Un-appointed Hackers: Should They Be Compensated?

Yonnique Francesca Goliath

A Research Report submitted to the Faculty of Humanities, University of the Witwatersrand, Johannesburg, in partial fulfilment of the requirements for the degree of Master of Arts, Applied Ethics for Professionals

Johannesburg, 2019.

Abstract

Cybersecurity and data privacy have been prioritised by financial institutions due to legislative requirements, an increase in system security breaches, and in fulfilment of their obligations to their stakeholders. This paper discusses stakeholders' interests, the moral duties of financial institutions, and the harm caused by hacking activities, in the context of data security. Specifically, the paper seeks to answer the question whether un-appointed hackers, who alert institutions to their security vulnerabilities and do not have malicious intent, should be compensated. Stakeholders' interests and financial institutions' moral duties are considered in the context of the stakeholder theory, and Kantian norms. I argue that financial institutions should not compensate un-appointed hackers, because hacking violates the principle of respect due to the data subject, and the financial institution's moral duty to act in the interests of its stakeholders.

Declaration

I Yonnique Goliath declare that this Research Report is my own unaided work. It is submitted for the degree of Master of Arts, Applied Ethics for Professionals, in the University of the Witwatersrand, Johannesburg. It has not been submitted before for any other degree or examination in any other University.

_____

Yonnique Goliath

_____ day of _____, 2019

Acknowledgements

I would like to thank my supervisor for the guidance and honest feedback, and the Cybersecurity Executive who made time to meet with me and share some insight into the industry. A special thank you to my partner, Marek Hanusch, for supporting me during my late nights and for believing in me. Thank you, Mommy, for the paying my registration fees, and thank you to my employer for my bursary and study leave throughout the programme. This one is for me.

Contents

1. Introduction

South Africa is no exception to the lucrative, fast growing industry of cybercrime. Statistics released by the South African Banking Risk Information Centre (SABRIC) in 2018 show that for 2017, 13 438 incidents of cybercrimes were reported to the SABRIC taking place across online banking platforms (Smith 2018, Fin24). This excludes the incidents that financial institutions (FIs) are not aware of or choose not to disclose.

Cybercrime is listed as one of the top risks being managed by the financial services industry. To respond appropriately, it is imperative for companies' boards and management structures to understand the respective company's role in combatting cybercrime and its strategy for implementing secure digital platforms. Companies should also prepare for system and data security breaches, which includes having the necessary governance frameworks and policies in place. Cyberattacks and security breaches arise unexpectedly, and companies do not have the luxury of time to consider risks, best-practice and available response-strategies. It is therefore necessary for companies to be proactive in addressing cybersecurity and its related events. Following a proactive approach ensures that FIs take the time to consider their stakeholders' interests and the FIs moral duties which will equip them to react appropriately to cyber risks.

This paper will argue that FIs should not compensate un-appointed hackers who alert institutions to their system's security vulnerabilities without malicious intent. While I believe the discussion can inform the decision of any hacked company, I will specifically focus on FIs due to their role in the economy, as well as the trust relationship required for their sustainability. The G30 Report on Banking Conduct and Culture states:

> In addition, from a societal perspective, many people believe that banks have an integral role in supporting individuals, businesses,

> communities, and the economy more widely by providing, in an appropriate fashion, complex products and services that are needed for the financial health of individuals and economies. And, as such, the financial services industry should be held to a higher standard than other industries.

What follows in Section 2 is a discussion on the value of data and privacy. Section 3 is an analysis of different hacking activities and hackers' motives. Section 4 includes an overview of the stakeholder theory, Kantian norms, and corporates' social responsibilities. Section 5 highlights the South African legislative framework applicable to cybersecurity and information privacy. Given the discussions held in the preceding sections, in Section 6 I argue against compensation are consider potential opposing arguments.

2. The Value of Data

Databases are valuable to FIs for many reasons including that they allow them to understand the value of their book in relation to the number of customers, which further presents cross-selling opportunities. Data therefore not only represents current value, but also the potential future value to be derived from the current database. In addition, data derives its value from its confidentiality as it presents the holding FI with a competitive advantage. For this reason, stealing databases through hacking and ransomware can result in high financial rewards for the hacker. These financial rewards result from requests for ransom or bounties from the institutions owning the database, or the sale of the data to third parties, including other hackers. Black hat hackers are more often the requestors or acceptors of compensation because their requests are often accompanied by threats and intent to do harm, which will be further discussed in section 3. Hackers understand how much companies value the data in their possession. Therefore, hackers believe that their requests for compensation will be

considered due to the possible harm that could be caused to the company should they refuse to respond positively to the request. Cyber extortion occurs through withholding data and system access for ransom, which is the *modus operandi* for ransomware and denial-of service attacks (DDoS) or threatening to sell data or security vulnerabilities to a willing buyer.

Not all data are private as there are data that already exist in the public domain and viewing data from internal to the FI's systems could be no different from cutting and pasting the data from public websites. This does not mean that public data poses no risks. Hackers could still amend information, remove it, or use the information to duplicate the online site creating a fake site. The unauthorised access breach and the ability to amend the data is what is at risk in this instance. Therefore, while this category of information is not private, access to it is still secured. The reason for the breach is more likely due to exploiting security vulnerabilities rather than stealing the information, as is the case with private information.

The value of data is largely determined by the content of the data, what it can be used for, as well as the quality or integrity of the data. If data have expired, it can be deemed less useful. Data expires when it is no longer relevant because it is outdated, not deemed useful, or new data is available. Data can be permanent or non-permanent. Permanent data includes biometrics and identity numbers, for example, because once they are stolen or observed they remain relevant for the duration of the data subject's life. This does not mean that non-permanent data are less valuable. Passwords, contact details, and status falls into this category, and it is easy to understand its worth. There are cases where data generally regarded as permanent can change, for example through sex and name changes; or where non-permanent data becomes permanent. An example of the latter is if people use the same physical address for the duration of their lives. Security measures should therefore be applied irrespective of the permanency of the data. Extortionate cyberattacks are not always about the value of the data but rather about the value FIs place on having secure systems, sole access to certain data, and the value of the perception that data subjects have of FIs' systems'

security. If system access is denied to customers or the FI's employees, transactions cannot be facilitated which impact revenue as well as the FI's reputation for security. In other words, a cyberattack can cause a temporary shift in power or control from the FI to the hacker in respect of data that the FI should be securing.

Studies on the impact of cyber breaches found that there is a time-value linked to stolen information and that the value of the information decreased over time until a subsequent event or news relating to the initial attack. Once a cyberattack occurs the public's perception of a negative impact is widespread for the duration of the investigation. If the investigation yields no results, the value of the information and the breach may decrease. However, if the information is retained and only used at a later stage when it is no longer expected, the impact of the breach will be limited to those directly affected by the breach (for example, to those whose credit cards have been used compared to the perceived broader impact), including the FI (Hovav and Gray 2014, 896).

Consolidated data creates a data subject's profile, and access to it shares the most personal details of a data subject's identity. FIs obtain customer data at different stages and intervals dependent on the customer's profile. Due to policies internal to the FI, they may require and retain more information about their customers than required by The Financial Intelligence Centre Act. To meet the minimum standards for anti-money laundering and countering terrorist financing controls, FIs divide their clients into high, medium, or low risk profiles. I will not be discussing this further but would like to highlight that clients included in the high-risk category could be politically exposed persons, or persons against whom adverse media exists. In addition to understanding risk profiles, the purpose of obtaining the specific client information is to *know your customer*, determine credit worthiness, and to understand additional cross-selling opportunities. While the type of data protection afforded to customers should not differ depending on the profile of the customer because respect to customers should be applied equally, data protection may differ across industries or dependent on the sensitivity of the

data. Where the implementation of data protection measures is relatively immature, companies may deem it acceptable to prioritise the protection of high risk client data, given the reputational risk, to the company and the specified clients, personal risks to the clients, and damages that may result from a control weakness. Certain high-risk customers' information could be more sensitive to public scrutiny and if their information are publicly disclosed, the disclosure may have other socio-economic consequences to the country's stability. In other words, FIs have a duty to equally protect all of their customers' personal information, however where it is not practically possible to provide the same level of assurance to all customers, a risk-based approach is likely to be followed which could result in certain information being more secure than others. A security trespasser can derive value from data without databases being copied, amended, or removed. Being able to view data allows the trespasser to draw possible uninformed conclusions regarding the content of the data which could have negative consequences for the data subject, for example, if a member of parliament's bank transactions were made public. However, Wolf and Fresco states that "even when the database is still intact, metadata about the database, such as assumptions regarding the security of information in the database, have been violated, and thus the attack instils entropy in the infosphere" (Wolf and Fresco 2016, 271). In other words, when security vulnerabilities are exploited, and access is gained to data, the access to the system in itself is unwelcome and disruptive. The access breach disrupts the security status quo, because the negative perception created by customers about the security of the data due to the breach may be harmful, despite the database being intact.

The transfer of personal information from the customer to the FI is voluntary to the extent that it is required for initiating a contractual relationship. Customers choose to open account with a FIs, and as a condition to fulfilling the customer's request, prescribed personal information is required by the FIs. Because the requested information is mainly prescribed by legislation, all FIs will request at minimum the same list of information. It is different if personal information becomes accessible to a hacker during a breach because firstly, it was not voluntarily provided

by the data subject (the customer) and was in the FIs care, and secondly, there was no regulatory or contractual requirement or reason for the personal information to be provided to the hacker. The personal information was in the FI's care which meant that the FI has a duty to keep the information safe and make it accessible only for the purpose contracted upon. The disclosure of personal information by the FI to third parties is in the normal course of business. For example, personal information is accessible to an FI's vendor if the FI uses their vendor's system as part of the account opening process. Customers contractually consent to having their personal information disclosed to these third parties, chosen by the FI, to facilitate the service to the customer. The FI is bound to the customer by their contractual obligations relating to the handling of data. Therefore, the customer's recourse in the event of a data security breach will first and foremost be to the FI irrespective if the breach is due to third party negligence. The FI's recourse to its vendors is a separate issue and does not concern the customer. "The unifying feature of privacy incidents is the violation of certain expectations about how data will be handled. [A]n individual has an expectation of being able to control the flow of personal information, and restrict access where appropriate" (Acquisti *et al* 2006, 1555 - 1566). However, as previously explained, fulfilment of this expectation is not practically possible and is also not reasonable in the customer's relationship with a FI. The only control the customer has is the decision to release the information to the FI. Thereafter, the flow and access restriction to the personal information are the responsibilities of the FI.

