SACJ 31(2) December 2019
Research Article

Context-aware technology public discourses and (un)-informed use: The case of users in a developing country

Ayodele A. Barrett, Machdel Matthee

Department of Informatics, University of Pretoria, South Africa

ABSTRACT
There is a move towards a future in which consumers of technology are untethered from the devices and technology use becomes subliminal. With this increasing device opacity, loss of user control and increasing device autonomy, there are calls for more research on users' privacy and freedom of choice. There are, however, key figures in the creation of modern technologies who suggest that consumers are informed of the implications of the use of these technologies or, that consumers use the technologies willingly. This paper examines, using Critical Discourse Analysis, two genres of IT-related communication *viz*. a speech made by the CEO of Facebook, the largest social-networking site and, the privacy policy document of Truecaller, said to be the most-downloaded app in Africa. Furthermore, 25 Sub-Saharan African users were interviewed on their use and understanding of smartphones. The analysis reveals concerns of consumers regarding the absence of choice, a lack of knowledge and information privacy erosion are not unfounded. The results show also that with the speech and policy document alike, there was information that was distorted or omitted. The conclusion was that the discourses surrounding context-awareness, through confusion, misrepresentations, false assurances and illegitimacy, contribute to information imbalances and asymmetry but most importantly, an uninformed consumer.

Keywords: public discourses on context-aware technologies, informed use of smartphones, context-aware technologies, critical discourse analysis, smart phone users in developing countries, privacy violation

Categories: • **Human-centered computing** ∼ **Ubiquitous and mobile computing** • **Security and privacy** ∼ **Human and societal aspects of security and privacy**

Email:
Ayodele A. Barrett barrettaa@tutanota.com,
Machdel Matthee machdel.matthee@up.ac.za (CORRESPONDING)

Article history:
Received: 22 Mar 2019
Accepted: 16 Oct 2019
Available online: 20 Dec 2019

1 INTRODUCTION

The recent controversy surrounding Facebook (FB), the world's largest online, social networking site (Facebook, 2018; Statista, 2019), and Cambridge Analytica Ltd. (Analytica, 2018), a now inoperative, political consulting firm, has brought into sharp focus, perhaps as never before, the issue of data privacy. By inviting Facebook users to install an app, ostensibly to assist in academic

Barrett, A.A. and Matthee, M. (2019). Context-aware technology public discourses and (un)-informed use: The case of users in a developing country. *South African Computer Journal 31*(2), 1–33. https://doi.org/10.18489/sacj.v31i2.694

SACJ is a publication of the South African Institute of Computer Scientists and Information Technologists. ISSN 1015-7999 (print) ISSN 2313-7835 (online).

research, a researcher was able to gain access to, and collect, Personally Identifiable Information (PII) of the app users. Additionally, the app collected information about friends of app users, resulting in upwards of 80 million FB users' data being garnered, from 270,000 app installations. The data collected was subsequently sold to a firm called Cambridge Analytica (CA). The firm is alleged then to have used the data to alter and influence the opinions of voters in America and beyond. The data collection has been shown to have occurred without full knowledge of the users (Confessore, 2018). The use of data manipulation tactics seemingly was not restricted to western democracies. News reports suggest that CA attempted to weaponize data in Sub-Saharan Africa (SSA) politics. In Kenya, there are claims that the firm may have assisted current president Uhuru Kenyatta to win the recent 2017 elections (Crabtree, 2018; News, 2018). Whilst in Nigeria, it is believed that CA attempted, unsuccessfully, to assist in the re-election of former president Goodluck Jonathan (Cadwalladr, 2018; Lynch, Willis, & Cheeseman, 2018). It has not been established, however, how many Facebook user accounts were harvested in both scenarios.

As a result of this scandal, the CEO of FB, Mark Zuckerberg, was summoned to testify in a United States congressional hearing in April 2018. In response to questions from politicians, a constant refrain from the CEO was that users knew what they had signed up for. Repeatedly, there was emphasis by Mr Zuckerberg that users voluntarily chose to provide and share their information and this was done with full knowledge of the repercussions. Assertions such as (Post, 2018):

"*You know, every day, about 100 billion times a day, people come to one of our products, whether it's Facebook or Messenger or Instagram or WhatsApp, to put in a piece of content ...*"

"*... someone chooses to share something on Facebook ...*"

"*The content that you share, you put there. Congressman, as I've said, every time that a person chooses to share something on Facebook, they're proactively going to the service and choosing that they want to share.*"

The Facebook-Cambridge Analytica saga and subsequent discussions have focused mainly on social networking sites, particularly Facebook. Also at issue is the willingness of users to share their information on such sites and their willingness to be vulnerable to the actions of others over whom they have no control. Consumer choice, however, of how much to share, when and, with whom, is more limited with other forms of modern technology being used to achieve a vision of technology pervasiveness and ubiquity. Achieving this concept requires a world in which data is gathered with minimal human interaction, from a series of inter-connected computers with greater degree of device autonomy and, technology which fades into the subconscious - a concept famously articulated as "ubiquitous computing" by Weiser (1991). This vision is being actualised through context-aware computing, of which the smartphone is arguably the most widely and commonly-used example. Indeed with smartphones, user data can be gathered easily, without direct user input or possibly without the knowledge or consent of the user as evidenced by a notice from an Android app, depicted in Figure 1.

