African Journal of Business Management Vol.6 (44), pp. 10799-10806, 7 November 2012
Available online at http://www.academicjournals.org/AJBM
DOI: 10.5897/AJBM12.992
ISSN 1993-8233 ©2012 Academic Journals

Review

The case for a technically safe environment to protect the identities of anonymous whistle-blowers: A conceptual paper

Johan van Loggerenberg

Department of Informatics, University of Pretoria, Pretoria, 0001 South Africa. E-mail: johan.vl@up.ac.za.

Accepted 25 September, 2012

Whistle-blowing is one of the most important aspects in the fight against corruption. In most cases, it is impossible to commit a corrupt deed without at least one other person being involved in, or, knowing about it. Many businesses and public entities have a 'crime lines' in place to facilitate whistle-blowing but these facilities are mostly limited to a particular telephone number. Using a telephone to report corruption has inherent problems when anonymity is required. Organisations can easily trace calls made from their facilities. Even calls made from cellular phones can be traced. Eavesdropping, although illegal, is not technically difficult to achieve. The fact is: Telephonic whistle-blowing provides little protection for the whistle-blower who wants to remain anonymous. This paper focuses on the problem of current ways for whistle-blowing and suggests an improvement conceptually. It aims to open up debate and discussion on this topic with the intention to attract further contributions and stimulate research on this topic. Although the paper focuses strongly on the situation in South Africa, it is probably equally applicable anywhere else in the world.

Key words: Whistle-blowing, Information Technology, Anonymity, Onion Routing.

INTRODUCTION

Reporting suspicious incidents is one of the prime components in the detection of criminal activities. Without such reporting, law enforcement becomes much less effective with the result that many crimes take place without being detected.

Suspicious incidents are typically facilitated through the use of "Crime Lines". These are typically telephone numbers that can be dialled by whistle-blowers.

In most cases protection of the identity of the whistle-blower is of paramount importance. To report an incident which exposes another individual can be seriously dangerous to the person blowing the whistle and cases are known where such whistle-blowers have lost their lives.

Many cases have been documented where whistle-blowers chose to reveal their identity. When the identity of the whistle-blower is known, investigation by law enforcement agencies is strongly facilitated and is, as such, always preferred. An argument can be made that a whistle-blower is protected by the law and should, therefore, have no fear. However, whilst the law theoretically protects whistle-blowers from being victimised, the practical side is far from safe.

Anonymity must therefore be viewed as a pre-requisite for whistle-blowers that choose to remain anonymous.

Crime lines (that is, telephone lines) are currently being used as the preferred mechanism to report suspicious incidents. Unfortunately, telephone reporting provides very little in terms of anonymity. Most companies keep logs of telephone calls being made from internally and if someone is suspected to have reported an incident, such logs can, with relative ease, be accessed by perpetrators to determine where the call was made from.

The aim of this conceptual paper is to investigate the potential of Information and communications technology (ICT) to enable a safe alternative to facilitate anonymous whistle-blowing.

As is the case with concept papers, the research

methodology is primarily based on the limited literature available on the topic. The author made use of news-paper reports to provide situational context.

WHISTLE-BLOWING

The term whistle-blowing originated from the days when the whistle was blown by a police officer when witnessing a criminal deed or by a referee when witnessing some-one contradicting the rules of the sports game. There is, however, as metaphors regarding whistle-blowing, a distinct difference between the use of a policeman or a referee. Policemen and referees have the authority to enforce their actions whereas present day whistle-blowers do not enjoy such authority (Ellison, 1982). The whistle-bloweris dependent on someone else with authority.

The idea behind the term 'whistle-blower' is, however, very positive. It occurs when someone violates an accepted rule or law and should be stopped from doing so. The whistle-blower does so in the public interest. The whistle-blower is, in fact, trying *"…to enlist the support of others to achieve social objectives"* (Ellison, 1982).