3. It is more than *just* hacking

In this section I will provide brief distinctions between hacktivism and vigilantism, bounty hunting, and grey hat hacking. I have chosen these groups because despite varying nuances between them, their profiles and activities generally fit those of the type of hacker relevant to this research.

Hackers are generally divided into three categories namely, black, white, and grey hat hackers. Black hat hackers are known for their malicious intent. Their activities are aimed at causing harm to both the hacked company, and stakeholders whose data have been compromised. Black hat hackers' efforts result in theft, requests for ransom, and fraudulent use of private information. White hat hackers include employed or contracted security researchers or "ethical hackers" who conduct penetration testing, which Cloudflare defines as "scaling planned attacks against a company's security infrastructure to hunt down security vulnerabilities that need to be patched up", to enable these companies to improve their cybersecurity (Cloudflare 2018). Similarly, Microsoft, Apple and Google have advertised bug bounty programmes which invite hackers to find vulnerabilities and to report them in a prescribed manner.

The defining differences between white hat hackers and black hat hackers are that white hat hackers have permission to perform their activities, are contractually bound, and will not threaten or disclose their findings except to the authorised company by whom they were contracted, or recognised bug bounty programmes. White hat hackers operate within the realm of the law. If white hat hackers are the good guys and black hat hackers are the bad guys, grey hat hackers operate in the grey zone in between, and are therefore considered to be on the fence of morality. They are neither categorised by the malicious activities of black hat hackers, nor as well-intended as white hat hackers. Their activities range from acting as agents for state intelligence research, to acting as hacktivists for matters which they believe are to the public benefit (Hartley 2015, 3).

The hackers relevant for my research, I believe, are also in this grey zone. They are neither black hat hackers because their intentions are not extortionary or malicious, nor white hat hackers, because they are not employed or contracted to test the security of the respective company. Instead, they are more closely associated with grey hat hackers. While their objectives may be well-intended or at least not intended to have harmful consequences, they are accessing data and breaching security infrastructure without consent and often without

warning. The hackers relevant to my research are those who hack systems and provide the hacked companies with the discovered vulnerabilities in their systems, the data found, and in some instances, provide a solution to the discovered vulnerabilities or patch them. These hacks take place for various reasons and are often accompanied by requests for compensation or donation. These are not requests for ransom, as the vulnerabilities and data are voluntarily provided, even sometimes unconditionally.

White and grey hat hackers are often both referred to as ethical hackers. I will refrain from using the term “ethical hackers” as it is too broadly defined and carries the risk of being misinterpreted. Grey hat hackers, in comparison to other types of hackers, are relatively scarcely researched. For this reason, I have specifically described that the hackers relevant to my research provide the FI with its security vulnerabilities and do not have malicious intent. They generally request compensation from the FI for their submission. They may be grey hat hackers, but it is important to note that not all grey hat hackers request compensation.

One of the reasons that grey hat hacking is scarcely researched is that companies are not forth-coming about the nature of these hacks, and if requests for compensation are made, companies do not disclose these requests possibly because they are not sure about their stance on the matter, or do not apply a consistent approach and do not want to be challenged on the decision taken.

FIs are however publicly listing cybersecurity as a prioritised risk being attended to. General Electric (GE) has the following statement published on their website:

> GE regularly partners with researchers, academia, government, and coordinating authorities to continuously assess for vulnerabilities and improve security in our products. In addition, GE regularly discloses to its customers mitigations and remediation for GE product vulnerabilities, both directly and in cooperation with coordinating authorities. Consistent with responsible

> disclosure practices, GE does not publicly communicate information concerning vulnerabilities unless a remediation is available.

Noteworthy is that General Electric mentions partnering with researchers, and this is a broad category that could include grey hat hackers. After all, the hacking industry is also called security research. FIs disclosing their use of penetration testers could become more common but is currently not the norm. Instead of only disclosing if a security or data breach occurred which could prove to impact customers, General Electric goes further and discloses not only vulnerabilities but also mitigation and remediation of these product vulnerabilities. The disclaimer that the information will not be provided unless a remediation is available highlights the company's awareness of the risk associated with these disclosures. FIs generally do not disclose that they have been approached by hackers or that they have bug bounty programmes, due to the perception it might create with customers and other stakeholders.

In 2013, Khalil Shreateh found a bug which allowed Facebook users to post on others Facebook users' pages even though they were not linked as Facebook friends. Khalil informed Facebook's security team about the bug, but they disputed the validity of his findings and did not give the matter the attention that Khalil believed it deserved. To prove his point, Khalil, who was not Facebook's Chief Executive Officer Mark Zuckerberg's Facebook friend, posted a message on Mark Zuckerberg's Facebook wall. He reported that he had told the security team that doing so was possible but did not do it initially as he respected Mark's privacy. Khalid's note included an apology for violating Mark's privacy which shows that there was a clear awareness that although the disclosure of the bug was important, it included a violation of privacy. For Khalil, the need to disclose the bug and have it corrected exceeded Mark's right to privacy.

Facebook usually offers a minimum reward of $500 for vulnerability disclosures made in accordance with their bug bounty programme. The disclosures of these bugs or vulnerabilities have to follow strict requirements. Khalid did not qualify to receive the bounty because he did

not adhere to the requirements of the programme. In a public statement issued by Facebook it reported that “we will not change our practice of refusing to pay rewards to researchers who have tested vulnerabilities against real users. It is never acceptable to compromise the security or privacy of other people” (Facebook Security, 2013).

More recently, Eskom proved that they were not prepared for the cyber risks they were asked to address. “[R]esearcher Devon Stokes accused Eskom of ignoring his complaints that the power utility’s live customer database, including credit card and other payment details, had been exposed online” (Moyo 2019, ITWeb).

The approach taken by many FIs not to discuss issues of cybersecurity with the public is understandable. The caution, and perhaps fear, prompting this sort of response has been justified by instances like the Liberty Holdings cyberattack. The South African financial services provider recently refused to pay a hacker after being threatened by the release of confidential information. The decision not to compensate was made easier by the FI’s confidence that the hacker did not have access to materially sensitive information. The extent of Liberty’s security and data breach was reported to be limited to mainly emails and attachments (Cranston 2015, Business Day).

In light of proven extortionate behaviour by hackers, it may be irresponsible especially for FIs to follow the approach taken by Google and Facebook to invite hackers to find vulnerabilities, albeit in adherence to policies. Instead, it can be argued that in being a responsible corporate citizen effort should rather be directed at putting long term, sustainable measures in place to improve system security.

As seen above, South African FIs have also been targeted by hackers in the grey zone and are not naïve about the impact of these security breaches or the likelihood of reoccurrence. In the opinion of an IT security executive from one of the leading South African FIs, all bug

bounties break the law (personal communication). However, FIs have still listed contact details on hackers' network platforms to indicate where vulnerabilities can be reported securely. This was clearly absent in the Eskom case. While permission will never be granted to these hackers, the executive highlighted that their work is also not discouraged due to the benefit derived from the awareness of the vulnerability.

Although hacktivism, vigilantism and bounty hunting are distinguishable from the hackers relevant to this research, there are similarities worth noting. The different types of hackers highlighted in these sections are all human beings and are all motivated by what they believe to be a higher moral purpose. Yet, humans are fallible and are therefore "not pure moral beings and even when we act in accordance with morality we still cannot know what our deepest motives are" (Kant 1996 [1797], 196). FIs should therefore not consider the hacker's motives in deciding the best moral action to take. Hackers may believe that there they have a certain motive, but they may just not be acknowledging what their true desires are when hacking and causing harm.

Hacktivism is a form of activism through hacking or computer network disturbances. An act of hacktivism is usually associated to a political or social agenda on the part of the hacker. While the political agenda may be somewhat personal to the hacktivist, he could also be acting on behalf of an activist group with a shared agenda. For example, the hacking group Hazmah Uygun targeted a few South African companies in 2014 stating the group's stance on the ongoing conflict about the Western Sahara's independence. The hacked companies' website displayed the message "The Sahara is Moroccan". This hack was apparently in protest of companies operating or making a political statement on the matter (van Zyl 2014, Fin24).

I do not agree with Delmas's argument that "[t]here is no lawful online equivalent of protesting outside a company's storefront or headquarters. To do the latter, hacktivists must digitally trespass on private property" (Delmas 2018, 66). The argument appears to justify digital

trespassing. In the digital age of Twitter, Instagram, and Facebook, it is easier to get the attention of companies by disgruntled members of society tagging the company in complaints posted online. Posting these complaints online is not unlawful, especially if it is factual and cause no harm to others and does not breach a contractual relationship with the company. Street protests can be easily shut down by law enforcement officials with some even using violence. Even peaceful protesters can be arrested and charged for not dispersing. Enforcing governance is more complicated online. It is likely that once the protest is posted online it will be available online for a long time. It will only be removed by the poster (and even in these instances it will not really be removed as it may have been screenshot or reposted by others) or if flagged as breaching the search engine or platform's policies. Hacking is a more severe form of an online complaint or protest and is more difficult for the company to address. Firstly, the protester might not be detected, because the hacker could trespass unnoticed or in a manner that is not traceable to an individual. Secondly the rules governing online protests will not be clear, that is if they even exist. There are conflicting arguments as to whether hacktivism is morally acceptable as a protest activity. It may be easier to prove that hacktivism is an illegal activity. From a corporate perspective, online privacy policies and questionable ethical business conduct can attract hacktivist attacks. Hacktivists are faced with an ethical trade-off between the dignity of private information and the social or political duty to expose corporate misconduct. The trade-off is similar to the one made by Khalil on the Facebook matter.

Compared to hacktivists, grey hat hackers are less politically motivated (although they may act at the request of government officials) and are instead intrigued or motivated by the technological challenge which validates their skills. Furthermore, while the awareness and threat created by hacktivists could be the intended outcome (besides having their target change their position), they rarely seek monetary reward, and will not provide the targeted institution with security insight about their vulnerabilities.

Due to the ambiguity of the terms “grey hat hacker”, “security researcher” and “ethical hacker”, going forward when referring to hacker, I mean an un-appointed hacker, one who has not been asked to research vulnerabilities or been given approval to access systems or information, but still does so and requests voluntary compensation or a donation for his findings.