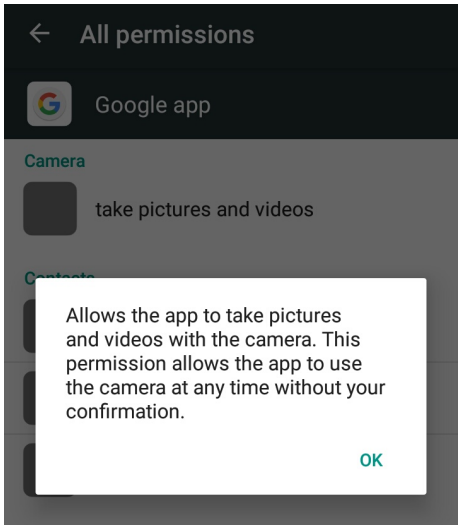

Figure 1: Example of the permissions list of an Android app

This FB-CA saga has brought to the fore not only the issue of privacy erosion but a few other areas of concern. These include, but not limited to, research ethics, propaganda, misinformation, disinformation, privacy rights, the ownership of data, informed consent and the adequacy of the consent. It is the latter that will be addressed in this paper, specifically with the use of context-aware technologies.

Makers of modern, ubiquitous technologies allude to a level of understanding by consumers, that people are aware of what they are doing and how their actions will affect them. Communication with, and consent by, consumers of these technologies is typically conveyed via policy statements, such as a privacy policy statement. For smartphone apps, consent is assumed to be given when a user accepts a permission list or dialog (Krasnova et al., 2013). A number of researchers have investigated privacy policy statements from different perspectives such as their readability (Luger, Moran, & Rodden, 2013) and the appropriate time for displaying them (Balebako, Schaub, Adjerid, Acquisti, & Cranor, 2015). It has been established also that users do not read these policies in detail when accepting them (Meinert, Peterson, Criswell, & Martin D, 2006). Little of this research, however, involves the perspective of the user and consequently, with less focus on the disempowering nature of these documents. This paucity is particularly stark within a developing world context. This paper thus endeavours to contribute further to the investigation of informed decision making.

Jürgen Habermas, a critical theorist, suggests that for communication to be valid, there must be full and mutual understanding by all parties (Habermas, 1984). Through interviews with users in addition to the analysis of software documentation and commentary by notable Information Technology individuals, the validity of assertions made by some technology producers are interrogated. The examination begins first, in the next section, with background literature review for two streams that are thought to be relevant to the paper *viz.* informed consent from differing epistemological lenses and, privacy concerns from an emerging economy perspective. This paper is an extension of a paper

presented at the SAICSIT 2018 conference (Barrett & Matthee, 2018).

2 LITERATURE REVIEW

2.1 Informed Decision Making

Research on informed consent has been undertaken in various disciplines particularly in the medical field where, ethically and sometimes legally, patients are required to formally agree to partake in forms of clinical practice or trials. The onus often is on the health provider to ensure that every effort has been made to guarantee full understanding by the patient and, if needs be, as an on-going process (Bartholome, 1989). Despite the long history of medical intervention, however, the practise of formally establishing informed consent is fairly recent, following the Nuremberg Trials of the 1940s after the second World War (Murray, 1990). Accordingly, the definition of informed consent used will be adopted from the medical field as being the process of granting permission by one party (the recipient of a service, product etc.) to another (the provider of a service, product etc.), in full knowledge of the possible benefits, risks and consequences. This requires not only the provision of sufficient information, but also ensuring the full understanding of that information (Beardsley, Jefford, & Mileshkin, 2007).

In the relatively-younger field of information technology, there is comparatively less research in informed consent regarding modern technology use. There is, however, growing interest in this field. Informed consent with the use of information technologies is said to be achieved primarily with Terms and Conditions (TC) statements and Privacy Policy Statement (PPS). Both are legally-binding documents often used by technology providers to communicate with their consumers. A TC statement typically stipulates what a user can do with the technology and what could cause the termination of service, by the provider, to the user. A PPS stipulates what user data will be gathered, how it will be used and stored and, with whom the data may be shared. A TC can subsume a PPS, although it is recommended that both documents are kept separate (Fitzgerald, Marotte, Verdier, Johnson, & Pape, 2002; Luger et al., 2013).

Information Systems (IS) research is undertaken to understand the use of information technologies by people. Typically, this research is done using any of three generally-accepted paths to conducting research. Two of these being long-established approaches of positivist and interpretive research. The former is described as objective and generalisable with phenomena of interest said to be represented and measured in a simple and an uncomplicated manner. It matters not if they are animate or inanimate (Hirschheim, 1992). Significantly, historical contexts are disregarded and the status quo is that which is considered (Orlikowski & Baroudi, 1991). The positivist paradigm, when applied to information systems research, has been utilised to explain and predict, with no attempt to interpret the phenomenon (Walsham, 1995).

Interpretive research, eschewing the notion of objectivity, is premised on the idea that all reality and human action are subjectively meaningful and socially constructed by human actors (Orlikowski & Baroudi, 1991). There is an (over) emphasis on subjectivity and hence practitioners of interpretive studies are constrained in their ability to intervene in situations of conflict or power inequality

(Watson & Watson, 2011), with no allowance made for the possibility that the lived experience is mediated by power relations within social and historical contexts (Ponterotto, 2005). Interpretive studies typically focus on understanding how issues have come about, with emphasis on coping with the dynamics of inequality but not questioning them (Walsham, 1995).