Whistle-blowing is, in general, defined as "raising a concern about malpractice within an organisation". This definition is attributed to the UK Committee on Standards in Public Life (Camerer, 2001; Martin, 2010). Another definition is the "pursuit of a concern about wrongdoing that does damage to a wider public interest" (Public Concern at Work, 2005). This second definition puts whistle-blowing specifically in the context of the public interest as opposed to the first one which is more specifically about the 'organisation'.

Near and Miceli (1985) define whistle-blowing as "*the disclosure by organization members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action"*.

Definitions identify that something illegal or un-acceptable is taking place and the person raising the alarm (the 'whistle-blower') is drawing attention to this fact. The ultimate intention is to avoid a repetition. The person blowing the whistle is, therefore, simply the 'messenger' who acts in the best interest of the organisation, or in the best interest of society (Camerer, 2001).

It is understandable that those people actively parti-cipating in the deed will not appreciate their actions being exposed. What comes as a surprise, is that, often, even innocent 'onlookers' are also critical of the whistle-blower's action. The result is that whistle-blowers have been getting a poor reputation from some quarters (Camerer, 2001).

In an organisational sense, a whistle-blower can be either one of the employees (that is, internally to the organisation), or externally to the organisation. Famous internal whistle-blowers were Sherron Watkins (in the Enron case) and Cynthia Cooper (Worldcom) (Colvin, 2002).

The auditing profession, for instance, can be seen as mandatedwhistle-blowers. They are mandated by the shareholders to look for anything outside of the rules, regulations or laws and formally report it to the management and the shareholders.

There can be no doubt that whistle-blowing plays a very important role in the fight against corruption (Martin, 2010). Not only does it play a deterring role, but it also assists in bringing criminals to book by making law enforcement agencies aware of criminal activities for further investigation.

Estimates of the scale of corruption in South Africa vary considerably, but it is safe to say that it runs into the billions of Rands every year. The South African Minister of Finance (speaking of Income Tax revenue), reported that R13 Billion less would be collected than what was budgeted. This 'loss' is probably far less than what is lost through corruption, let alone what is lost on wasteful expenditure and, what the Minister calls *'extravagance in public administration' (*Treasury, 2011). South Africa can certainly not afford the losses suffered through corruption. Whistle-blowing, therefore, plays an important role to combat such losses.

LEGAL PROTECTION FOR WHISTLE-BLOWERS

Identified whistle-blowers face many risks (Martin, 2010). These risks can take the form of being victimised in the workplace, and/or the very real possibility of retaliation by those involved in the criminal deeds.

To protect whistle-blowers in the workplace, legal protection is available in many countries, including South Africa. Martin (2011) makes the point that *"[p]rotection for whistle-blowers is essential to create a culture of disclosure of wrong-doing*".

The primary South African Act addressing the phenol-mena of corruption, is the Prevention and Combating of Corrupt activities 2003, Act 12 of 2004 (Republic of South Africa, 2004).

The Protected Disclosures Act, 26 of 2000 (Republic of South Africa, 2000) was designed specifically to provide such protection. Martin (2010, 2011) and Camerer (2001) deal extensively with the legal intentions of the Act in their papers.

Both the Companies Act, Act 71 of 2008 (Republic of South Africa, 2008) and the Companies Amendment Act, 3 of 2011 (Republic of South Africa, 2011) also provide legal protection for whistle-blowers. These Acts do not specifically refer to anonymous whistle-blowing, and seem to assume that the identity of the whistle-blower is known.

What also needs to be noted is that the legal protection provided by these Acts, is limited to whistle-blowers with known identities. This is to be expected as protection can only be provided to someone who is known. This point is further discussed in the summary to the area dealing with legal protection.

Despite the legal protection provided in the Acts, cases are still reported where whistle-blowers did not enjoy the protection promised in the Acts.