Hacking generally has a negative connotation associated with it which has created challenges for hackers in their attempt to brand hacking as a credible and recognisable profession. In the case of hackers and hacktivists, similarities can be drawn with terrorist activities which include hacking state intelligence servers or confidential information related to military plans. The activities of the hackers, hacktivist, and terrorists are all executed with believed morally worthy purposes in mind. I am inclined to say that another similarity is that their activities can be described as paternalistic because they interfere or restrict the data subject’s or state’s liberty in pursuit of a different interest, for example welfare, profit, national security or other predefined objectives. Hacktivists and terrorists associate their actions with a duty to the public, country, or religion, as their primary motivation. Hackers differ from hacktivists and terrorists in that there is no perceived moral or public duty associated with infringing the privacy of the customer. Hackers have no responsibility, including no perceived responsibility, to protect the data subject or to enhance an FI’s security.

Vigilantism occurs when people or institutions take the law into their own hands by personally causing harm to another instead of following the legal process. The vigilante takes on the role of a regulator or law enforcement official without the authority to do so. “Digital vigilantism” can be defined as the “illicit use (or credible threat of use) of computers and computer networks, motivated by a concern for justice or the good of the (online or offline) community, undertaken by agents who are not willingly accountable to the state, for the purpose of controlling (preventing, punishing, and/or retaliating against alleged wrongdoer (individuals, corporations, institutions, states)” (Delmas 2018, 72). Delmas suggests further that vigilantes’ conduct could

be justified dependent on the means used, if it does not “unjustifiably intimidate”, has a “legitimate target”, and is conducted in a situation where it would not be expected that a regulator would address the matter. I do not agree. Gaps in the law, and the state’s failure to act should not automatically permit vigilantism. Gaps in the law perhaps create an opportunity to act due to less governance around the matter but should not promote action. The appeal of vigilantism can however be understood, specifically in South Africa where crime is rife, law enforcement is under-resourced, and the justice system strained. The digital economy and its impact on privacy were recently legislated in South African law with its enforcement not fully understood. Despite this, vigilantism cannot be justified. There is a difference between morality and the law. Not everything considered to be immoral is legislated against.

As will be addressed further in this paper, a legal framework is required to maintain order and to promote freedom and the protection thereof. These laws are regarded as moral duties which dictate the behaviour and actions between rational beings. Kant believes this is necessary as people are not able to live in an orderly manner, respecting others’ rights, in the natural state described by philosophers like Thomas Hobbes. This, however, does not mean that in the absence of laws, moral duties are also absent.

Because moral duties guide behaviour, people are not allowed to take the law into their own hands. They have agreed to the rational authority to promote and protect freedom and autonomy. The obedience of laws assists with this but is not sufficient. People should rather be guided by their moral reasoning.

Vigilantism and hacking are similar in that they are both digitally opportunistic when laws are absent or vague and both take advantage of these gaps.

Similar to vigilantism, bounty hunting is a means of private intervention in finding perpetrators as an alternative to state intervention. While bounty hunters are generously rewarded,

because of the time, expertise, and risks taken to identify a perpetrator, they have limited physical and legal protection.

In South Africa, bounty hunters are called private investigators and must be regulated by the Private Security Industry Regulatory Authority (PSIRA). Using a private investigator can be costly. They are therefore not generally accessible to the public. There is also an immoral association with the job, which in effect does extensive research into individuals, groups or institutions' history, and activities. During the process, intimate personal details are obtained by the private investigator and are interpreted or provided to the employer as a means to build a case or draw a conclusion. The immorality of the job could be attributed to it not being conducted transparently and is against the wishes of the targeted individuals. The process followed to conduct an investigation is only clear to the one conducting the investigation and possibly his employer. Therefore, the information owner's privacy is being breached without their knowledge because if they were asked, it is likely that they would have chosen to keep the information confidential. Not many people would willingly hand over private information about themselves to a stranger who is conducting an investigation on them to which they did not consent.

In a German court case, two private investigators were convicted for using Global Positioning System (GPS) technology to track the movements of people they were employed to investigate. The judges opined that the use of GPS to track people (presumably without their consent) could not be justified, and that even the police would not be allowed to use that tracking method. In other words, it was against the conduct of conduct and law adhered to by enforcement agencies.

> Given that not even the police would have been allowed to use GPS tracking methods in those specific cases, the district court argued that the methods used by private investigators should also be limited. The judges did not consider

> whether important interests could have justified the data collection in any of the individual cases. (Pues, 2013, 22).

This should not mean that if the police were allowed to track people using GPS, the private investigators would be more likely to be allowed to as well. The responsibility and authority given to regulators and public servants exceed those given to the broader public due to the former's public mandate.

In effect, what a private investigator is being compensated for is the provision of information that the employer previously did not have access to through traditional means. This information includes personal information. The harm to the person being investigated will differ on a case by case basis. If the investigation exposes immoral acts committed by the subject, it is more likely to be justified. However, if the opposite is true, the subject may not ever be made aware that he was investigated. This does not negate the breach. However, the employer will still have access to the same personal information, and the subject's privacy would have been breached. In both instances, the private investigator is rewarded, but maybe more so if an immoral or illegal act was discovered. The German Federal Court stated that "[d]ata collection might exceptionally be lawful if there is a strong legitimate interest. This may, for example, be the case in a situation similar to self-defence" (Pues 2013, 22).

Hacking is similar to private investigation in that the hacker investigates and tests ways of entering into a private system, although the attacked person is most likely a juristic person. While private investigators have the opportunity to be licensed, they do not all follow this route. Similarly, not all hackers are certified.

If successful, the hacker obtains access to a private system and through the process becomes aware of the system's security vulnerabilities. The hacker may have obtained access to a customer's personal information or to sensitive intra-organisational information. The severity

of the privacy breach may hold different weight and confidentiality than evidence obtained by the private investigator. The result of the hack relates to the identification of security vulnerabilities, and potentially exposing its customers to harm. The results of a private investigation may prove corruption, people involved in violent crimes, or even adultery. By this basic comparison, private investigators' activities may be more beneficial to society. The harm or immoral acts were supposedly already taking place at the time of the private investigation. To the contrary, the customers of the FI experienced no imminent harm until security flaws were exposed by the hacker. Had the hacker not investigated, there may have been no harm to the FI and its customers, although it could just be a matter of time until another inquisitive hacker comes along.

For both hacking and private investigation, the materiality of the information and the skill required to obtain the information are contributing factors to the value of the reward or compensation requests.

4. Ethical Theories and Corporate Social Responsibility

4.1 Stakeholder Theory

Stakeholder theory can be defined both narrowly and broadly. In its narrow sense, stakeholders are those who the business will not be able to sustain itself without. For example, customers, suppliers, stockholders, and employees. As per the broad definition, stakeholders are all those who have an interest in, or are impacted by, the goods, services and activities of the business. "[Firms] are expected to exhibit goodwill in dealings with all groups and individuals, regardless of whether individuals or groups are accorded stakeholder status. The difference between this duty and the one owed specifically to stakeholders is that there is no obligation to actively promote the interests of all these groups" (Lea 2004, 207). The requirement to promote stakeholders' interests is very cumbersome, and practically it should

be limited to instances when identified options are weighed based on the impact on stakeholders, rather than making a decision solely to promote the interests of all stakeholder.

Stakeholders can only be identified once a company understands its purpose, function, and impact on society. For the effective management of stakeholders, consideration should be given to the unique needs and methods to address the needs of each identified stakeholder group (Boatright 2006, 123). These interests should be legitimately considered and weighed against what is practically possible for the business to implement and sustain.

Ultimately, when institutions believe in a stakeholder-inclusive approach, their objective should be to create as much value for the stakeholders in fulfilment of the FI's purpose. Trade-offs, however, are part of running a business and this means that for one opportunity to be gained, another opportunity will be lost, for example an infrastructure security upgrade is put on hold to launch a new product. Stakeholders may have competing desired actions to derive the value they require. This results in the company having to make trade-offs. The decision whether to compensate a hacker also requires a trade-off to be made by a FI. The payment is made in lieu of further value creation for stakeholders. For stockholders it means less available capital for dividends, and for other stakeholders it may mean decreased expenditure on community development projects, or performance bonuses. It could also be argued that stakeholders have benefited from the insight gained from the detection of the system vulnerabilities.

Companies should "consider the opportunity costs associated with the ethical dimensions embodied in any and every decision-making situation" (Primeaux and Stiber 1994, 291). In addition, decision-making should both promote and protect the interests of the stakeholders (Boatright 2006, 123). When stakeholders have competing interests, they are not necessarily in conflict. Instead, due to time constraints or economic conditions, the company has to prioritise which interest is the most pressing to address without compromising business

objectives. Opportunity costs in decision-making are limited to ethical considerations affecting stakeholders per the narrow definition. The monitoring and guidance of these decisions should be performed by FIs' social and ethics committees at board-level. The mandate of this committee is deemed so important that it is a legislative requirement that all companies listed on the Johannesburg Stock Exchange must have a social and ethics committee. The utilitarian theory is closer aligned to the broad definition of stakeholder theory because utilitarianism applies "universally – that is, to all who are affected by the decision, not just an individual" (Jones *et al* 2007, 138). An FI cannot effectively consider opportunity costs for such a broad group. However, the opportunity costs affecting this broader group can be considered by policy-makers, industry-bodies, or through other focussed reviews.

Stakeholders have rights and duties. For example, as a stakeholder, an ordinary stockholder has the duty to elect directors at a FI's annual general meeting and have the right to receive notices of stockholder meetings in the prescribed manner. Yet, rights and duties are not absolute in terms of South African law.

Kantian ethics and the stakeholder theory meet at the topic of respect for persons (which will be further discussed later in this section). FIs believe that stakeholders, narrowly defined, are essential to their sustainability as stakeholder-support is required for commercialisation, operability, and for the FI to have an effective and lasting impact on society's welfare. Therefore, to obtain stakeholder buy-in and trust, the FI has to be seen to be providing a benefit to society. This is evident in the purpose of sustainability reporting which is used to demonstrate organisations' social mandate. Because stakeholders are valuable in themselves, and not as a means to an end, their inputs and interests must be respected by the FI. Many companies who have subscribed to the Sustainable Development Goals, Global Reporting Initiative, among others, have an increasing number of sustainability reporting requirements to meet. The report should include the impact of the FIs products and services on the community, as well as any additional impact made on the community. However, in most

instances, when the report exists, it highlights positive actions as opposed to the FIs negative duty to society.