Much of the research conducted on informed decision making of modern technologies fall within either of these two streams. Examples include assessing the breadth, clarity and brevity of employee security policies in determining how well-written the documents are (Goel & Chengalur-Smith, 2010). In a similar vein, the readability assessment of the terms and conditions for a web-based supplier revealed that the level of literacy required for understanding was higher than that of a functionally-literate adult (Luger et al., 2013). There has been effort to standardise contents of privacy policy statements with findings suggesting that the use of rigid and directly-comparable privacy policies would be beneficial to website users (Cranor, 2012; Kelley, Cesca, Bresee, & Cranor, 2010). A longitudinal, comparative study of privacy policies in terms of length and readability finding the length of website privacy policies increased over time, and the readability of the policies decreasing over the same period (Milne, Culnan, & Greene, 2006). Attempts have been made to monetarise time spent reading privacy policies of different websites (McDonald & Cranor, 2008). By examining scores of privacy policies of companies based in North America, and by conducting a web-based survey of hundreds of users, it was found that there is a disparity in what users expect and what companies stipulated in privacy policy documents (Boritz & No, 2009). In context-aware related technologies, it was found that majority of the medical apps under consideration had no privacy policy statements, despite their access to sensitive medical data Goh, 2015. A negotiated approach to setting app permissions Baarslag et al., 2016 and the rethinking of the design of consent mechanisms for ubiquitous computing were suggested Luger and Rodden, 2013.

Researchers have shown the benefit of plurality of epistemologies by demonstrating a difference in results as epistemological lens shift from positivist paradigm to the interpretive and lastly critical theory (Trauth & Howcroft, 2006; Trauth & Jessup, 2000). There is a growing number of critical research, albeit fewer in numbers relative to the former two epistemologies. In contrast to other paradigms of IS, however, critical theory is based on the belief that the social and technological systems being studied need not only be understood and explained, but must also be scrutinised and critiqued for situations that are unjust and unequitable (Fitzpatrick, 2002; Lyytinen, 1985; Richardson, Tapia, & Kvasny, 2006). Applying the critical lens to phenomena implies an assumption that society can and should be improved (Stahl, 2008).

2.2 Information Privacy Concerns: An Emerging-Economy, African Perspective

There have been many calls advocating for an increased use of ICT, ostensibly to bridge yawning gaps between emerging economies and developed economies (Stahl, 2008). Emerging Economies, as most African countries are classified, are places with some of the fastest growth in ICT use. Despite this, mainstream Information Systems research remains focused more on developed economies such as the North America and Europe. In the many years since the paucity was pointed out (Roztocki &

Weistroffer, 2008), the situation remains largely the same (Ponelis & Holmner, 2015). As a case in point, a global survey of respondents of 38 countries regarding information privacy concerns spanned all continents with the exception of mainland Africa (Bellman, Johnson, Kobrin, & Lohse, 2004). Nevertheless, research numbers are increasing and research has been undertaken in areas such as advocating technology use, particularly mobile technology, in empowering citizenry in areas such as economic, gender and political enfranchisement (Andjelkovic, 2010; Naidoo, 2010; Sane & Traore, 2009; Watkins, Goudge, Gomez-Olive, & Griffiths, 2018).

Information privacy, said to be a subset of privacy in general, has been described as an individual's right to control how their personal information is used by others, such as corporate organisations (Cullen, 2009; Makulilo, 2016). Information privacy discourse often is framed as data protection (Steijn, Scouten, & Vedder, 2016). A number of African countries have, or are in the process of enacting data privacy laws. Of the 54 countries and territories which make up this region, only 14 have enacted privacy and data-protection laws, as of 2017 (Andjelkovic, 2010). There is, however, no unified set of privacy laws such as those recently implemented by the European Union (Commission, 2018; Makulilo, 2016). Furthermore, in a country such as Nigeria which follows a federal system, government-enacted laws are applicable only to government institutions and the Federal Capital Territory, Abuja. Each of the nation's 36 states is required to formally table federal laws for them to be enforceable within the states (Nwankwo, 2016).

While there is no cohesive, continent-wide approach to ensuring data privacy, there is nonetheless ongoing research, particularly on Internet use. In South Africa, it was found that while Internet users within a higher income bracket were more likely to be concerned about the information privacy, the more educated respondents were less likely to be concerned (Zukowski & Brown, 2007). Other research finds that while the cultural worldview supports individualism, influences of communal living and interdependence makes for privacy being less of an important concept to many African societies, than in Western cultures (Makulilo, 2016). Also, the lack of infrastructure coupled with the need for communication has led to developing economies, particularly in Africa, adopting many technologies with little or no consideration for associated unintended consequences (Nwankwo, 2016).

3 THEORETICAL FOUNDATION

Critical theory, the underlying epistemology, is particularly apt. Wodak (1989), quoting van Dijk (1986, p. 4) states that "it starts from prevailing social problems, and thereby chooses the perspective of those who suffer most, and critically analyses those in power, those who are responsible, and those who have the means and the opportunity to solve such problem." The issue of information privacy, the ability for one to determine when and how others collect and use people's personal information is increasingly becoming important with rapid information technology development, and the evolution of norms (Sloan & Warner, 2013).