The (London) Guardian newspaper (Syal, 2010) reports that "…*[employment tribunal statistics show that the total number of people using whistleblowing legislation, which aims to protect workers from victimisation if they have exposed wrongdoing, increased from 157 cases in 1999 to 1,791 10 years later*". The article quotes many cases of whistle-blowers being dismissed or being 'gagged'.

Statistics for the South African situation are not available, but there is plenty evidence of whistle-blowers being dismissed or victimised (Martin, 2010). In an article appearing in the (South African) Mail and Guardian (Calland, 2011) a case is described where a municipal manager was dismissed and her house burnt down when she initiated an investigation into fraud. The article indicates that, although her dismissal had been ruled unfair in the court, her employers still refused to give her back her job.

In the same article, it is reported that "…*14 government officials or politicians have been murdered [in Mpumalanga province] since 1998*' and that there was a *"…twelve-fold increase in wasteful expenditure since 2007, but a sharp decrease in the number of whistle-blowers coming forward to report malfeasance"* (Calland, 2011).

In yet another article, the (SA) Mail and Guardian Online (2007) reported a case where the medical superintendent of a hospital in the Eastern Cape was dismissed when *"speaking out against [the hospital's] handling of the Frere Hospital maternity saga"* (Mail and Guardian Online, 2007). The superintendent alleged that "*200 babies were dying every month at East London's two largest hospitals"* (Mail and Guardian Online, 2007).

Martin (2010, 2011) raises a number of concerns about the adequacy of the protection provided by the legal framework in South Africa. Adv. Madonsela, The Public Protector in South Africa, echoed the same concern (Martin, 2011; Public Protector, 2010).

Miceli et al. (1999) point out that, whilst lawmakers generally want to believe that protecting whistle-blowers from retaliation will encourage the practice of whistle-blowing, the contrary is true. They quote several research papers with supporting evidence that *"legal protections neither reduce the incidence of retaliation nor increase the incidence of whistle-blowing"* (Miceli et al., 1999). In their research (covered in the 1999 paper) they again tested, *inter alia,* two hypotheses. The first was that an effective law (that is, protecting whistle-blowers) was likely to cause whistle-blowers to identify themselves rather than do so anonymously. The second was that an effective law was likely to cause perceived retaliation to be less likely to follow identified whistle-blowing.

In both hypotheses they found the opposite to what they expected. In the first hypothesis, the number of identified whistle-blowers reduced from 74 to 60%. In the second hypothesis they found that the percentage of identified whistle-blowers who suffered retaliation increased from 15 to 33%.

In summary: Despite the legal protection found in the Acts, whistle-blowers experience that such protection is only partly effective at best. This, in itself, should discourage whistle-blowers from disclosing their identities when blowing the whistle, thereby leading to anonymous whistle-blowing. Blowing the whistle anonymously, however, disqualifies them from the legal protection they would have enjoyed as an identified whistle-blower. As an anonymous whistle-blowers, *they would not need protection, on condition that they remain anonymous*.

ANONYMOUS VS IDENTIFIED WHISTLE-BLOWING

Anonymity means that the person's *"…identity is not publicly known"* (Ellison, 1982). The question is: Is it acceptable for someone to remain anonymous when blowing the whistle or is the person obliged to reveal his identity?

As Ellison (1982) points out, one has to distinguish between anonymity and two other, closely related terms, namely, secrecy and privacy. He argues that secrecy requires a *"conspiracy of silence"*, thereby implying that more than one person knows the secret (Ellison, 1982). Something only known to one person is, according to Ellison, the *"extreme form of secrecy"*. This type of secrecy seems to fall outside of the scope of whistle-blowing as it is highly unlikely that one will blow the whistle on oneself.

In the context of whistle-blowing, it is the *denial of access to information to others* that makes it a secret (Ellison, 1982).

Privacy, according to Ellison (1982), occurs when one can justify why others are not allowed to share information that one has. He quotes the example of one's sex life. One has *the right* to exclude others from such *private* information, unless someone else can invoke a higher right than one's own to force one to disclose such information.