The main "convergent theme" across ethical theories is "a concern for the interests of others, as opposed to self-interest" (Jones *et al* 2007, 137). This theme is clearly present in the stakeholder and utilitarian theories, as well as in the Kantian principle of respect for persons.

4.1.1 Stakeholders

Having discussed the stakeholder theory, I will now highlight the relevant stakeholders and the impact that a data breach will have on them, as well as the impact of a decision whether to compensate the hacker.

To determine the stakeholders a distinction should be drawn between those impacted by the security and data breach, and those impacted by the decision to compensate the hacker. The distinction is necessary because they may be different stakeholder groups with different interests. Jones *et al* discuss their model of Moralist Cultures and Stakeholder Salience.

> Moralist firms have a genuine concern for stakeholder interests, making legitimacy the *primary* driver of salience for their managers. However, moralist firms are also sensitive to power issues, since power may give stakeholder derivative legitimacy, a *secondary* driver of salience. Since urgency provides impetus for stakeholders and firms alike to deal with legitimate concerns, it is a booster of salience generated by either legitimacy or power (Jones *et al* 2007, 152).

Jones *et al* also explains how corporate egoists, companies "acting exclusively in [their] own self-interest", determine stakeholder salience.

> Since powerful stakeholders are most able to adversely affect corporate outcomes, power will be *primary* driver of stakeholder salience for corporate egoists. Shareholders with large holdings, workers with strong unions, high-volume customers with alternative sources of supply, and governmental agencies with relevant regulatory powers are likely to be salient to these firms.

The stakeholders relevant to this research will be customers, stockholders and competitors. The primary stakeholders who will be directly impacted by the security and data breach are customers and secondly, stockholders and competitors. All stakeholders will be impacted by the decision whether to compensate hackers, however the impact of a security breach will mainly affect stockholders and competitors, although competitors may be affected through the perception of the security of the industry.

While regulators are not being listed as a stakeholder, their role will be to maintain confidence in the financial market. In reality, regulators and employees (including management) are also salient stakeholders to FIs, despite them being excluded from the group of stakeholders for the purpose of this research. The reason for this is that legislation is clear on the action to be taken against data and security breaches. The current obstacle is that the legislation has not been fully rolled out yet. This impedes the regulator's ability to function effectively. While regulators are important stakeholders to financial institutions, when it comes to security and data breaches, or the decision to compensate the hacker, their interests have already been clearly articulated in legislation. Due to the fulfilment of their legislative oversight and monitoring role, the protection and consideration of their interests are less open for debate. Security breaches do not always result in a breach of personal information. Similar to customers, employees could also be affected by a data security breach as FIs also retain personal information about their employees. The information includes copies of identity documents, resumes, qualifications, bank account details and salary information. An FI's

obligation to protect the privacy of employees' personal information is equal to the obligation to protect the personal information of customers. The differences between employees and customers (besides contractual agreements) are that employees have less flexibility to leave the FI. Customers can switch to a different FI in a matter of hours. Given the economic conditions and the job market, employees do not always have the same flexibility. In most cases, FIs' employees are also their customers so what is covered in the section discussing customers will also relate to employees. For that reason, I do not deem it necessary to add employees to stakeholder list below, although I agree that they are salient stakeholders.

The following stakeholders will be discussed below; customers, shareholders, and competitors.

4.1.2 Customers

The customers' perception of how safe FIs' transactional channels are affects how often they will make use of them. In many instances they may not have been personally affected by a previous privacy breach, but they fear the possibility of a future breach occurring. Customers' fear could limit FIs' growth or strategy to transition to digital channels and out of physical branches. This will become less of a risk with a natural move to a more digital landscape with increased digital education and awareness. Companies are moving away from requesting customers to present their documents in person to instead sending certified copies via email. This presents its own security challenges. In most cases individuals will not have access to encryption technology, and therefore their personal data is already at risk when being electronically sent to the FI. Inconsistencies exist in obtaining customers' personal information. While some digital channels allow secure upload options, in certain instances it is still acceptable to email personal documents, and when delivering hard copies to a bank branch, it is uncertain whether the secure retention and timely destruction procedures are followed, despite this being a requirement in the Protection of Personal Information Act. While these

methods pose a risk to the customer it is generally superseded by the convenience of digital rather than physical submission. Be that as it may, it is less likely that a hacker would seek to target the natural person, unless the theft of data could be lucrative, for example to be used for identity fraud. Customers also consist of corporates (juristic persons) which are presumably more enticing to hackers. Therefore, it is not only the FI that has a high exposure to risk, but also its many corporate customers, which collectively possess more data than the financial institution itself. FIs, as do other industries for example Retail, have many customers, and on this basis alone should be intriguing for a hacker. Beyond this, the FI's customers are also depositing money, transferring money between bank accounts, and making withdrawals which makes the financial industry a jackpot target. The points of entry into the financial system are vaster, and there are thousands of customers using that portal to log in and transact every day.

Customers are at immediate risk once a data security breach takes place, because they experience the instant financial impact of a hack if their data are removed, used, or copied (in the event of a malicious attack). The FI is often not aware of the hack and only becomes aware once alerted to it by a customer who logged into their account and realised that something was wrong. The customer then logs a fraud incident with the bank, which investigates the incident, and returns the money to the client's account if it is due to a fraudulent incident resulting from a security vulnerability. The impact to the customer is less easily identifiable if the hack is undetected, or if there is uncertainty about the extent of data exposed (as was the case in the Liberty incident). Although even in these instances data are at risk.

Customers' relationship with their FI goes beyond their contractual relationship (which generally spans pages long and is not critically considered by the customer, neither up for negotiation between parties). The trust given to the FI is accompanied by a reasonable expectation for the FI to use the customer's personal information responsibly and only for the purpose for which it was contractually intended. Trust is accumulated over time when a

customer believes that the FI is fulfilling its contractual obligations and is acting in the customers' best interest. Trust is diminished or withdrawn once a customer becomes aware of a failure to meet these obligations. Once instance breaching trust is enough to tarnish the trust accumulated over a period of time. "It is only when 'data' is understood to mean 'people' that individuals will demand accountability from those who seek to know them…But the first step towards ensuring the fairness of the new information age is to understand that it is not data that are valuable. It is you" (The Economist 2018, 14). Without the customer, which includes his data, there is no demand for business.

4.1.3 Stockholders

The Companies Act defines a shareholder as, "the holder of a share issued by a company and who is entered as such in the certificated or uncertificated securities register, as the case may be". The act defines a share as "one of the units into which the proprietary interest in a profit company is divided. A share therefore should hold value, and the shareholder holds it for that purpose, namely value or wealth creation. Shareholders are effectively the owners of the company, and therefore an important stakeholder. Besides in case of share incentive schemes, shareholders inject capital into the business, and are required for certain decisions prescribed by the Companies Act.

Milton Friedman is well-known for stating that "there is one and only one social responsibility of business – to use its resources and engage in activities designed to increase its profits so long as it stays within the rules of the game, which is to say, engages in open and free competition without deception or fraud" (Friedman 1970, 51). In other words, Friedman believed that the social responsibility of business is to operate within the framework of the law. Other than that, business' only objective is to be profit-maximising. In accordance with this view, management has a fiduciary duty to stockholders which means that management has a

legal duty to serve the interests of stockholders. Friedman's view is demonstrative of the stockholder theory, which rejects the stakeholder theory proposed in this paper. In accordance with the stockholder theory, the management of stakeholders, albeit employees, customers, stockholders, are done to ensure that the managers consider the interests of their stakeholders to maximise returns to the stockholders. It is in the shareholders' interests that shares perform well, and that there is growth in the value of the shares. This growth results in increased value for the shareholder, and potential increase in dividend pay outs. From the descriptions given by the Companies Act and Friedman, respectively, the shareholders' interest is deemed to be purely financial.

The difference between the stockholder and stakeholder theories is that with the stockholder theory the FI will serve the interests of the stakeholders for profit-maximisation in line with its fiduciary duties to stockholders. With the stakeholder theory, the FI will serve the interests of its stakeholders because in doing so it fulfils the FI's social purpose and is the right thing to do. Stakeholders' expectations of FIs have evolved and through experience FIs have learnt that they need to be stakeholder-focussed to remain sustainable, and to make a lasting impact. For these reasons, and because of the law, FIs have a social responsibility. In other words, FIs are managed to benefit society holistically, beyond just the stockholders and stakeholders' interests will be weighed against each other until an ideal compromise is reached (Hasnas 1998, 26).

As mentioned previously, the FI has a duty to not cause harm. Due to the shareholders' interest being predominantly financial, the most obvious harm caused to a shareholder is through financial loss on the value of the shareholding. An example of this is being played out in the 2018 class action represented by BarentsKrans against Steinhoff where investors who held shares in Steinhoff during the 2017 fall in the share price suffered severe losses after the announcement relating to the discovered accounting irregularities (BarentsKrans, 2018).

Harm is not caused to shareholders when large amounts of money are spent on system security, because despite the short term decrease in profit, the long-term security benefits creates a more reliable and secure digital offering to the customer. The security comfort given to customers will make them more likely to trust the digital platform and to demonstrate this trust by using the platform for transactions. As discussed in the previous section, customers are the most valued stakeholder as they are the main source of revenue generation for the FI, and ultimately the stockholders as owners of the business. Although the money spent on digital security enhancements does not yield a financial return, the benefit is experienced through decreased risk of system outages and intrusion, as well as customers' perception of a secure digital platform.

Although unusual amongst FIs, if the decision whether to compensate a hacker is publicised, it may create panic in the market. The uncertainty and perceived risk to shareholders could negatively affect the share price resulting in a devaluation of the company. Even prior or separate to the decision whether to compensate a hacker, a publicised data breach event could also affect the value of the share price. It is therefore essential that shareholders' interests be managed for sustainable growth in the valuation of the company.

4.1.4 Other FIs (Competitors)

Consumer, economic, and political confidence, are necessary for the effective functioning and stability of the financial industry. The effect of this is evident in country and financial institutions' ratings by international rating agencies, and the impact these ratings have on the country's economy.

While competition is limited and there are high barriers to entry, the financial industry is not monopolistic. Policy and regulatory decisions are equally relevant to all FIs, and poor decisions

taken by one FI could negatively affect the credibility of the financial sector, thereby affecting all other FIs.