The theoretical foundation of this research is based on the Theory of Communicative Action (Habermas, 1984). In addition to being arguable one of the most influential theoretical frameworks in the field of IS and CST (Johnson, 1991), it was chosen also for being a theory based on

communication, one which provides a means of analysing and detecting distorted communication (Cukier, Ngwenyama, Bauer, & Middleton, 2009). Communication is said to be distorted if there is resultant misrepresentation, confusion, false assurance and illegitimacy. In contrast, communication which is free from distortion builds comprehension, trust, knowledge and consent (Cukier, Bauer, & Middleton, 2004). According to Habermas, "the concept of communicative action presupposes language as the medium for a kind of reaching understanding, in the course of which participants, through relating to a world, reciprocally raise validity claims that can be accepted or contested" Habermas, 1984, p. 99. The validity claims spoken of, implicit in communication, are those of comprehensibility (so that the speaker and hearer can understand one another), sincerity (so that the hearer can believe the utterance of the speaker), of truth (so that the hearer can share the knowledge of the speaker) and a claim of legitimacy (so that the hearer and the speaker can agree with one another based on a recognised, normative background) (Habermas, 1976, 1984). Of the four validity claims of an utterance, three are each associated with a world of reason that contain possible conditions that make their validity claims acceptable. Thus a claim may be made against the objective world which may or may not be true. The claim to the social world is regarding something that may or may not be right or legitimate. The claim to the subjective world is a claim to being sincere or otherwise.

When a breakdown in communication occurs, one or more of the validity claims has been called into question. This could be for a number of reasons such as gaining additional insight based on other opinions on the subject matter (Johnson, 1991). Through discourse, a process of engagement which occurs only if a validity claim is called into question, there is an attempt to answer how a problematic claim can be supported by good reason (Habermas, 1984). Upon testing statements against the claims, should the communication not satisfy one or more of the validity claims, the person doing the analysis should examine the orientation and objective of the speaker to make a judgement call on the true intent of the discourse. Participants may also decide to abandon the communicative act of seeking consensus and adopt a strategic stance which entails influencing with a view to gaining ascendancy (Johnson, 1991). An alternative to communicative action is strategic action in which the intention of the speaker is not to seek mutual understanding but one of achieving strategic success either by influencing, manipulating or systematically distorting communication to achieve a particular end (Cukier et al., 2004; Cukier, Ngwenyama, et al., 2009; Habermas, 1984). There are other excellent sources of explanation of the theory such as (Janson & Cecez-Kecmanovic, 2005; Johnson, 1991; Klein & Huynh, 2004).

4 METHODS

An assertion by prominent IT personalities, such as Mr Zuckerberg, that consumers of Information Technologies are in control of their private data is more likely to be believed by users. According to Hoffman et al. (Hoffmann, Proferes, & Zimmer, 2018), certain individuals are better able to influence technology-oriented messages which in turn, shape how public opinions are formed. Given such an assertion that consumers likely have an understanding of the implication of using Information Technologies, semi-structured interviews were conducted of Nigerian consumers. In addition, validity

clams from two genres of IT-related communication were analysed critically using Critical Discourse Analysis (see Section 4.2). Conducting empirical critical research is vague (Myers & Klein, 2011). This lack of clarity is, in turn, exacerbated by a dearth of empirical work to provide guidance for pursuing further empirical research (Stahl, Tremblay, & LeRouge, 2011; Trauth & Howcroft, 2006). As such, those undertaking critical research are encouraged to draw from existing critical studies (Myers & Klein, 2011). Accordingly, prior critical research utilising semi-structured interviews and Critical Discourse Analysis (CDA) were drawn upon for methodological guidance, specifically (Cukier et al., 2004; Trauth & Howcroft, 2006). The research was therefore conducted in two phases. The first being that which included conducting interviews and analysing interviewee responses. The second phase consisted of collecting and analysing public discourses on context-aware technologies.

4.1 Data Collection and Analysis: Interviews

Since this is a Critical Theory study, the intent is not about generalising to a larger population. Accordingly, it was decided to select a *non-probability sampling* technique, specifically the *snowball sampling* technique. This also ensured that the sampling of potential interviewees could be conducted in a systematic, rather than arbitrary, manner. Snowball sampling entails the identification of one or two potential interviewees that meet the necessary criteria. Interviewees had to be businesspersons who owned their own (typically very small) business and made use of their smartphones in conducting their business. In addition to selecting them for interview purposes, the interviewer relies also on the initial interviewees to help in identifying more potential interviewees. This approach was particularly useful being that the researcher does not reside in the same country as the citizens who formed the base of the empirical situation and did not know enough people who met the criteria. Thus from an initial three interviewees an additional 27 potential interviewees were recommended, five of whom were omitted for reasons such as not using or owning a smartphone or not being available for interviews. The interviews were conducted in two of Nigeria's 36 states (Lagos and Oyo), as well as the Federal Capital Territory, Abuja. Ethical clearance for questions asked and the data gathering process was granted by the Faculty Committee for Research Ethics and Integrity, in the Faculty of Engineering, Built Environment and Information Technology, at the University of Pretoria, South Africa.

