

Chapter 5

5.0 Summary.

The project presented a method for brand hate detection based on the state of the art natural language processing a common sense knowledge base, by classifying sentiments from a number a number of tweeter-handles of Kenyans talking about Safaricom. Safaricom being the case study firm for the project. The project analyzed comments made towards the brand name of Telecommunication Company “Safaricom”. The system implementation goal was to provide the Kenyan companies with the information they need to address quickly and protect their businesses and reputation. Despite the focus on the market share gain, taking proactive measures in mitigating security risks will help companies realize benefits in the long term and as a result, can save them from financial losses and reputational damage. Around 700 tweets were crawled for the study.

The main sections of these project were to identify the existing risks in social media in the Kenyan industrial realm, suggest mitigation strategies for countering this risks and modeling the contextualized classifier for brand name tracking.

5.1 Key findings

The project goals was to create a contextualized methodology for brand reputation tracking within the enterprise that can be replicated locally among the Kenyan companies. This was achieved and can be seen in the word cloud that plotted the accounts that have most of the negative tweets about Safaricom.

In addition brand tracking can help organizations take proactive security measures such as getting to identify social media squatting accounts masquerading as their company name, A common problem in social media, such kind of accounts can lead to brand and reputation damage by deceiving customers and luring them to phishing attacks, which if not mitigated on time might even lead to financial losses for the company and customers as well.

Social media monitoring will also help companies to get wind of situations in the work place such as flash mobs and go slows in time just before they are actualized resulting into disruption of normal business and the overarching losses that ca be realized when that occurs. They can identify perpetrators since social media is open for everyone to post anything they wish.

Finally, another important factor, in which social media monitoring can help companies is identifying when sensitive or confidential information is leaked to the public, way before, it creates an uproar in the social media, such sensitive information as trade secrets, company presentations, and even documents can find their way into the social media. This documents normally have the company names and hence can easily be captured when conducting brand mentions tracking.

5.1.1 Identified risks of social media Safaricom Case Scenario

5.1.1.1 Cyberloafing

Employees are normally doing unproductive activities like chatting, surfing the Internet, downloading videos and music during office hours, activities that are bandwidth-hungry and slow the speed of internet for those using it for business. This analysis could not be proven for the case of Safaricom since the project was done, by just crawling and analyzing tweets and not in the Safaricom business environment.

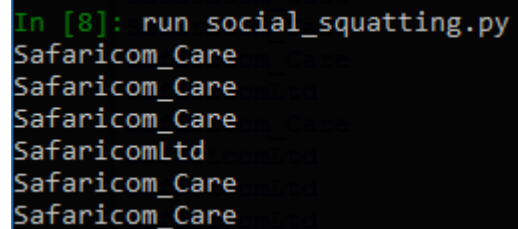
5.1.1.2 Social media squatting

Social Media squatting is where people masquerade as genuine company accounts on Facebook, Twitter, and LinkedIn. They are mainly known to target large organizations. In the case of Safaricom. An Analysis of the tweets revealed that there are no persons that are squatting on Safaricom accounts on Twitter. This was done by searching for accounts associating/relating with Safaricom from a dataset of 700 tweets crawled from twitter. All the verified accounts that were revealed were:

1. SafaricomLtd
2. Safaricom_Care

Which are the Telcos? Verified accounts.

This analysis was done by running the social_squatting.py file as shown in the figure above.



```
In [8]: run social_squatting.py
Safaricom_Care
Safaricom_Care
Safaricom_Care
SafaricomLtd
Safaricom_Care
Safaricom_Care
```