FIs are subject to a similar moral code, although the prioritisation of their values differs slightly. Moral obligations applicable to one FI, will be applicable to all FIs. This is because all FIs customer bases are made of natural or juristic persons, or both, with similar moral expectations from the FI resulting in similar moral duties to the customers.

South African FIs have similar business and social objectives which include contributing towards inclusive growth, socio-economic development, and strengthen financial stability. They are subject to the same regulator and should be held accountable in the same way. In contrast, security vulnerabilities discovered in one FI is unlikely to be applicable to another due to the different systems and firewalls used. Despite that system vulnerabilities are not shared amongst FIs, a breach in the security of one FI affects the integrity of the whole financial market. Although not publicised, data security and privacy are important features of a FI's brand. Without it, many customers would not transact with the FI and the business would not be successful. Apple has realised how costly this can be, as "[c]ompromising its customers' data security, or even being seen as not defending it vigorously, could diminish the value of that brand, estimated at $229b." (Newkirk 2018, 15). What it means to defend customers' data security vigorously is not clear, but at a minimum it would mean compliance with laws and putting the necessary technological safeguards in place to prevent a security breach. At most, FIs would engage in advocacy measures to ensure that the industry is held to a high data security standard.

The actions taken to address concerns of data security could improve FIs' reputation and raise trust through transparency and accountability exercised by the FI. An admirable and positive action taken by one FI may become an industry benchmark, and therefore expected to be executed by all other FIs as a new standard. Implementation of digital security improvements

are costly and detract from the time spent on core business activities. To manage this, FIs participate in organised industry fora discussions, albeit in a manner that does not disrupt competition. Discussions include cyber risks facing the industry, vendor exhibitions, industry challenges, and sustaining the integrity of the financial industry. If the moral duties to provide a secure financial service and not to cause harm to stakeholders are generally accepted, so too should the consequence of a penalty from a failure to comply with these obligations.

If one FI decides to compensate a hacker, although not publicised, through C-suite networks, it is possible that other FIs will find out and be put in a position to reconsider their policies. However, the compensation of hackers is not a point that FIs would want to compete on, specifically due to the unwanted attention it may create. It is therefore in the FI's interest to use industry fora to discuss policy and ethics around compensation as well as what the best response would be to maintain the stability of the financial market. This is a discussion that can be led by the South African Reserve Bank and the Financial Sector Conduct Authority.

Other FIs are, therefore, important stakeholders due to the competitive nature of the relationship between FIs, the ripple effect of industry events like cyberattacks, and decisions taken by FI's that can impact the perception of industry security.

4.2 Kantian Theory

Kantian ethics is a deontological theory, which means that the focus of the theory is on the rightness of the action, and not on the consequence as is the focus of consequentialism. What follows is a rendition of Kant's political state and categorical imperative.

4.2.1 Political State

Liberalism has its roots in Kant's philosophy of the political state and the promotion of autonomy. To achieve Kant's vision of a political state, autonomy meant that "each person has the freedom, the capacity, and the responsibility to form his or her own conception of happiness and to seek that happiness, each in his or her own way, so long as this is done in a lawful fashion" (Sullivan 1994, 8).

Kant believed that the role of the state was to protect and promote the freedom and autonomy of the person. "The rationality and autonomy in question here are capacities and dispositions that virtually all sane adult human beings are presumed to have, not the full manifestation of these in actual conduct" (Hill 1992, 202). Protection is a negative obligation on the state because it requires the state to create a legal order that limits the infringement and interference of one person with another person's freedom. This limitation is required to promote a liberal state. In a natural or original state where everyone pursues individual interests without political authority and legal structures, he believed that civil war was inevitable. Civil war was likely, because people are naturally inclined to promote their personal interests, and in doing so to act selfishly, taking what does not belong to them to ensure survival. This will inevitably lead to a break down in communal trust and cause harm. A focus on promoting self-interest is often accompanied by a need to protect ones' own. Jealousy and inequality can result in theft, and proactive measures towards protection could result in violence. To prevent this a state or political authority should be elected which creates rules to maintain legal order, similar to the role of the South African Reserve Bank and the Financial Sector Conduct Authority. "The legal system of the state must constrain both the power of the sovereign and the citizens' unregenerate desires in order to establish the conditions under which people can live together in peace as a community" (Sullivan 1994, 10). In this desired liberal state, a "free person is a self-governing person, capable of acknowledging the imperative nature of moral principles in the face of opposing inclinations" (Dubbink and van Liedekerke 2009, 125).

In South Africa, the state's negative obligations are derived from the law, specifically the Bill of Rights. Through legislation, the state exercises its authority to promote autonomy and prohibit the interference of citizens to infringe on other citizens' autonomy.

The FI's role is to comply with the legal framework that the state put in place. These laws must be tested against the Constitution which puts processes in place for laws to be reviewed and disputed. Compliance to laws are required unless these laws are found to be invalid or unconstitutional. Laws are intended to make moral conduct obligatory. This is not unfamiliar for FIs, as the financial sector has legislation and codes imposed on it to ensure an appropriate and effective culture of business and market conduct. The introduction of the Conduct of Financial Institutions Bill and regular banking conduct reviews performed by The Group of Thirty further solidifies this approach. These laws are required because without them, FIs did not voluntarily conduct themselves by what is recently publicised as best-practice. The finance industry follows a culture of compliance-based decision-making, and while this approach is important, ethical conduct further requires morality-based actions and decision-making. For Kantian ethics, the latter determines the rightness of the action.

If an FI promotes the values of the company and believes that their actions should be moral despite legislative guidance, and it is managed in a way that promotes ethical business practices, then it can be deemed to conduct itself freely and autonomously.

"Principled autonomy requires that we must be able to communicate the reasons for our actions to others, effectively ruling out arbitrary and irrational actions as well as actions that could harm others" (Myskja 2008, 214). Therefore, as an autonomous agent, the FI should be able to communicate the reason for making a decision not to compensate a hacker. Because the decision will be applied consistently, the reasons should be well understood so that they can be clearly explained to hackers, stakeholders, and the public. The rationale for the decision will include that hackers have caused harm to customers and the FI and must not be

rewarded for that, as well as the harm that the awareness of the decision to compensate will cause to shareholders and other FIs. Principled autonomy does not require that these reasons *must* be communicated. It means that because the decision is principled, if it is communicated it can be done with confidence that it is right. The decision will be right if it was justified by principle-led reason and duty. It may not be in the interests of the stakeholders to have this decision communicated as the transparency of the decision may cause further harm.

Thomas Hill opines that "[t]he coercive power of state must provide incentives so that even without conscience everyone will have clear and sufficient reason not to violate the liberty of others". He states further that "the system can serve to 'hinder hindrances to freedom" by credible threats that provide rational incentives, apart from conscience, for each to stay within the bounds of the freedom he or she has been fairly allotted. The threats must be genuine, enforceable, and public in order to be credible, and they must be carried out as legally prescribed for the sake of both fairness and efficacy" (Hill 1992, 209). However, if all people are rational beings, their rationality should guide their behaviour to attain state coercion and not necessarily incentives. While this would be ideal, it is not realistic. Promoting a culture of doing the right thing will inform the sustainability of moral decision-making, while state coercion will be better positioned as a second line of defence if the promotion of a moral decision-making fails.

The cost of implementing legislation and executing on the values of an institution is one of the main reasons for non-compliance. For example, project teams are constituted to manage people, technology, and processes affected by the implementation of legislation, and it is usually also more cost effective to make a decision that will increase revenue rather than to make a decision in line with the values of an FI, resulting in the decision to decline a business opportunity because it is not ethical. These costs however are superseded by the duty to respect customers' privacy which is essential for the effective functioning of an FI. A data security breach can disrupt the market and lead to a breach in trust.

4.2.2 The Categorical Imperative

The categorical imperative sets out the ultimate moral norms which guide and motivate individuals' actions, decisions and behaviour. It is different from the consequentialist theory in that the action is what matters, and not the consequence of the action. The consequences of the action taken are irrelevant as long as the action is based on universal moral norms. The categorical imperative is "unconditionally binding on all human beings, whatever their circumstances and regardless of what ends must be sacrificed to satisfy it" (Hill 1992, 201). If applied correctly, it is not possible that a conflict between ultimate moral norms can exist. For example, dignity will not conflict with freedom.

A discussion of the formula of universal law and the formula of humanity will follow.

The Formula of Universal Law

The formula of universal law puts forward that laws, which in this context are moral duties, should apply unconditionally to all by virtue of their status as rational beings. "[A]ct only in accordance with that maxim through which you can at the same time will that it become a universal law" (Johnson and Cureton 2016, §5). These duties apply across jurisdictions, socio-economic conditions, and beliefs.

For laws to be universally accepted, they should be expressed in terms that everyone can understand. In other words, the moral duty imposed by the law should be easily recognised, understood, and accepted as binding. The duty is shared, and through accepting it, one agrees to be held accountable to it (similar to the undertaking by FIs to be held to a higher standard). The role of regulators like the Financial Sector Conduct Authority is to create awareness, provide clarity on legislative provisions and impose penalties where FIs fall short of what is required.

Respect is one such duty, as it forms part of dignity. “[R]espect for persons can’t be one that claims to be universal but actually expresses the interests or homogeneous ideologies of only certain classes of persons or persons only in certain contexts. The global nature of IT presents both the opportunity and the pressing need to develop ethical conceptions that arise from and express the full range of human voices, perspectives, cultures and traditions without becoming a mere conglomeration of relativistic conceptions. So, a parameter for developing rich conceptions of respect for persons in IT contexts is that these conceptions be suitable for a global ICT ethics” (Dillon 2010, 27). Even a hacker, will acknowledge the need for respect for persons (even though they do not respect persons as part of their hacking activities), because they too are people with personal lives in which they demand respect. This demanded respect includes instances when hackers are customers. Respect for persons, including online, is a universal principle. This respect may be represented in different ways, but it is universally accepted that it is required, despite many companies not consistently fulfilling their duty of respect to their customers.

The Formula for Humanity

Section 1 of the Constitution states:

> The Republic of South Africa is one, sovereign, democratic state founded on the following values:
>
> (a) Human dignity, the achievement of equality and the advancement of human rights and freedoms.