Interviews are social interactions in which questions are put to people for the purpose of discerning people's experiences and perspectives regarding issues being investigated (Ho, 2013). Interviewees were informed about the research focus on the use of digital devices and privacy-related matters. Semi-structured interviews were particularly apt since it allowed for prepared questions to be asked while making allowance for asking improvised questions (Myers & Newman, 2007). When used for critical theory research, in addition to seeking a participant's subjective representation, interviews are used to encourage reflections on experiences that have been recounted. Reflections could take the form of encouraging an awareness of any contradictions between, perhaps, what is being said in the interview and behaviours in times past (Trauth & Howcroft, 2006). The semi-structured interview questions were grouped according to:

- consumers' historical context (choice of technology and reasons)

- technology use (frequency of use, habits, reasons for use)
- views on privacy and security (awareness of privacy violations and behaviour to avoid it)
- opinions and behaviour regarding informed consent and trusting behaviour (willingness to use technology despite risks)

Various themes were identified during the analysis of the interview transcripts, a few of which are discussed in Section 5.1, such as a lack of technology know-how and a high degree of dependency.

4.2 Data Collection and Analysis: Public Discourses

Responses from interviewees were key in deciding the subsequent selection of Truecaller (Truecaller, 2018a) as the app whose privacy policy statement was analysed. All the interviewees had downloaded and installed the app on their phones. Additionally, the website associated with the app claimed to be one of the most fastest-growing, downloaded apps in Africa since 2016 (Kok, 2018). Truecaller, a Swede-developed smartphone app, is a global, crowd-sourced telephone directory with additional functionality. Furthermore, Truecaller's business model is akin to the approach taken by the Cambridge Analytica-associated researcher – one of overreach as friends of app users have their data harvested. Truecaller's database is reportedly populated with over 3 billion telephone numbers (Press, 2016). As stated on the company's website, their number of users is "hundreds of millions." The implication of this being that people are likely to have their data stored in the company's database despite not having installed the app or agreeing to their terms and conditions.

Additionally, all of the interviewees had Facebook accounts albeit with varying levels of use. Most accessed the platform via the app on their smartphone. Facebook is the world's largest social networking site with an estimated 2 billion active users (Facebook, 2018; Statista, 2019). Even for people who do not have a Facebook account, the app often is pre-installed on many Android smartphones as a system app, which are apps that cannot be easily uninstalled by the user. Thus analysis of commentary related to the recent Facebook-Cambridge Analytica scandal is perhaps apt. In the words of Senator Orrin G. Hatch of the United States Congress, uttered during the Zuckerberg congressional hearing: "Well, in my opinion, this is the most — this is the most intense public scrutiny I've seen for a tech-related hearing since the Microsoft hearing that — that I chaired back in the late 1990s. The recent stories about Cambridge Analytica and data mining on social media [Facebook] have raised serious concerns about consumer privacy..." (Post, 2018).

The analysis of the two IT-related discourses is undertaken using Critical Discourse Analysis (CDA), a critical take on discourse analysis. CDA subscribes to the overall Critical Theory (CT) notion of identifying power relations and how resulting acts of dominance are enacted. It subscribes also to the tradition of eschewing the notion of value-free science (van Dijk, 2001). It is a study of text to understand how social inequality is enacted, to expose disparities and also, to resist inequality and dominance of the powerful. Language use is the commonest form of social behaviour (Fairclough, 1989). It is therefore not unexpected that "language and meaning are used by the powerful to deceive and oppress the dominated" Howarth, 2000, p. 4. What makes CDA markedly different from

other forms of discourse analysis is the fact that it is problem-oriented, focusing on social phenomena rather than linguistic units (Wodak & Meyer, 2009). Modern discourse analysis began in the 1960s for the study of texts and communicative events (van Dijk, 1985). The critical form of discourse analysis, however, began in the 1990s (Wodak & Meyer, 2009).

Theoretically and analytically diverse, there is neither a specific methodology used, nor is there a particular theory aligned with CDA (Wodak, 1989). It is also inter-disciplinary (Wodak & Meyer, 2009), or transdisciplinary, as preferred by (Fairclough, 2013). Indeed, it is in keeping with the critical theory tradition of promoting inter-disciplinary research and eschewing the formation of specialised academic domains (Fjortoft, 2013). Huckin (1997) describes CDA as an attitude, rather than a step-by-step method. As such, there are various approaches to undertaking the critical analysis of a given discourse. van Dijk (1995) describes CDA as either problem-oriented or issue-oriented, but not paradigm-oriented. He continues, however, by advocating for the use of suitable discourse-related theories to ground the analysis in. Thus, a chosen approach in this study is one which was pioneered by Cukier, Ngwenyama, et al. (2009) using Habermas' Theory of Communicative Action (Habermas, 1984) as the framework. The tenets of the approach of Cukier, Ngwenyama, et al. (2009) are given in Section 4.3.

Cukier, Ngwenyama, et al. (2009) further call for its use in interrogating wide-ranging and diverse discourses. This call, which subsequently has been answered, include evaluating favourable mass-media representation of an e-commerce retailer in the midst of a technology-induced economic slump (Cukier, Ryan, & Fornssler, 2009) and the internal security policy document of an IT company (Stahl, Doherty, & Shaw, 2012). Although Hoffmann et al. (2018) adopted a different CDA approach, the authors analysed the utterances of Mark Zuckerberg over a decade, with an emphasis on how he defined Facebook, its users and the relationship between the social networking site and its users demonstrating the effect of his word choices over the years. As an example, one of the findings of Hoffmann et al. (2018) is that Zuckerberg misleads Facebook users about their control by creating the impression that the users on one hand, and Facebook and its commercial actors on the other hand, are of equal importance thus downplaying the large difference in power between these groups.