Ellison (1982) makes an important point that, regarding *privacy*, the burden of the proof rests with the *other party* who wants to have access to such information. Regarding *secrecy*, the burden of proof is reversed in that the person with the information has to justify why it should remain secret.

This raises the question of whether anonymity in the

context of whistle-blowing is more on the side of secrecy or more on the side of privacy. Ellison (1982) argues that the kind of information which is being withheld is not about the deed itself, but about the whistle-blower's identity.

The question becomes whether the public has a right to know the whistle-blower's identity or whether the whistle-blower has the right to withhold it (Ellison, 1982).

Ellison (1982) points out that many members of the public would consider an anonymous whistle-blower to be *"saying nasty things behind people's backs"* and, as a result, would argue that anonymous whistle-blowing should be discouraged. However, when one considers the risks associated with identified whistle-blowing, the case for anonymity gets much stronger (and the case for speaking behind people's backs, weaker).

Ellison (1982) argues in favour of identified whistle-blowing but concedes that many factors influence the argument. On the one hand, anonymous whistle-blowing *"impedes the pursuit of truth"* because it makes law enforcement considerably more difficult. Another factor to take into consideration in favour of anonymity is that fear or retaliation by the whistle-blower may result in keeping quiet if not allowed to report it anonymously. Clearly, blowing the whistle anonymously is infinitely more valuable than not blowing it at all (Ellison, 1982).

Ellison concludes that *"…blanket condemnation on anonymity is not warranted"*. He proposes that the justification must take three factors into consideration: the seriousness of the offense, the probability of retaliation and the social relationships.

One can conclude that identified whistle-blowing is definitely the preferred way of blowing the whistle, but, given the risks that have been outlined, there is a strong case to be made for anonymous whistle-blowing.

CURRENT WAYS OF BLOWING THE WHISTLE

There are many ways by which a person can report a suspicious incident. In an organisational context, the first option is to share the concern with a colleague or, more likely, with a supervisor. This unequivocally means that the person who reports the deed is known (referred to as an identified whistle-blower). An identified whistle-bloweris, as minimum, known to the person reporting it to, and may also be publicly known.

If the supervisor does not respond in a way acceptable to the whistle-blower, the person can report it to higher levels of management, or, report it externally to, say, a newspaper. It could also be reported by means of a 'crime line' to an agency put in place by the organisation. Crime lines are commonly services procured from outside the organisation, such as ones offered by auditing firms.

Reporting a suspicious incident to an external source allows the whistle-blower to either be an identified whistle-blower, or to report it without mentioning his[1] identity. By using technology (as opposed to face-to-face communication), the whistle-blower is given the choice to remain anonymous.

Reporting a suspicious incident by not revealing one's identity, *assumes* anonymity but when one analyses the mechanisms facilitating such reporting (the channels), the identity of the caller may be revealed through the channel used. In some cases it may be very simple and in others, whilst more difficult, still very possible and feasible. This has the unpleasant surprise to the whistle-blower that he may be identified - despite his intention to remain anonymous.

Internal telephones

Consider the case where a whistle-blower makes a call from inside his organisation by using the telephone exten-sion assigned to him. Most organisations, as normal good practice, keep logs of all calls made from extensions. These logs, commonly only records the event and not the content itself (although there are some cases where the entire conversation is recorded). By simply analysing the logs of calls made to the 'crime line' would reveal the extension from which the call was made and the identity of caller can be revealed. This is, obviously, the worst way of trying to be an anonymous whistle-blower. We are of the opinion that many whistle-blowers use this option without realising the risk of being identified as a standard feature of technology.

Making the call from someone else'stelephone exten-sion will cause the wrong person to be suspected of making the call. This will make it more difficult for a pursuer to identify the true whistle-blower but, the organisation, and the extension from where the call was made, is known. Because pursuers, typically, have good suspicions as to who may possess the relevant information to report them, a good guess can lead them to the whistle-blower. In the worst case, an innocent person may targeted.

