other network, the harmful content that exists on the internet, the prevalence of criminal activity on the internet, the emergence of internet browsing on mobile phones, and the fact that censorship exists for similar mediums.

5. CONCLUSION

The fact that the internet is a truly global network should not make it exempt from regulation. A small company with a Local Area Network (LAN) can regulate the use of its network to abide by the laws of the country it operates in, so there is no reason as to why the global network itself cannot be regulated. Obviously this presents several issues, such as the regulation of content that may be illegal in one country while being perfectly acceptable in another. The current trend is that governments and internet service providers (ISPs') are taking these matters in to their own hands (Boran, 2010; Magnanti, 2011). The internet is also a 'hotbed' of harmful content, particularly pornography. There is no denying that a large amount of the Internet consists of material of a pornographic nature Shamoon (2007). Even the most genuine internet user has stumbled across a pornographic result while using a search engine in pursuit of other content. The widely accessible nature of this material is quite alarming. If such content can be found by mishap, then it must be censored. This material is of a harmful nature, particularly to minors and should be blocked without a doubt. This can also include child pornography which is obviously illegal. Not a month seems to go by without hearing in the news of the arrest of someone for possession of such terrible material both globally and locally (RTE, 2011).

The internet has also in recent times been used a medium for the sexual solicitation of minors (Broach, 2009). Authorities work tirelessly on the ground to prevent such things happening yet it occurs regularly in cyber space. This cannot be tolerated and must be stopped. Additionally, the internet also provides illegal activities to thrive. Extremist views, terrorist groups, money laundering, copyright theft, fraud, computer hacking, prostitution, and drug smuggling are all easily accessible online, despite the fact they are all illegal in Ireland. Again, these are all areas of crime that are rigorously policed in the real world yet are simply just a search away on the internet. I have actually embedded hyperlinks to this type of content just to demonstrate how easily accessible it actually is.

The emergence of mobile phones and the increasing amount of children owning mobile phones along with augmented usage of the internet on them is another cause for concern (Allen, 2009; BBC, 2008). Parental control software to filter internet content on desktop computers is widely available yet such software is quite limited for mobile phones. The software does exist, although it is marketed at the newer phones on

the market and does not cover older models (Parental Control Bar, 2009; PhoneSheriff, 2011). Obviously if the technology is not there to prevent harmful content being accessed, then surely it makes sense that the internet be regulated on the server side if it cannot at the client side? I know some will argue that a child should not have a mobile phone, but in this day and age but is that truly realistic? There is also the issue of radio, newspaper, cinema and television censorship (Broadcasting Authority of Ireland, 2011). These similar communication and entertainment mediums are all regulated yet the internet is not. The internet cannot provide a means for such activities to take place; such a widely used and easily accessible network must be policed to protect society from crime and harmful content, particularly our most vulnerable members - children.

From the case study here, it is possible to see why people would call for internet regulation. The woman in question, Susan Clements-Jeffrey had her privacy invaded and was photographed naked (Keegan, 2011; Schwartz, 2011; Zetter, 2011; Matyszczyk, 2011). Yes, this is inappropriate but one could argue that it was just unfortunate. The obvious benefits of using a webcam to capture an image of a person using a laptop are there to be seen. Society widely condemns Absolute Software's practices in this instance, but these people are not in a position where they have had their computer stolen. In their public statement, the Clark County School District admitted they had no knowledge that Absolute Software would intercept the communications of those involved, but they did not publicly state their disapproval of the company's methods either (Zetter, 2011). After all, it was these methods that retrieved their computer. What struck up the sympathy of the public in this case was that Susan Clements-Jeffrey was an unfortunate, innocent victim, and that Kyle Magnus' actions and intentions were clearly not work related. Surely the internet cannot be censored in such a way that would prevent a person recovering their stolen property? Such an act would give a thief the upper hand.

Others reason that internet regulation should be avoided are: the global nature of the internet, the way in which the internet is used, imperfect filtering methods, and the responsibility of parents to ensure their children's safety. The fact that the internet is a truly global network should prevent it from censorship. It is designed so that information from one part of the world can be viewed in all other parts of the world. By censoring this, people would be denied their freedom of speech. Internet regulation would also raise the question of how to censor it with respect to different cultures. What is acceptable and legal in some countries is not in others. Clearly it would be impossible to satisfy all societies and cultures with respect to this. We as internet users choose what we want to view on the internet. The content is not forced upon us like others mediums such as television and radio. Therefore we should have a right to choose to view whatever content we like. We choose to view such content because we as individuals believe it is good for us. By censoring this information, peoples' right to freedom of expression is being impeded. The Irish Constitution states that only radio, TV, cinema and printed media be censored. Any censorship of the internet without first holding a successful referendum would be a violation of the constitution Citizens Information Board, 2008).