4.3 Operationalising Validity Claims

Cukier, Ngwenyama, et al. (2009) pioneered an approach to operationalising Habermas' theory by utilising Critical Discourse Analysis (CDA), deriving a series of questions as a means of identifying and interrogating validity claims within a discourse. A subset of these questions is utilised in the Section 5. Legitimacy, or normative rightness, is concerned with "existing normative context" (Habermas, 1984). Legitimacy regards the social world as its domain, one which is universally accessible to all. Thus norms and rules are negotiated, intersubjectively. The truth claim is used in assessing statements as being factual. The truth validity claim regards the objective world as its domain. This world, in turn, is accessed by and is the same for everyone in the discourse. The search for truth involves considering objective facts made within a statement being examined. Sincerity is concerned with the "manifest intention of the speaker" Habermas, 1984, p. 99. Sincerity claims are those made by the speaker, in relation to their inner subjectivity. This includes the speaker's desires, beliefs and other feelings

known only to the speaker. As it is difficult to assess the truthfulness or honesty of the speaker's claim discursively, the assessment is likely to occur by comparing the speaker's utterances to the speaker's behaviour. Thus redeeming this claim may require a sufficient period of time for interactions and observations to occur (Cukier et al., 2004; Cukier, Ngwenyama, et al., 2009). "Comprehensibility is the only one of these universal claims that can be fulfilled immanently to language" Klein and Huynh, 2004, p. 28. This claim is related to the use of language, rather than the contents of the speech act itself. Sometimes referred to as "intelligibility", this claim is the implicit counterpart to the question "what does that mean?" (Zinkin, 1998). If there is no shared understanding in speech between the speaker and the listener, that is no linguistically-understandable utterance, then there is nothing that needs to be assessed. Thus, this validity claim is sometimes called the precursor to the truth, legitimacy and sincerity.

5 FINDINGS

In this section, based on identified themes, excerpts from the interviews are presented. The themes include usage, the level of dependency on smart phones and the level of technological knowledge. Additionally, awareness of possible remote access to personal data and concerns regarding theft of data is highlighted, as are feelings towards privacy policy documents. Also included are the results of analysing critically, the privacy policy statement of Truecaller as well as a speech made by the CEO of Facebook.

5.1 Themes Identified from Interviews

Interviewees were numbered and the excerpts below are presented per interviewee. One of the questions asked of the interviewees was done so to gauge their **usage and level of dependency** on their smartphones. A few excerpts are presented below:

[P2]: [Laughs] More like, when don't I access my phone? My phone is part of my daily life. I do [carry the phone around]. Sometimes to the bathroom.
[P10]: Oh, I live by my phone. It's bad, so bad. I live by my phone. My wife calls my phone "my first wife."
[P13]: My phone is with me 24/7.
[P14]: It's my second life.
[P15]: [Access]? 24 hours - when I am awake. If I wake up during the night, I am picking it up.
[P20]: I think I'm addicted to it. Yeah, I'm always with my phone.
[P23]: There was a time, my phone - my android phone was stolen [it was] as if I lost somebody.

Questions were also asked to gain an understanding of **the level of technological know-how**. The questions asked were general queries on what a few IT-related terms such as "cookies", "permissions lists" as well as users' attitudes and approach to security and privacy. One question was

related to the use of public Wi-Fi:

[P9]: When I travel.
[What about here, in Nigeria?]
[P9]: Do they even have Wi-Fi in Nigeria? And maybe because of security, I'm a bit [conscious]. I don't know if they [hackers] can do anything. But for me, I don't want to be dealing with my bank or whatever [using Wi-Fi].
[But you do overseas?]
[P9]: Yeah, I do that.
[So you're willing to lower your security needs overseas?]
[P9]: I think it's more secure [overseas], that's why. I think so, I don't know if I'm right. I just feel they are more secure.

[P11]: [Public Wi-Fi?] Yes, when I'm out of Nigeria, yes. Because I feel that public Wi-Fis are not well screened here, but when I'm abroad, I want to believe that there are some sort of - [laughs] - it may be wrong - I want to believe that they should have done a bit more due diligence with their screening as against Nigeria.

[P18]: [Public Wi-Fi?] In specific places because I'm always a bit conscious about security. So, airports, shopping malls - pretty much that's it.
[Why would you think that a shopping mall's Wi-Fi is secure?]
[P18]: I don't have a - what's the word now? I don't have any facts to show that, but I tend to believe places where large numbers of people are logging on, without complaints, over a long period of time - gives me that comfort that the service is relatively secure.

[P4]: [Cookies?] Yes I do. I think I've been seeing it, but I don't know.
[P5]: Yes, I know - sometimes I follow a lot of people on social media and you don't really have to go to their websites because sometimes they allow you freely into their world, so you just get them [cookies] free sometimes.
[P7]: I've heard about them [cookies]. When I use all these HPs [laptops], even Mac, I see them. Especially when I go on newspaper sites. They are always annoying.
[P14]: What are those? No, never heard of them.
[P15]: I see them [cookies]. They say I should click on them to make something go faster. Sometimes I click, sometimes I don't.

[P19]: The permissions list? Yes I do [know]. I have it on my phone. People that I permit to — umm — maybe if my phone is lost, a message is sent to those people

There was little awareness of **possible remote access to personal data**. Oftentimes, responses were only about physical, present threats:

[You said earlier you secure your data from people around you, what about people not around you?]
[P1]: It's ok, I don't think they will want anything to do with my information.
[So you only care about people physically around you not having access to your data?]
[P1]: Exactly.