The principle of humanity is demonstrated through the dignity possessed by each person. The human dignity is derived from reason and autonomy by virtue of being human and requires that every human being should be treated as an end in itself, and never as a means to an end. “To treat someone as an end in him or herself requires in the first place that one not use him or her as a mere means, that one respects each as a rational person with his or her own

maxims" (O'Neill 2005, 641). Therefore, the value attributed to every human being is independently derived and therefore not associated with specific people. It is objective and intrinsic to being human. Respect and therefore dignity, are both rights to be demanded by all, and duties to be accepted by all.

Respect for the person, in this case the customer, is central to the argument that the hackers' activities are harmful. When hacking, value is attributed to finding one's way into the system or getting access to data that are intended to be secure. Yet, these activities do not consider the person and his right to be respected as a person and not just to be viewed as data. If the hacker disregards the person as worthy (by only attributing value to the data) despite the person having intrinsic worth, the hacker's lack of respect is wrong (Dillon 2010, 20). What is specifically wrong with the activities of the hacker is that they are "depersonalizing and dehumanizing, in the sense of being degrading of persons: they are the reduction of persons to things to be manipulated in non-person-acknowledging ways" (Dillon 2010, 26). This wrongful act is immoral and must not be rewarded.

Privacy is linked to respect and dignity of persons, and therefore is required for a person to be autonomous. This is so because "[p]rivacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1967, 7). Hackers have a duty to respect the privacy of customers and of the the FI being hacked.

Similarly, in the law of delict, "the general principles in respect of *animus iniuriandi*…is a subjective concept that involves the direction of the defendant's will towards infringing the plaintiff's privacy, and the defendant's knowledge that such infringement is wrong in the circumstances" (Loubser *et al* 2010, 320).

In *Aphane v S (A621/2007) [2009] ZAGPPHC 264 (10 September 2009)*, the North and South Gauteng High Court of Pretoria stated:

> [9] Crimen injuria may be defined as the unlawful, intentional and serious violation of the dignity or privacy of another - Criminal Law Snyman 4ed 453. What is protected by the crime is the dignitas, all the rights of personality other than reputation and bodily integrity - R v Umfaan 1908 TS 62 at 66-67. To determine whether a person's dignity has been violated a subjective and an objective test are applied. The subjective test requires that the victim must be aware of the offending behaviour and feel degraded or humiliated by it. R v van Tonder 1932 TPD 90 at 94; S v A 1964 (3) SA 319 (T) at 321 B; S vA 1993 (1) SA CR 600 (A) at 610e-f. The objective test requires that the accused's conduct must be of such a nature that it would offend the feelings of a reasonable person.

Companies have a duty to act honestly and with integrity (Hasnas1998, 26-27). Most South African FIs have a Code of Ethics which guides their business activity and decision-making. Upon review of the top South African FIs' values, integrity is consistently included across FIs. The use of integrity is also common in legislation where it refers to the integrity of personal information, and the integrity of systems.

Respect should be granted equally to all, irrespective of social status, the amount of wealth, and whether a customer is regarded as profitable. "The moral demand to respect persons is universal in its application to persons both as objects who must be respected and as subjects who must respect" (Dillon 2010, 23). It is a right that cannot be disregarded. All people should be respected and treated in a dignified manner. Therefore, the FIs duty to protect its customers applies to all customers equally. Enhanced security measures should not be taken to protect wealthy clients' money, and not the saving of the low-income client base. All individuals have

equal dignity, deserve respect, and are rational beings. Therefore, customers should be treated fairly. Relief should not only be given to customers who complain. If the complainant raises a legitimate breach of a FI's duty, relief should be provided to all customers affected by the breach and not only those who had noticed and raised the issue.

As a universal principle, the hacker must agree to be bound to the principle of humanity which includes dignity and respect. This does not mean that he will always conduct himself in a manner in compliance with the principles. Acceptance of the principle of humanity means he is bound to it despite failing to meet its requirements. Thus, the hacker should accept the consequence of his deviation from the moral principle "insofar as he or she is willing to look at the matter from the perspective of one rational agent, with dignity, among many" (Hill 1992, 210).

In the same way that customers should be respected, a hacker should also not be used as a means to an end and his dignity should be maintained. If the FI accepts the findings of the hacker and uses it to enhance their security systems, without due reward or consideration to the hacker, the hacker would be used as a means to achieve a specific end being a more robust security framework. Although, this is what Kant intended with this principle, I argue that the hacker is not being used as a means. The hacker voluntarily decided to hack without the FI's awareness, request or approval. "To use someone as a mere means is to involve them in a scheme of action to which they could not in principle consent" (O'Neill 2005, 640). The FI is therefore being used as a means to an end, not the hacker. If the FI requests the hacker to test its systems, as in the case of contracted penetration testers, consent would not be an issue. It is not only the FI that is used as a means, but also the customers whose private information makes hacking the FI's system more appealing, because the hacker knows that the FI has a responsibility to protect the data.

In addition to the rightness of the action, Kantian theory assesses the intention of the actor. Hackers' intentions may differ, but the one common thread is that they breach and take advantage of security vulnerabilities, without the owner's consent. The intention in itself is wrong and unjust, despite the consequences.

Kant's view on gratitude sheds a different light on the topic of respect for persons and presents an argument for the compensation of hackers. In *The Metaphysics of Morals*, Kant defines gratitude as "honouring a person because of a benefit he has rendered to us". What follows is a review of gratitude and reciprocity between the FI and the hacker, which I do not believe necessitates compensation.

For the purpose of this section, I think it is useful to reiterate the exchange of events between the FI and the hacker. The hacker, through research, finds an opportunity to obtain entry into what is supposed to be a secure system. The hacker's ability to access this controlled environment is due to a security defect or vulnerability that the hacker discovers. The hacker enters and exits the environment. The hacker sometimes patches the security vulnerability, providing a potentially helpful security solution to the vulnerability. The hacker makes contact with the FI and informs the FI of his activities in the system. In other words, the hacker informs the FI that he found a security vulnerability that the FI was likely not aware of. The hacker might also inform the FI that he either has a solution to the problem or already implemented the solution.

The perceived benefits to the FI are therefore the awareness created about the security vulnerability and possibly the solution provided. It is general courtesy that when one person does something beneficial to the other, irrespective of whether the action was not expected, that the latter expresses gratitude.

Von Tevenar highlights three features of Kant's view on gratitude (von Tevenar 2006, 182).

i. The recipient of a benefit is placed under an obligation

The obligation the recipient is under is to experience gratitude. The experience of gratitude includes the acknowledgement of the benefit and the appreciation of the benefit.

The first necessary step is for the FI to recognise the discovery of the security vulnerability as a benefit. It will be difficult to dispute the benefit because improved awareness of security vulnerabilities allows the FI to have a better understanding of their risks and to implement controls and remediation actions to mitigate the risks. The benefit is not only to the FI, as it extends to the customers of the FI who are provided with a more secure platform for the safeguarding of their assets, personal information, and transaction data.

I am not sure whether Kant intended for the obligation of gratitude to extend to all beneficiaries of the benefit. This is an important consideration especially with regard to determining who holds the duty to reciprocate.

ii. Once a benefit is received, an unequal relation exists between the giver and receiver.

If point (i) holds, the giver of the benefit is then placed in a superior position because he has a reciprocal duty due to him. As the initial beneficiary, the FI has to fulfil this duty to the hacker. From the onset, the FI is in a submissive position – the FI has no choice in being hacked. The duty placed on the FI to reciprocate further instils its submissive position.

iii. There is a reciprocal duty on the recipient

In law, for every right there is a corresponding duty. I argue that the hacker did not have the right to provide the FI with the benefit, or to investigate whether a security vulnerability existed. If the right does not exist, then surely there can be no corresponding duty. If the duty to reciprocate is not dependent on the right and is solely concerned with whether a benefit was received, then followers of Kant would probably argue that the FI would be required to provide an equal benefit to the hacker. It will be difficult to determine the value

of the benefit received, although the reciprocal benefit does not have to be compensation. I will discuss this further in section 6.

While benefits can be well-intended, the opposite is also possible, for example, “making or keeping recipients dependent on ones favo[u]rs; manipulating them via gifts into corners and concessions” (von Tevenar 2006, 184). This motive takes advantage of the recipient’s vulnerable position and does not have the purpose of putting the recipient in a better position. The intention is therefore wrong. The recipient, the FI, did not voluntarily accept the benefit, and had it known that it would be receiving the benefit and was under a duty to reciprocate, the FI would likely have chosen not to receive the benefit.

4.3 Corporate Social Responsibility (CSR)

In this context, it seems appropriate to consider the view that information privacy is an ethical responsibility that should be taken more seriously by FIs, in spite of the regulators current inability to enforce legislation that seeks to protect data privacy, as well as the reasons and manner in which it is processed, stored and destroyed. This ethical responsibility promotes the objective of autonomy. Individuals are autonomous when they can decide how and when their information is shared, because as the information owner this is their moral right (Pollach 2011, 88-90). This right to information privacy should be respected by FIs, who in turn have a moral duty to conduct themselves in a manner that effects and promotes that right.

According to Aguilera, one of the reasons companies accept their social responsibilities is due to their “relational motives”, which is demonstrated through a company’s desire to weigh and promote the interests of its stakeholders, to achieve “social legitimacy”, trust, and stakeholder wealth (Pollach 2011, 3). “Relational motives include the recognition that customers have a desire for privacy, which the company seeks to meet, and the expectation that privacy protection will help the company win customers’ trust” (Pollach 2011, 93).

A distinction should be drawn between social responsibilities imposed on corporates through legislation, and corporates exercising their social duty because they believe it is the right thing to do, and therefore do not have to be regulated to do so. Social responsibilities are moral responsibilities and while they are not legislated, are still expected by society. For example, society may expect a company to provide employment to the local community or may prohibit a company from operating beyond certain hours or on religious days. In fulfilling these social responsibilities, companies show their respect to their stakeholders, and operate in manner that is just. Dubbink argues that companies can be regarded as moral actors, and that “CSR has accepted moral duty as an independent ground of action in a given case” (Dubbink 2009, 134). For example, many FIs were challenged by environmentalists for their role in financing coal plants and had to consider the financing of the Thabametsi and Khanyisa plants in line with their “commitment to balance Africa’s economic development and energy needs with climate change mitigation and adaptation" (Steyn, Lisa 2018, Business Day).