Public telephones

What if the whistle-blower goes to a public telephone and makes the call to the crime line? The only way for the pursuer to detect such reporting would be to constantly monitor the crime line number, in other words, to eavesdrop. This is technically quite feasible, albeit illegal. It may also require voice recognition to identify the caller. This may be easy in some cases and more difficult in

[1] When referring to the term 'his' in respect of a whistle-blower, pursuer or criminal both the male and the female gender is implied.

others. Public telephones, therefore, still hold risks to the whistle-blower.

Cellular telephones

Blowing the whistle by using a cellular phone is equally dangerous. Firstly, cellular service providers keep logs of calls made (excluding the content). Normally one needs a court order to get access to such logs and it is likely to be challenging for a pursuer to obtain such permission. Of course, the pursuer can always 'persuade' an employee of the cellular network to - illegally - obtain the data on his behalf.

Even if the pursuer is prevented from getting access to the cellular call logs, it is quite possible and feasible to 'eavesdrop' on the crime line number (illegal) and 'listen in' to all the calls being made to the crime line. Callers can be identified through voice recognition techniques or, if the whistle-blower is known to the pursuer, he can quite easily be recognised.

Postal services

Another option open to a whistle-blower is to use the postal service. For instance, a whistle-blower can easily obtain the postal address of the Public Protector and send her an anonymous letter detailing the incident. In this case the 'strength' of the anonymity is strong, but only the public is not encouraged to use this way of whistle-blowing. Once the public is encouraged to use this mechanism, pursuers only have 'persuade' someone where mail is received, to intercept suspicious mail.

Email

Some organisations have made facilities available to whistle-blowers to report incidents via email. In some cases, these emails are encrypted. Sometimes these are addressed to a recipient internally to the organisation (for example, Internal audit), or, sometimes externally (for example, an Auditing Firm).

The origin for such email messages are easy to trace for the organisation concerned through logs being kept as a standard feature of email platforms. If the message is encrypted, it may be difficult to decipher the content, but the origin would be simple to trace as it would normally have the originator's name appearing in the message.

The point is this: All the aforementioned mechanisms described have weaknesses regarding the anonymity of the whistle-blower. Weaknesses create risks to the whistle-blower and prospective whistle-blowers will assess such risks when deciding to blow the whistle or not. One needs to acknowledge that the seriousness (or scale) of the case also plays an important role. The extent to which the pursuer is prepared to go to prevent or detect whistle-blowers, is directly related to the seriousness of the offence and the severity of consequences the pursuer faces. There will be a world of difference between a traffic official taking a R100 bribe and someone taking a R10 million bribe in, say, an arms deal. Equally, a prospective whistle-blower in an arms deal involving billions of Rands, will expect a much higher level of anonymity than a prospective whistle-blower involving a few thousand Rands in traffic fines.

To make it more real: If large scale corruption did indeed take place in South Africa's much publicised arms deal, it is a reasonable assumption that 'someone out there' is in possession of, or have access to documentary evidence to prove such corruption. It is also reasonable to assume that such 'someone' will think twice before making such evidence available without adequate protection. Such protection has to be in terms of the workplace but, even more importantly, in terms of his personal life and those of his family. The perception of the adequacy and sufficiency of the protection, we argue, will be a deciding factor to the prospective whistle-blower when deciding (a) to blow the whistle or to remain silent and (b) to reveal his identity or to remain anonymous.

Anonymity – guaranteed anonymity – is essential, especially when the stakes are high. The current ways of providing anonymity to whistle-blowers have built-in weaknesses and, as a result, seriously jeopardise the safety of whistle-blowers and their families. If a way can be found to guarantee anonymity, we suspect that more people will be prepared to volunteer information about wrongdoings, including, and especially, about corruption.