5.1.1.4 Reputation risk

A case scenario from social media monitoring and analysis of the negative tweets about Safaricom helped in identifying instances of Reputation risk emanating from a customer. A tweet during rounds on the social media attracted a number of retweets. The classifier classified this tweets as negative with a higher polarity of up to 100% and all the usernames tweeting the same could be categorized. A sample run of the python file reputation_damage.py as below tracked the tweets and retweets of the link where a particular customer was trying to reveal a controversy in Safaricom, where apparently a sim swap by someone masquerading as Safaricom agent resulted into, loss of MPESA money. “<http://village.oyaore.com/home/post/2082/an-open-letter-to-safaricom-ceo-bob-collymore-the-elements-within> “.The link for the blog where the reputation risk emanated.

```

In [6]: run reputation_damage.py
(698, 'C_NyakundiH', "'Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/Kknzlkv0z5 via @C_NyakundiH https://t.co/iUvefuOnU4'"')
(701, 'C_NyakundiH', "'Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/Lzpaaw98im'"')
(702, 'WysiiDe', "'RT @C_NyakundiH: Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/Kknzlkv0z5 via @C_NyakundiH https://t.co/...'")
(703, 'EmmanuelTende', "'RT @C_NyakundiH: Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/Lzpaaw98im'"')
(705, 'JobAbuga4', "'RT @C_NyakundiH: Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/Kknzlkv0z5 via @C_NyakundiH https://t.co/...'")
(708, 'RobertSyundu', "'Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/MuL4o1LP6c ... via @C_NyakundiH https://t.co/Qhj4WDYrMx'"')
(709, 'RSwasa', "'Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/ksSY7JDysZ ... via @C_NyakundiH https://t.co/29rleySEE6'"')
(710, 'evansonomondi', "'Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/qbpMECs21j ... via @C_NyakundiH https://t.co/Gil0BHCHAR'"')
(711, 'C_NyakundiH', "'RT @RobertSyundu: Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/MuL4o1LP6c ... via @C_NyakundiH https://t.co/...'")
(715, 'C_NyakundiH', "'RT @RSwasa: Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/ksSY7JDysZ ... via @C_NyakundiH https://t.co/...'")
(716, 'kionyo78', "'RT @RobertSyundu: Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/MuL4o1LP6c ... via @C_NyakundiH https://t.co/...'")
(717, 'ReubenSimiyu_', "'Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/EmoYpmwVFG via @C_NyakundiH'"')
(718, 'RuthMusyk', "'Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/RS29exahcn via @C_NyakundiH'"')
(719, 'C_NyakundiH', "'RT @ReubenSimiyu_: Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/EmoYpmwVFG via @C_NyakundiH'"')
(720, 'C_NyakundiH', "'RT @RuthMusyk: Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/RS29exahcn via @C_NyakundiH'"')
(722, 'c_kwadha', "'Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/yvgr8ndNPz via @C_NyakundiH'"')
(724, 'C_NyakundiH', "'RT @c_kwadha: Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/yvgr8ndNPz via @C_NyakundiH'"')
(726, 'leon_omollo', "'RT @C_NyakundiH: Oh No, Not Safaricom Again! Fresh Controversy In Notorious Telecoms Firm https://t.co/Kknzlkv0z5 via @C_NyakundiH https://t.co/...'")

```

5.1.2 Mitigations strategy

To effectively control social media use by both employees and enterprises, a well-documented strategy needs to be developed, with the input of all the relevant stakeholders. This includes the business management, the human resource, officials entitled for risk management, and the legal representation. An approach of this perspective by holistically integrating emerging technologies into the business will help to ensure risks are considered, with the view of the broader business objectives. A strategy to address the social media risks should focus primarily on user behavior, with the development of policies and offer of support for training and awareness programs which covers.

- Individual use in the workplace:
 - Is it allowed or not
 - Is it a nondisclosure of business-oriented content
 - Is it a discussion of work related topics
 - Inappropriate content and conversations
- Individual use out of the workplace
 - Nondisclosure of business-oriented content
 - Ordinary disclaimers for employee identification
 - The hazards of posting a lot of personal information
- Business/Enterprise use

- Is it allowed
- Is there a process to gain approval for use
- What is the scope of information allowed to flow
- What are the disallowed activities
- Consider the escalation process for consumer related issues.

Proper training and education are imperative, vulnerabilities of social media usage should be well apprised to every employee. Organizations can also consider. A standard “Social Media Safety 101” class as a good starting point. Consequently, a compact and all-inclusive social networking policies should be put in place, and enforced through continuous monitoring leveraging the intelligence tools such as sentiment analysis, for monitoring real-time posts. In addition, a proactive, continuous monitoring is highly essential for success, hence all organizations should take responsibility by knowing the greatest goal beyond these social media sites. Lastly, business departments must subscribe to a solid organizational feedback loop. This is with regards to the common tendency for departments to point the finger to another department. Businesses should consider the fact that whenever a breach occurs it is more than just a public relations issue, or rather, just a normal security, legal IT, human resources or security issue. Every department has a specific role to play which can either make or break an organization's social media policy.

Threats and Vulnerabilities	Risks	Risk Mitigation techniques
Employee posting of pictures or photos that link them to the enterprise	<ul style="list-style-type: none"> - Privacy Violations - Loss of competitive advantage - Reputational damage - Brand Damage 	<ul style="list-style-type: none"> - Social media monitoring. - Ensure existing policies address postings of employees. - Develop awareness training and campaigns.
Cyberloafing	<ul style="list-style-type: none"> -Productivity loss -Increased risk of exposure -Strains on bandwidth 	<ul style="list-style-type: none"> - Social media monitoring. - Managing social media accessibility through content filtering.
Employee access to social media through enterprise – supplied mobile devices(PDA’s and smartphones)	<ul style="list-style-type: none"> - Data leakage - Phishing 	<ul style="list-style-type: none"> - Routing enterprise smartphones through corporate network filtering technology to restrict social media usage. - Social media policy