Most of the top FIs in South Africa all have publicised codes of ethics or conduct, as well as internal policies which guide their behaviour and the way they consider the impact of their products and services. The documents are not all legally imposed which lead me to believe that FIs acknowledge their moral social duties to protect and promote autonomy, and to avoid harm. If this is true, FIs should be held accountable in the event of policy breaches, albeit policies that are internal to the organisation. FIs should therefore be held accountable to the self-imposed higher standard, despite it not being legally imposed.

There is a duty on the FI to not cause harm to its stakeholders. This is a moral duty which exists independently from legislation being in place and should therefore be the basis of FIs implementing security controls. Beyond the controls, it should also inform data processing methods, data integrity, management decisions, and stakeholder communication.

5. Legislation

As a highly regulated industry, FIs have been subject to legislation impacting information privacy. These include the Protection of Personal Information Act (POPIA), the Cybercrime and Cybersecurity Bill, General Data Protection Regulation (GDPR), and the Constitution.

In common law, privacy is not a separate right, but rather included in the right to dignity. Apart from the common law, the right to privacy was introduced into South African law as section 13 of the 1993 Interim Constitution. It later became section 14 of the final 1996 Constitution, which states:

> Everyone has the right to privacy, which includes the right not to have—
>
> (a) their person or home searched;
>
> (b) their property searched;
>
> (c) their possessions seized; or
>
> (d) the privacy of their communications infringed.

The right to privacy is not absolute, and therefore may be limited with adherence to section 36 of the Constitution. The Constitution is the supreme law and all “law or conduct inconsistent with it is invalid” (The Constitution of the Republic of South Africa 1996, 3).

Between 2017 and 2018, many documents under the title “Gupta Leaks” were released across South African media platforms. The leaks included a series of emails and communications highlighting the extent of state capture as well as who was involved. This leaked information resulted in a breach of privacy on the part of the individuals whose correspondence was leaked but even more so for the company that owns the information. The confidentiality of the emails should be protected and restricted to conducting the company’s service. However, the “Gupta Leaks” is be an exceptional case where the company’s right to confidentiality should be

weighed against the need to expose corruption. Whoever leaked the emails will not be considered a hacker by definition, however the intention and outcome were arguably similar. This brings into question the balance between the right to privacy and what is in the best interest of justice, and national security. Had the company, whose server the emails were kept on, been asked to share the information voluntarily, they would have likely declined. They would rightly have taken themselves to be obligated to protect the privacy of their staff and their stakeholders especially if the request for information did not stem from a credible investigation. The right to privacy is not absolute, and neither is the right of access to information, which is only allowed under specific conditions.

In Mistry v Interim National Medical and Dental Council of South African 1998 (4) SA 1127 the factors considered by the Constitutional Court in the context of information privacy were "whether the information was obtained in an intrusive manner; whether it was about intimate aspects of the applicant's personal life; whether it involved data provided by the applicant for one purpose which was then used for another; whether it was disseminated to the press or the general public or persons from whom the applicant could reasonably expect such private information would be withheld" (Currie and de Waal 2005, 324). The above factors do not consider the extent of harm caused to the data subject. The consequences of the privacy breach are not included in the factors mentioned. The factors mainly relate to actions, that is the action of obtaining the information in an intrusive manner, the action of using the data for a purpose it was not intended for by the data subject, the action of accessing data that the hacker would not have ordinarily had access to. The factors are more closely positioned to a deontological theory than a consequentialist theory.

The Protection of Personal Information Act (POPIA) was assented in 2013 but is not yet fully effective and the commencement date is yet to be declared. Given that the legislation has been promulgated, I will proceed on the assumption that it is effective. The purpose of the Act includes the provision of rights and remedies to data subjects which allows them to protect

their personal information in line with the Act. The Act is applicable to public and private bodies who “determines the purpose of and means for processing personal information” (Protecton of Personal Information Act 2013, 17). A FI is an example of such a body, which makes use of personal information to commence, enhance, and terminate business relationships with their clients, also referred to as “data subjects” in the Act. Section 19 (1) of POPIA, places the following responsibilities on FIs, as responsible party:

> (1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—
> (a) loss of, damage to or unauthorised destruction of personal information; and
> (b) unlawful access to or processing of personal information.

While the Act is not fully effective yet, it may be enforced within one year of the published commencement date. For this reason, many FIs have employed resources and commenced readiness assessments to determine the risks they currently face, as well as the actions and controls required to mitigate this risk. The implementation of the Act does not only affect legal and compliance functions within a FI, but also Information Security, Information Technology, and Operational Risk.

The General Data Protection Regulation (GDPR) relates to the protection of data in the European Union (EU), specifically affecting business activities conducted in Europe or business activities in other jurisdictions which involve European citizens. GDPR is relevant, because it places additional legislative obligations on FIs, although the impact will be limited in comparison to POPIA.

The Electronic Communications and Transactions Act became law on 20 August 2002 and is the first legislation seeking to criminalise cybercrimes in South Africa. Section 86 (1) states “a

person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence". I interpret this to mean that grey hat hacking is an offence, because by definition the hacker obtains access without authority.

The Cybercrimes and Cybersecurity Bill is still tabled in Parliament and has received extensive commentary. It is understood that once the Bill is enacted, the sections related to cybercrime and cybersecurity in the Electronic Communications and Transactions Act will be repealed.

Legislation are put in place to define the rights that require protection as well as to prescribe conduct to achieve this protection. It can thus be regarded as a step in creating the desired culture where irrespective of laws, people will live in accordance with universal moral principles without having to apply a compliance approach. It is only a step because law does not always reflect morality and "respect and disrespect can be expressed or represented or instantiated by or through things that are not agents, such as guidelines, rules, or principles" (Dillon 2010, 20).

Regulators

FIs are strictly regulated. The regulators include the South African Reserve Bank and the Financial Sector Conduct Authority (FSCA). Satisfying the regulators and avoiding non-compliance is important, because one of the most immediate consequences of a security and information privacy breach could be the penalty from a regulator (Acquisti *et al).*
The implementation of regulation is costly. Both the implementation and penalty negatively affect profits. Proactive engagement and management of the regulators are crucial for the sustainability of the business, as well as the for the financial stability of the market.

To inform and guide best practice and effective corporate governance, the King IV Report on Corporate Governance (King IV) has a section dedicated to IT governance, and all South

African listed companies are required to adhere to the code as outline in the JSE Listings Requirements. Listed FIs therefore either have information technology sub-committees to the board, or have IT and, or IT risk as a standing item on the board agenda. King IV specifically requires that attention be given to information and technology, respectively.

6. The Issue of Compensation

As previously stated, I believe that FIs should not compensate hackers. The request for compensation is rooted in self-interest, the quest for recognition, and the belief that they have traded their intellectual capital.

Compensation is generally provided in response to a service rendered or good received and can be due despite the recipient's dissatisfaction with the goods or services. In the case of a willing buyer and willing seller, the recipient of the goods or service would have consented to the service or would at least be reasonably expected to consent. If consent is absent, the recipient will either return the good or reject the service and compensation will not be due. This is demonstrated in negative option marketing strategies declared invalid to ensure consumer protection. FIs have not consented to the receiving the hacker's service. It is therefore reasonable for the FI to decide not to compensate the hacker. If the hacker argues that the FI has been unduly enriched, the FI's defence should be that it believed that the necessary security measures were in place to avoid receiving such a service, and therefore the enrichment was unwanted. In addition, the hacker proceeded intently knowing that consent was absent.

There are companies that have reluctantly made ransom payments to black hat hackers to restore access to their systems. There are many other companies and countries that equate negotiating with hackers to negotiating with terrorists and therefore refuse to do so. Being a

victim of ransomware is a high-risk scenario, and companies can experience serious financial losses because of a ransomware attack. If companies are inclined to believe that compensating black hat hackers is immoral, they should not be willing to compensate un-appointed hackers. Surely the request for compensation unaccompanied by a threat should not be the critical factor in the decision whether to compensate a hacker.

Some might argue that making a definitive decision not to compensate hackers underestimates the influence and threat of the hacking industry. I disagree. FIs undoubtedly understand the seriousness of a security breach and endeavour to put in place the necessary controls to provide system security. Skilled IT and cybersecurity professionals understand hackers' motives as well as the seriousness of their threats from a technical perspective. What often lacks is for board members to possess these skills. Listed companies are required by King IV to consider technological risks, but the skills required to do so are scarce. The skills possessed by hackers are not restricted to the hacking community, so while hackers will remain a threat, the security measures implemented to mitigate security threats, will be also improve.

Facebook, unlike many other companies, did have a policy on the compensation of hackers, and in line with that policy had decided not to compensate Khalid. Hackers around the world were not satisfied with Facebook's decision not to compensate Khalid and mobilised themselves to raise donations for Khalid. Despite Khalid not meeting the requirements for Facebook's bug bounty programme, other hackers still believed that he deserved to be compensated. Besides not fulfilling the requirements of the Facebook programme, more importantly, Khalid breached a data subject's privacy. If Facebook applies the policy against privacy breaches strictly towards all users, this is a move in the right direction especially in the cyber world where privacy breaches are common. Facebook decided to prioritise the right to privacy and the protection of it publicly. Hackers now know that while Facebook invites hackers to find bugs, this should not be done at the consequence of a privacy infringement.

If the decision taken by the FI is not to compensate hackers, and the Kantian theory is applied, the decision should apply absolutely and cannot be assessed on a case by case basis. In other words, if the FI decides that hacking without consent is wrong, they cannot provide compensation in cases where they admire the hacker's intentions or believe that he presented the facts in a respectable and friendly manner. If in certain cases they suspend their decision not to compensate, this allows for gaps which creates inconsistency and a misinterpretation of the legitimacy of their approach and decision. In reality, corporates do not choose an ethical theory on which they base all policy decisions on. Instead they may combine elements of different theories which best articulate the values of the FI, and the spirit in which their policies should be drafted. Therefore, while the policy taken should be applied rigidly, this does not mean it cannot be reviewed and amended to meet societal and technological changes. What is important to consider is how proposed changes consider the interests of stakeholders, while prioritising the respect due to its customers and make decisions based on the FI's ethical duties. In taking stakeholders interests into account, it must also be highlighted that changes can only be made to the way moral duties are actioned. In other words, changes can only be made to the action taken and not to the existence of the moral duty.