The point has to be made that the current ways of facilitating whistle-blowing (for example, crime lines and all of the others) must remain in place. An *additional* way of blowing the whistle is required; a way to *guarantee* anonymity.

TECHNICALLY SAFE ENVIRONMENT

The idea is to create an additional channel to the existing ones for whistle-blowing, but a channel which guarantees anonymity. It is, however, doubtful if the ideal of a 100% guarantee will ever be achieved, simply because of the very nature of technology. Technology advances at a rapid rate and newer technology is always available not only to legitimate users, but also to those wanting to exploit it for selfish or illegitimate purposes. This makes a '100% guarantee' a theoretical impossibility.

Despite this, it is still, in our opinion, meaningful to try and get as close as possible to the goal so that, when the prospective whistle-blower does his risk assessment, an outcome in favour of blowing the whistle is still achieved. It is hoped that such a safe environment will encourage

prospective whistle-blowers to deliver their messages and evidence to law enforcement authorities.

Email

Telephone based technologies for providing the safe environment do not hold much promise, whether land-line based, public or wireless. One therefore has to look for a different kind of technology and email seems to be the next logical choice.

Apart from technology constantly changing, it is quite a daunting task to design an environment where the originator of an email message cannot be traced. Every computer which a log on to a data communications network anywhere in the world gets a unique number assigned to it at the moment of logging on. This 'number' is referred to as the Internet Protocol (IP) address. This IP address is - unknown to most email users - always transmitted along with the message, irrespective of where the message originates or where it terminates. Even when logging onto a website, the website is 'aware' of the IP address of the computer logging on[2]. The IP address is typically (and deliberately) not under the control of the user of the computer with the result that a user will not be able to hide this unique identifier. An ordinary whistle-blower, for instance, would certainly not have the technical skills to send a message by hiding the IP address assigned.

In trying to design a technically safe environment, one cannot, therefore, simply advertise an email address as a means for whistle-blowers to inform organisations or law enforcement authorities of suspicious incidents. Just like hackers are traced despite their attempts to hide their identities, a non-technical user sending an email would be relatively easy to trace for someone with the necessary technical skills.

Encryption

A commonly used technique to protect the content of an email message (or even data attached as a file) is to encrypt the message and/or the data. This would make it impossible for a pursuer to read the content of the message even if he gets access to it, but the IP address could be identified and that, in most cases, would reveal thewhistle-blower's location and, perhaps, his name.

[2] It is for this reason why one is sometimes surprised to see that a website has identified you as originating from, for instance, South Africa when logging on. A typical example is when trying to log onto www.google.com (the Google service based in the US), one is automatically rerouted to the local website in South Africa (www.google.co.za).

Internet café

One way to overcome the problem posed by the IP address, is for the whistle-blower to send the email from an internet café and, of course, not revealing anything else about his identity in the message. This would make it more difficult for the pursuer to identify the originator despite tracing it back to the originating internet café.

Internet café's, typically, do not keep records of the identities of their clients with the result that the whistle-blower is reasonably safe from that perspective. However, many internet café's record the activities of the clients on video camera, so the whistle-blower could still be identified if the pursuer can trace the message or email back to a particular internet café and then getting access to the video recordings to look for suspects. This, however, will have to be done in a relatively short period of time as the video recordings are typically overwritten after a few days or weeks.

There is another danger that the whistle-blower must avoid when making use of an internet café, namely, the data contained in any attachments to the message. When one creates a document in Microsoft Word, for example, it automatically creates a profile of the user and stores it with the rest of the document. Many users are not even aware that this is the case. Depending on how the computer was set up, the creator of the document may well be easily identified by name and surname without him being aware of it. (This is easily seen by simply clicking on 'File', then 'Properties', then 'Summary' of any document created using MS WORD).

It is easy enough to delete any such identifiers before attaching the document, but whistle-blowers must, firstly, be made aware of the danger and, secondly, remember to do so – consistently - before sending the attachment. Both aspects pose risks to the kind of technically sound environment one ideally would like to see.