		<ul style="list-style-type: none"> - Conduct a rigorous training and awareness campaigns emancipating employees of the risks posed by social media sites.
Social media Squatting	<ul style="list-style-type: none"> - Reputation Damage - Brand damage 	<ul style="list-style-type: none"> - Social media monitoring to analyze fake, unverified company accounts.
Using personal Accounts for work-related postings/information	<ul style="list-style-type: none"> - Loss of competitive advantage - Reputational Damage - Privacy Violations 	<ul style="list-style-type: none"> - Formulate effective social media policies - Update policies regularly - Training and awareness campaigns - A standard “Social Media Safety 101” class

5.1.3 Suggested Policy Formulation guideline for Social Networking Sites.

<Company Name>

Social Networking Policy

1. Overview

Social networking is gradually being seen as a fundamental element of work as well as personal life. Whilst industries are simultaneously gaining approval for social media tools as a means for endorsing goods and services, at the same time improving retention of workers, there is always an ever present risk of employee abuse or sensitive information pilferage.

2. Purpose

The drive is to provide a framework for contractors, workers and other personalities carrying out work for <Company Name>, on the acceptable use of the Enterprise social networking tools at work and in personal usage situations.

3. Cancellation or Expiration

This policy document has to be reviewed and updated as required in line with the dynamic nature of these social media tools. Therefore the policy does not particularly have an expiry date

4. Scope

The Social Media Policy applies to all those personalities working on behalf of <Company Name> regardless of whether they are part-time or full-time employees, on contract, casual workers, business partners, temporary agency workers, and vendors.

5. Policy

5.1. Speaking on Behalf of <Company Name>

Specific individuals doing work on behalf of <Company Name> will, in lieu of their position, be familiar with particular aspects of <Company Name> and for that may be legalized to talk on the behalf of <Company Name>

- One must not express his/her views on behalf of <Company Name> unless (the person) is influential on the matter And has been legalized, by the book, to communicate on behalf of <Company Name> by the manager or liable <Company Name> executive.
- You must not give out information confidential or proprietary. Only public available
- Information or information which you have been authorized to share may be disseminated.
- Be transparent. Clearly identify yourself, that you work for <Company Name>, and what your Role is.
- Be professional. This includes being honest , respectful and factual at all times.
- Do not refer to the Products or services of vendors, client's customers or partners without obtaining their consent.

5.2. Personal use of Social Media Activities

It is well known that particular personalities working on behalf of <Company Name> will be active on social media.

If one is discussing products or services provided by <Company Name> , then one obligated to identify themselves as an employee distinctly show that the views are theirs and do not epitomize the views of <Company Name> .

You must not express disapproving statements about <Company Name>, its employees or officers, or any Product or service provided by <Company Name>.

You may not trade or recommend any product or service which would compete with products or services sold by <Company Name>.

When on the job, social media access should be confined to limited personal use.

6. Enforcement

Any individual found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contract and potentially legal

action.

7. Definitions

Limited personal use – A philosophy that employees are permitted limited personal use of <Company Name>computing resources when that use does not:

- Interfere with the business usage of<Company Name>resources.
- Is performed on non-worktime

This policy is adapted from: “Datei, C. K. G. Social Networking Policy”

Chapter 6

6.1 Problems encountered during the project

Some of the problems encountered in the project included:

Lack of enough time, the project was executed within a limited timeframe and hence we had to work with time constraints, which in one way or another helped us to cope with the pressure of meeting the deadlines.

Financial Constraints, the project execution was not without financial constraints such as printing the documentation and purchasing bundles for the doing research online in addition to implementing the project.

Inadequate time with supervisors was also another impediment in the study, not getting adequate time with the supervisor always meant, creating time for correcting errors at a later time.

How Objectives of the Project were met

6.2 Potential future work.

According to “*Six Converging Technology Trends*”. (2016) a report by KPMG. A number of converging trends are emerging for businesses such as big data and social media, and companies can use the big data crawled from social media to enhance security by finding insights from the data. Wright, (2016) indicates that social media data can be beneficial when there is a need for near-real-time visions into crime patterns. Experimental data gathered from social media can eventually be used or applied hate crimes. Hence future works on the project will entail using the big data from social media in predicting crime. In addition to sentiment analysis, image analysis can also be used to determine and analyze images posted on the internet and how they might contribute such crimes as cyber bullying.

6.3 Conclusions

Companies should be able to enhance social media security in their enterprises, by having social media strategies and social networking policies to help them in dealing with the inherent risks. These coupled up with intelligent social media monitoring will help in mitigating this risks.

6.4 Recommendations

Enterprises should not be left out in the uptake of social media since it a great social business strategy that has a greater return on investments in terms of profits. However, relevant personnel should be included in conducting a risk assessment before accepting this E.S.N.Ts into the business. Policies and Social media monitoring tools are great for any business embracing social media for market share gain since it will help them reduce both financial losses and reputation risks