[P2]: Oh yes, I'm definitely concerned. And I don't see any reason why anybody else should have access to my data.
["Anybody else" being whom?]
[P2]: Anybody else being the second person next to me. I am aware that you can access my data via Wi-Fi or any other means that is technologically available but I don't want to see somebody pick up my phone right in front of me.

[P4]: I normally don't allow my phone out of my sight.
[P9]: [Who wants access?] My wife — she's the number one. She's the only one I can think of.
[P10]: My wife [laughs]. Basically, a lot of people just believe that there's something that you're hiding.

All too often, the concern regarding **theft of data** was linked to finances when asked what was the worst thing that would happen if people got access to their personal data:

[P7]: They will steal my money.
[P9]: My [bank] account - that's the major.
[P11]: What I have at the back of my mind really is what is the possible downside of me downloading this app ... how much money do I have that I am going to lose?
[P14]: I don't have so much to hide in life, but my finances is important.
[P15]: Just stealing my money, because there's really nothing you can do with my demographics. I'm a black, Nigerian girl, living in [city] with one child, one husband - what evil can you do with that? [Laughs]
[P23]: What will I consider to be personal data, to me? Things like bank details. Where I am, who I'm with, that one doesn't really matter.

When the issue of information privacy, regarding data other than personal finances, was discussed further **there was a lack of concern**:

[Would you care about Apple, other tech providers etc., having possible access to your data?]
[P1]: Apple has access to 130 billion people in the world [laughs], why would they care about me?
[P2]: Maybe when I become president. [Laughs] I don't know if anybody will be [interested in my data].
[P4]: I know they have access, but I don't think there's any thing that they need my data for. They will have as many [access to many], so why should it be mine that they will be after?
[P7]: I'm not worried about that. If they have access to it, am I the only one in this world? [Laughs]

https://doi.org/10.18489/sacj.v31i2.694

[P8]: No idea. Why would anyone want to be interested in my personal data? I don't know. I've never given it a thought.
[P12]: [Do I care?] Not as an individual. I somehow think I'm so small ... in the whole world's population and everything. That it'll be a chance in a billion for someone to choose me. So that's what I am thinking.
[P14]: Not really cos I don't see anything on my phone that I am trying to keep a secret.
[P18]: No. Because it's little old me, in little Nigeria. Nobody really cares about us.

It is possible that the lack of awareness of what can be done with their data could be as a direct result of **general misgivings about privacy policy documents**:

[P1]: I just rush through the terms and conditions. ... I just press agree. It's usually very long. I think they write it like that to deter people from actually sitting down to read [it]. I think it's a trick. 'Cos you know when you write so much stuff, nobody can sit down an read it — so that a lot of people just press [accept].
[P2]: I know that a lot of these manufacturers are crooked, so they put it in fine print and then I don't read it.
[P7]: No. I agree and move on [laughs]. Why? Do people read it? The 16 pages?
[P10]: No [laughs]. You know, it's always sooooo long. You just go to the "accept" and, accept.
[P12]: No. They don't mean for us to read it, because it's always like God-knows how many pages long.
[P13]: Yes, but not all the time because some of them are like a 100 pages long, true. I read up to some point — Ok, ok, ok — let me just browse through — anything pique my interest — alright, I am going to download this anyway [sigh], and I accept.
[P17]: It [policies] is for their own personal interests ... because of litigations. ... It's difficult to read through the fine lines, but they expect you to have read it — it's part of their tricks.
[P18]: Not in detail. You know those things are very wordy. And I think it's deliberate so you don't read the fine print.
[P19]: I think that they are really, really, really, really, really long. I think that they do that to dissuade people from reading it.

5.2 Senate Hearing Speech Analysis

The full speech given by Mark Zuckerberg, CEO of Facebook, at the United States Congress in April 2018, is presented below (Post, 2018). The opening greeting and the concluding thanks are omitted.

> *We face a number of important issues around privacy, security, and democracy, and you will rightfully have some hard questions for me to answer. Before I talk about the steps we are taking to address them, I want to talk for a minute about how we got here.*
>
> *Facebook is an idealistic and optimistic company. For most of our existence, we focused on all the good that connecting people can bring. As Facebook has grown, people*

everywhere have gotten a powerful new tool for staying connected to the people they care about most, for making their voices heard, and for building communities and businesses. Just recently, we've seen the MeToo movement and the March for Our Lives organized, at least in part, on Facebook. After Hurricane Harvey, people came together and raised more than $20 million for relief. And more than 70 million businesses - small businesses use Facebook to create jobs and grow.

But it's clear now that we didn't do enough to prevent these tools from being used for harm, as well. And that goes for fake news, for foreign interference in elections, and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our responsibility, and that was a big mistake. And it was my mistake. And I'm sorry. I started Facebook, I run it, and I'm responsible for what happens here. So, now, we have to go through our — all of our relationship with people and make sure that we're taking a broad enough view of our responsibility.

It's not enough to just connect people, we have to make sure those connections are positive. It's not enough to just give people a voice. We need to make sure people aren't using it to hurt people or spread misinformation. And it's not enough to just give people control of their information. We need to make sure that the developers they share it with protect their information, too. Across the board, we have a responsibility to not just build tools, but to make sure those tools are used for good. It will take some time to work through all the changes we need to make, but I'm committed to getting it right. this includes the basic responsibility of protecting people's information, which we failed to do with Cambridge Analytica. So here are a few things that we are doing to address this and to prevent it from happening again.