In addition, there is a question mark over the accuracy of web content filtering software. The web filtering software employed in the Letterkenny Institute of Technology (LYIT) is a perfect example of this. Any website that attempts to be accessed in the college that is not categorised or has yet to be approved appears to be automatically labeled as pornographic in nature. Just recently a lecturer attempted to demonstrate something on the website, www.python.org, however when they typed in the URL they accidentally typed www.python.com. Much to the amusement of the class, the lecturer was refused access to the site because it was apparently pornographic in nature; however, the site is clearly not. Brooke Magnanti, a journalist for The Guardian Newspaper in Britain, recently described her experience of adult content filtering on her mobile phone. She states that the web browser on her mobile phone was configured to filter out adult content; yet, she was able to view a pornographic image that a rival newspaper had mistakenly posted on their website. She also states that the same browser blocked sex education websites, which are clearly not pornographic, but in the public interest (Magnanti, 2011). Clearly there are areas of underperformance that need to be identified before the idea of regulation can even be considered.

Some would also argue that it is the responsibility of parents and teachers to protect children from harmful content. This is a valid point as many parents allow their children to view content such as films, television programs and books that are not legally deemed suitable by the censorship authorities. If this is the case then surely such a practice is also possible for the internet, in which case, it would defeat the purpose of regulation. The content of unsuitable films and television programs is no worse that the unsuitable content on the internet. A responsible parent should watch a film with their child or even review the film before the child can watch it to deem it suitable or not. Surely it is not much to ask to do the same in terms of their children's internet usage? If parents are that concerned about their children using the internet, they should supervise them. The internet cannot be censored. Such a step would lead us in the direction of communism. The internet is a place of free speech and free expression. Yes, the internet does contain harmful content, but so does every other medium used to deliver a message.

REFERENCES

[1] Absolute Software (2011a) L4L-FAQ. http://www.absolute.com/Shared/FAQs
[2] Absolute Software (2011b) LoJack for laptops: How It Works http://www. absolute.com/en/lojackforlaptops/technology.aspx
[3] Allen, P. (2009). France cracks down on children's mobile phone use but Britain still ignoring warnings http://www.dailymail.co.uk/health/article-1112123/France-cracks- childrens-mobile-phone-use-Britain- ignoring-warnings.html
[4] BBC (2008) Mobile internet usage on the rise, November 25th 2008 http://news.bbc.co.uk/1/hi/technology/7748372.stm,
[5] Boran, M. (2010) Eircoms anti-piracy crackdown begins today, Silicon Republic, http://www.siliconrepublic.com/comms/item/16313-eircoms-anti-piracy-crackd
[6] Broach, D. (2009) Soliciting sex with 'minors' over internet sends dozens to jail http://www.nola.com/news/index.ssf/2009/03/internet_sex.html
[7] Broadcasting Authority of Ireland (2011) http://www.bai.ie/
[8] Citizens Information Board (2008) Right to freedom of expression http://www.citizensinformation.ie/en/government_in_ireland/irish_constitution_1/freedom_of_expression.html
[9] Keegan, C. D. (2009). Absolute software voyeurs settle with victim clements jeffrey out of court, New Orleans Metro Real Time News, March 28th 2009 http://www.computerpartsgreenvillesc.com/ absolute-software-voyeurs-to-face-court-challenge-from-victim/
[10] Keizer, G. (2010) Pennsylvania schools spying on students using laptop webcams, claims lawsuit, Computer World, http://www.computerworld.com/s/article/9158818/ Pennsylvania_schools_spying_on_students_us ing_laptop_webcams_claims_lawsuit?taxonomyId=84
[11] Magnanti, B. (2011) A web porn 'opt-in' scheme is no quick fix, Guardian, October 11th, http://www.guardian.co.uk/commentisfree/2011/oct/11/web-porn-opt-in
[12] Matyszczyk, C. (2010) School accused of off-campus webcam spying, CNET, February 18th 2010, http://news.cnet.com/8301-17852_3-10456128-71.html?tag=mncol
[13] Matyszczyk, C (2011) Laptop-tracking company can be sued for spying on sex chats, CNET, May 3rd http://news.cnet.com/8301-1009_3-20100463-83/laptop-tracking-company-can-be-sued-for-spying-on-sex-chats/
[14] Parental Control Bar (2009) http://parentalcontrolbar.com/
[15] PhoneSheriff (2011) http://www.phonesheriff.com
[16] RTE (2003) Ex-priest jailed for child porn possession, RTE, http://www.rte.ie/news/2003/1015/childporn.html
[17] RTE (2011) US bishop charged in child abuse case, RTE, 15th October, http://www.rte.ie/news/2011/1015/abuse.html
[18] Schwartz, M. (2011) Laptop tracking software faces new privacy heat, Information Week, September 1st, http://www.techweb.com/news/231600626/laptop-tracking-software-faces-new-privacy-heat .html
[19] Shamoon, E. (2007) Surprise, surprise: Internet porn is popular, Switched.com, 15th May, http://www.switched.com/2007/05/15/exclusive-internet-porn-is-popular/
[20] Zetter, K. (2011) Couple can sue laptop-tracking company for spying on sex chats, Wired, August 2011, http://www.wired.com/threatlevel/2011/08/absolute-sued-for-spying/

BIOGRAPHY OF AUTHORS

Shaun McBrearty is a recent graduate in Applied Computing from the Letterkenny Institute of Technology.

Nigel McKelvey is a lecturer in the Computing Department of the Letterkenny Institute of Technology.

Kevin Curran is a lecturer in the School of Computing at the University of Ulster.