TOWARDS A SAFE ENVIRONMENT

To get closer to the vision of a '100% guarantee', one should not have rely on the whistle-blower to, firstly, remove all of the identifying information on attachments, then encrypting the message and data using a robust encryption technique, and then using the internet café to send the email and, even then, run the risk of being traced back to a particular internet cafe.

There are simply too many unacceptable risks in the scenario and something more robust and more reliable must be designed.

Onion routing

The IP address poses a challenging problem. However,

there is a way of getting rid of that in a relatively simple, but safe, way. This opportunity is provided through making use of a so-called 'Onion Routing' facility (Feigenbaum et al., 2007). This facility was originally developed by the United States Naval Laboratory for the purpose of *'protecting government communications'* (TOR Project 2011).

This facility makes use of several websites situated around the globe at undisclosed locations. The user 'drops' a message or data into a 'drop box' typically provided by the advertised website for whistle-blowers. The message is then automatically routed in a random route from one location ("node") to several others (called a 'tunnel'), at the same time, automatically stripping away originating IP addresses. After passing through a random number of nodes, the message is eventually delivered to the receiving party but the receiving party only sees the IP address of the last node sending the message. This IP address is simply one of the many nodes in the Onion Network and of no use to anyone, hence guaranteeing anonymity to the originating node and, the originator.

Ironically, the Onion Network was developed by the US Navy to safeguard government communications, but this very same network was used by the Wikileaks[3] organisation to publish government cables and other documentation which caused such an embarrassment to the US Government (and others). Not even the US Military or Navy was able to trace the originator of the documents published on the Wikileaks website. The fact that Bradley Manning was eventually identified as the whistle-blower happened as a result of Manning revealing his identity to someone else whom he thought he could trust and who then disclosed it to the US government (Leigh and Harding, 2011).

The claim is made that the Onion Routing facility provides 'provable anonymity' (Feigenbaum et al., 2007) and this facility is available, free-of-charge, to anyone caring to use it. Of course, this claim only applies to the technical environment used to facilitate anonymity. From what can be gathered in the literature, using the Onion Network is relatively simple as the user is isolated from the technical complexities associated with the network.

Potential solution

Our solution involves a combination of the aforementioned, in the following process:

1. The whistle-blower goes with the evidence to an internet café
2. The whistle-blower drops the message and/or data into an electronic drop-box provided by the whistle-blowing organisation
3. Any data in the message or in the documents that could identify the sender is automatically deleted by the website when dropped in the box
4. The message and data get encrypted automatically by the website
5. The message and data is sent to the whistle-blowing organisation through the TOR network
6. The whistle-blowing websitedeliberately does not keep any logs of email received so that they would not be able to provide information whatsoever about the originator, even when forced to do so with a court order
7. The whistle-blowing organisation waits at least 14 days before making it available to law enforcement authorities so that video recordings at the originating internet café are likely to have been overwritten.

CONCLUSION

The scale of corruption in South Africa, and, for that matter, everywhere else in the World, is unacceptably large. Many African and other countries have poverty problems of immense magnitudes and cannot afford to waste billions of currencies to enrich a few corrupt individuals at the expense of the majority of the citizens. This money could go a long way to improve living conditions, healthcare to and education of the poor.

In this respect whistle-blowing plays a very important role. Detection of corrupt deeds is in the hands of people of integrity to observe such corrupt deeds and report them to the relevant authorities. Such reporting carries huge risks, including loss of life, damage to property and/or dismissal or victimisation in the workplace.

Whistle-blowers deserve to be protected. Such protection must be rooted in the legal framework but it needs to be complemented by mechanisms that allow whistle-blowers to remain anonymous if they choose. Such anonymity must get as close to a 100% guarantee as one could possibly get.