Wolf and Fresco believe that that there is "no ethical case for the buying and selling of zero-day exploits" (Wolf and Fresco 2016, 276). Instead, they argue, that the state should incentivise organisations to incorporate internal controls to proactively detect vulnerabilities instead of relying on a third party (Wolf and Fresco 2016, 278). This is aligned to Thomas Hill's argument, previously discussed, on the coercive power of the state in providing incentives. In South Africa, the legislature has taken a slightly different approach. Instead of incentivising businesses, they impose penalties for not incorporating internal controls and not acting responsibly to proactively address cybersecurity.

As it has been shown, there is a market for penetration testers who are contracted to find vulnerabilities. This is a reasonable and legal alternative to compensating a hacker. Even without considering a FI's moral duties to its stakeholders, the use of penetration testers should prevail. Where FIs are already using penetration testers and are still approached by hackers, they should still reject the request for compensation based on the hacker's breach of respect as well as the FI's duty to its stakeholders.

Once a security breach is exposed and the regulators are functioning effectively, the most likely outcomes of reporting the breach are a fine from a regulator and depending on the severity of the breach, legal action can be taken against the FI for failing to adequately secure its systems, and for not meeting their fiduciary duties. This is in addition to the reputational damage, the costs to implement the appropriate security measures and retrieve the data, and the increased insurance premiums against security breaches. It is not reasonable for an FI to compensate a hacker given the reputation and possible financial damage that the hacker has caused. However, as previously discussed, these consequences are irrelevant when following a principle-based approach. Hacking is wrong, and by virtue of that, compensating the hacker is wrong.

Instead of compensating the hacker, efforts should rather be directed towards increased readiness to meet the minimum standards imposed by legislation, and thereafter to work toward achieving potentially higher internal standards to complete the fulfilment of value and mission statements declared by these institutions. Furthermore, hackers have the option to obtain compensation through other means, for example becoming accredited penetration testers and contracting their services to FIs.

Compensation is not the only form of recognition that can be given to the hacker. In the digital domain, recognitions are given with kudos and the more kudos hackers receive, the more

recognised and respected they are amongst their peers. Giving hackers kudos validates their skills and not the morality of their actions.

7. Conclusion

In doing business the right way, FIs should act in fulfilment of their moral duties to its stakeholders. These duties include to respect its customers and provide secure systems. The hackers' activities violate the respect due to customers and causes harm to all stakeholders. Compensating hackers is neither an action in expression of a moral duty nor within stakeholders' interests. Further to that, it does not promote the spirit of the law and does little to maintain integrity in the financial market.

8. Bibliography

Acquisti, Alessandro; Friedman, Allan; and Telang, Rahul. 2006. “Is There a Cost to Privacy Breaches? An Event”. *ICIS 2006 Proceedings* 94: 1563-1580.

Aphane v S (A621/2007) [2009] ZAGPPHC 264 (10 September 2009). Accessed October 21, 2018. www.saflii.org/za/cases/ZAGPPHC/2009/264.html.

BarentsKrans. “South African Institutions back Steinhoff class action run by BarentsKrans”. Accessed on December 28, 2018. https://www.barentskrans.nl/en/news/south-african-institutions-back-steinhoff-class-action-barentskrans/

Boatright, John R. 2006. “What’s Wrong – and What’s Right – with Stakeholder Management”. *Journal of Private Enterprise* XXI: 106-130.

Bose, Utpal. 2012. “An Ethical Framework in Information Systems Decision Making using Normative Theories of Business Ethics”. *Ethics and Information Technology Journal* 14:17-26.

Cloudflare. “What is Penetration Testing?”. Accessed on October 21, 2018. https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/.

Companies Act 71 of 2008. Accessed October 21, 2018. www.justice.gov.za/legislation/acts/2008-071amended.pdf

Currie, Iain., and Johan de Waal. 2005. *The Bill of Rights Handbook*. Juta and Company Ltd.

Cybercrimes and Cybersecurity Bill. Accessed July 02, 2018. http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf

Delmas, Candice. 2018. “Is Hacktivism the New Civil Disobedience?”. *Journal Raisons Politiques* 69: 63-81.

Dillon, Robin S. 2010. “Respect for persons, identity, and information technology”. *Ethics and Information Technology* 12:17-28.

Driver, Julia. 2005. “Normative Ethics”. In *Oxford Handbook of Contemporary Philosophy*, edited by Jackson and Smith, 31-57. Oxford: Oxford University Press.

Dubbink, Wim; and van Liedekerke, Luc. 2009. “A Neo-Kantian foundation of Corporate Social Responsibility”. *Ethic Theory Moral Practice* 12: 117-136.

Facebook Security. “Recent reports on our whitehat program”. Accessed December 26, 2018. http://m.facebook.com/notes/facebook-security/recent-reports-on-our-whitehat-program/10151538365500766/

Fisher, James; Harschman, Ellen; Gillespie, William; Ordower, Henry; Ware, Leland; and Yeager, Frederick. 2001. “Privatising Regulation: Whistleblowing and Bounty Hunting in the Financial Services Industry”. *Dickinson Journal of International Law* 19: 117-143.

Friedman, Milton. 1970. “The Social Responsibility of Business Is to Increase Its Profits”. In Beauchamp and Bowie (eds.), *Ethical Theory and Business* (Prentice Hall, 2001), 51.

Gardner, Joshua. 2013. “Computer Expert Hacks in Mark Zuckerberg’s Facebook Page to Expose the Site’s Vulnerability After His Security Warnings were Dismissed”. Accessed on October 21, 2018. https://www.dailymail.co.uk/news/article-2396628/Mark-Zuckerbergs-Facebook-page-hacked-Khalil-Shreateh-expose-site-vulnerability.html.

General Electric. “Product Vulnerability”. Accessed on October 21, 2018. https://www.ge.com/security.

Group of Thirty. 2018. “Banking Conduct and Culture: A Permanent Mindset Change”. Accessed on February 15, 2019. https://www.oliverwyman.com/our-expertise/insights/2018/dec/banking-conduct-and-culture-the-g30-report.html.

Hartley, Regina D. 2015. “Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack” . *Journal of International Technology and Information Management* 24: 95-104.

Hasnas, John. 1998. “The Normative Theories of Business Ethics: A Guide for the Perplexed.” *Business Ethics Quarterly* 8: 19-42.

Hill, Thomas E. 1992. “Making Exceptions without Abandoning the Principle: or How a Kantian Might Think about Terrorism.” In *Dignity and Practical Reason in Kant’s Moral Theory*, 196-225. Ithaca: Cornell University Press.

Hovav, Anat; Gray, Paul. 2014. “Communications of the Association for Information Systems”. *Communications of the Association for Information Systems* 34: 894-913.

Johnson, Robert; and Cureton, Adam. 2016. “Kant’s Moral Philosophy”. In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta. Accessed 29 June 2019. https://plato.stanford.edu/archives/spr2019/entries/kant-moral/ .

Jones, Thomas M.; Felps, Will; and Bigley, Gregory A. 2007. “Ethical Theory and Stakeholder-Related Decisions: The Role of Stakeholder Culture”. *Academy of Management Review* 32:1 137-155.

Kant, Immanuel. 1996 [1976]. *The Metaphysics of Morals*. Translated by Mary Gregor. Cambridge University Press: Cambridge.

Lea, David. 2004. “The Imperfect Nature of Corporate Responsibilities to Stakeholders”. *Business Ethics Quarterly* 14: 201-217.

Loubser, Max; Midgley, JR; Mukheibir, André; Niesing, Liezel; and Perumal, Devina. 2010. *The Law of Delict in South Africa*. Oxford University Press: Southern Africa.

Institute of Directors Southern Africa. “King IV Report on Corporate Governance for South Africa 2016”. Accessed on February 15, 2019. https://c.ymcdn.com/sites/iodsa.site-ym.com/resource/collection/684B68A7-B768-465C-8214-E3A007F15A5A/IoDSA_King_IV_Report_-_WebVersion.pdf.

Moyo, Admire. “Eskom at odds with researcher over alleged database leak”. Accessed on February 15, 2019. https://www.itweb.co.za/content/KPNG878d53m74mwD.

Myskja, Bjørn K. 2008. “The Categorical Imperative and the Ethics of Trust”. *Ethics and Information Technology* 10:213-220.

Newkirk, David. 2018. ‘“Apple: Good Business, Poor Citizen”: A Practitioner’s Response’. *Journal of Business Ethics* 151: 13-16.

O’Neill, Onara, 2005. “Kantian Approaches to Some Famine Problems.” In *Reason and Responsibility*, edited by J.Feinberg and R. Shafer-Landau, 639-645. Belmont, CA: Wadsworth, Inc.

Pollach, Irene. 2011. “Online privacy as a corporate social responsibility: an empirical study”. *Business Ethics: A European Review* 20: 88-102.

Primeaux, Patrick; and Stieber, John. 1994. “Profit Maximisation: The Ethical Mandate of Business”. *Journal of Business Ethics* 13: 287-294.

Protection of Personal Information Act. Accessed October 21, 2018. www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf.

Prues, Anni. 2013. “German Federal Court of Justice (Bundesgerichtshof - BGH): A Grey Zone under the Spotlight – Illegal GPS Tracking by Private Investigators”. *The Journal of Criminal Law* 78: 22-26.

Smith, Carin. 2018. “Cybercrime now 55% of gross losses in SA banking industry – report”. Accessed on October 21, 2018. https://www.fin24.com/Companies/Financial-Services/cybercrime-now-55-of-gross-losses-in-sa-banking-industry-report-20181004.

Smith, Jeff; Hasnas, John. 1999. “Ethics and Information Systems: The Corporate Domain”. *MIS Quarterly* 23:109-127.

Sullivan, Roger J. 1994. *An Introduction to Kant’s Ethics*. Cambridge University Press.

Steyn, Lisa. 2018. “Banks under Pressure on Coal”. *Business Day. https://www.pressreader.com/south-africa/business-day/20180927/282119227469311.*

The Constitution of the Republic of South Africa. Accessed October 21, 2018. www.justice.gov.za/legislation/constitution/SAConstitution-web-eng.pdf.

The Economist. 2018. “Identity: Les stats, c’est moi”. *The Economist Newspaper Limited* 429: 13-14.

von Tevenar, Gudrun. 2006. “Gratitude, Reciprocity, and Need”. *American Philosophical Quarterly* 43: 181-188.

Westin, A.F. 1967. *Privacy and Freedom*. New York, NY: Atheneum.

Wolf, Marty J.; and Fresco, Nir. 2016. “Ethics of the software vulnerabilities and exploits market”. *The Information Society.* 32, 269-279.