RECOMMENDATIONS FOR FURTHER RESEARCH

This paper aimed at stimulating academic research on the topic. The topic can broadly be defined as the use of ICT in the fight against corruption. This paper only looked at one aspect of such broad topic, namely, anonymous whistle-blowing.

It is recommended that further academic research gets initiated. For instance, a theoretical framework describing the use of ICT in the fight against corruption could be useful. An Actor Network Research (ANT) approach to

[3] We must point out that we do not necessarily endorse or support any of the actions of the Wikileaks organisation. The Wikileaks organisation has its own objectives and we have our own. Yet, we do not want to pass judgement on what the Wikileaks organisation set out to do. The fact that we are proposing to use some of the same network technology (which technology does not belong to the Wikileaks organisation) must be seen as purely coincidental.

the topic is currently being investigated by the author to provide insight into the actors and the roles played by the actors in the corruption phenomenon.

ACKNOWLEDGEMENT

The initial research was partially supported by the German Development Cooperation (GIZ) awarded to Citizens against Corruption, a non-profit company.

REFERENCES

Calland R (2011). Blow the whistle at your peril. Mail and Guardian Online, Oct 17.

Camerer L (2001). Protecting whistle-blowers in South Africa: The Protected Disclosures Act, no 26 of 2000. Occasional Paper no 47, Institute for Security Studies.

Colvin G (2002). Wonder Women of Whistleblowing. Is it significant that the prominent heroes to emerge from the two great business scandals of recent years were women? Fortune Magazine, August.

Ellison FA (1982). Anonymity and Whistleblowing. J. Bus. Ethics p. 1.

Feigenbaum J, Johnson A, Syverson P (2007). A Model of Onion Routing with Provable Anonymity. Financial Cryptography and Data Security, 11th International Conference, FC.

Leigh D, Harding L (2011). Wikileaks. Inside Julain Assange's War on secrecy.Guardian Books, London.

Mail and Guardian Online (2007). Frere Hospital whistle-blower fired. 28 September. Cited on 23 October 2011 at mg.co.za/article/2007-09-28-frere-hospital-whistleblower-fired.

Martin P (2010). The Status of Whistle-Blowing in South Africa: Taking Stock. Open Democracy Advice Centre, June.

Martin P (2011). Corruption.Towards A Comprehensive Societal Response. CASAC March.

Miceli MP, Rehg M, Near JL, Ryan KC (1999). Can Laws Protect Whistle-Blowers?: Results of a Naturally Occurring Field Experiment. Work Occup. 26:129.

Near JP, Miceli MP (1985). Organizational Dissidence: The Case of Whistle-Blowing. J. Bus. Ethics p. 4.

Public Protector (2010). Address by Public Protector AdvThuliMadonsela during the Open Democracy Advice Center (ODAC) Conference on whistle-blowing held in Johannesburg, Wednesday, 17 November 2010. Cited at http://www.pprotect.org/media_gallery/2010/17112010_sp.asp.

Republic of South Africa (2000). Protected Disclosures Act 2000, Act 26 of 2000. 7 August. Government Gazette p.422.

Republic of South Africa (2004). Prevention and combating of corrupt activities 2003, Act 12 of 2004. 28 April. Government Gazette p. 466.

Republic of South Africa (2008). Companies Act, Act 71 of 2008. 9 April 2009. Government Gazette p.526.

Republic of South Africa (2011). Companies Amendment Act, Act 3 of 2011., 26 April 2011. Government Gazette p.550.

Syal R (2010). Tenfold rise in whistleblower cases taken to tribunal. Campaigners fear workers deliberately undermined despite repeated promises to protect them. The Guardian, Monday, 22 March 2010.

TOR Project (2011). Cited at https://wwwtorproject.org/about/overview.html.en.

Treasury (2011). Medium Term Budget Policy Statement 2011: Speech by the Minister of Finance, Mr PravinGordhan. Cited at http://www.info.gov.za/speech/DynamicAction?pageid=461&sid=22685&tid=47198.