First, we're getting to the bottom of exactly what Cambridge Analytica did, and telling everyone affected. What we know now is that Cambridge Analytica improperly accessed some information about millions of Facebook members by buying it from an app developer. That information — this was information that people generally share publicly on their Facebook pages, like names and their profile picture and the pages they follow.

When we first contacted Cambridge Analytica, they told us that they had deleted the data. About a month ago, we heard new reports that suggested that wasn't true. And, now, we're working with governments in the U.S., the U.K. and around the world to do a full audit of what they've done and to make sure they get rid of any data they may still have. Second, to make sure no other app developers out there are misusing data, we're now investigating every single app that had access to a large amount of information in the past. And, if we find that someone improperly used data, we're going to ban them from Facebook and tell everyone affected. Third, to prevent this from ever happening again, going forward, we're making sure that developers can't access as much information now.

The good news here is that we already made big changes to our platform in 2014 that would have prevented this specific situation with Cambridge Analytica from occurring again today. But there's more to do, and you can find more details on the steps we're taking in my written statement. My top priority has always been our social mission of

> *connecting people, building community and bringing the world closer together. Advertisers and developers will never take priority over that, as long as I am running Facebook.*
>
> *I started Facebook when I was in college. We've come a long way since then. We now serve more than 2 billion people around the world. And, every day, people use our services to stay connected with the people that matter to them most. I believe deeply in what we are doing. And I know that, when we address these challenges we'll look back and view helping people connect and giving more people a voice as a positive force in the world. I realize the issues we're talking about today aren't just issues for Facebook and our community. They're issues and challenges for all of us as Americans.*

5.2.1 Legitimacy of the Senate Speech

Legitimacy entails identifying texts within the discourse that indicate participation, to find out who is accorded legitimacy in a narrative by asking who is speaking and whose voices are heard. Also, by analysing the text for any claims to rightness, legitimacy claims can be assessed. Specifically to this scenario, one could also ask how decisions regarding consumer data use is legitimised.

In seeking to answer whose voices are heard, personal pronouns in speeches can give listeners an indication of whom the speaker identifies with (Wodak & Meyer, 2009). In the speech, the first person point of view used by referencing the pronouns "we, the people of Facebook" followed by "I, the creator" were, by way of reference, the loudest voices. Fairclough (Fairclough, 1989) suggests that another use of the pronoun "we" is one with ideological implications, expressing a common-sense view to which everyone is assumed to agree without finding it necessary for the community of agreeable persons to be explicitly defined. In the speech, there were three such references of "we" in which it may be assumed that everyone agrees that "we face a number of important issues", there was also a need of a debate focusing on "how we got here" and, there was reference to a prior solidarity movement organised partly on Facebook "we've seen the MeToo movement". Zuckerberg did not explicitly define who this "we" consists of.

In prior statements, Zuckerberg often made reference to Facebook as a community of its *members*. According to Brummett Brummett, 2010, p. 73, "visibility is empowerment, invisibility is disempowerment." It is telling therefore, that there was but one direct, third-person reference made in the speech about the "Facebook member", the organisation's *raison d'être*. There were other third-person references made using the pronoun"they", or using the generic term "people." This projects possibly, the impression of an attempt to create wide narrative distance. There was also, the use of "these" in reference to Facebook as a tool "we didn't do enough to prevent these tools from being used for harm ..."). It could be an attempt to create a distance, a polarisation (Rashidi & Souzandehfar, 2010), between the people of Facebook and their creation, casting suspicion over the legitimacy of its ownership.

Rightness, associated with legitimacy, is concerned with morals and ethics. Zuckerberg makes overt references to adhering to what is right. Describing the company as "idealistic" suggests that Facebook is a company of high moral value. Additionally, he said "For most of our existence, we focused on all the good that connecting people can bring", creating "tools that are used for good" which will, in retrospect, be seen to be "helping people connect and giving more people a voice as a

positive force." Finally, in justifying how decisions regarding consumer data use was legitimised, Zuckerberg said "That information - this was information that people generally share publicly on their Facebook pages ... like their profile picture ...". This is an over-simplification of the facts. People do not explicitly make public all the information that they provide as members. Indeed, a person's profile picture, as one example, is by default set to "public", a setting that cannot be changed by the user (Center, 2018b). This is the same for other granular settings that are set by default to public, that is, it can be seen by everyone. Everyone being not only all Facebook members, including those who are not friends on the platform, but anyone with access to the Internet.

5.2.2 Truth of the Senate Speech

The search for truth within documentation would require perusing statements to determine what is considered to be factual or true (Cukier, Ngwenyama, et al., 2009). Questions asked included "what evidence has been provided to support arguments given?", "are there ideological claims which are unexamined?" and, "has the relevant information been communicated without distortion or omission?"

In the speech, the CEO said that "what we know now is that Cambridge Analytica improperly accessed some information about millions of Facebook members by buying it from an app developer. That information - this was information that people generally share publicly on their Facebook pages, like names and their profile picture and the pages they follow."

This is called a strategy of negative other-representation and one of positive self-representation. The strategy could also be used in emphasising the moral superiority or implying the good acts of self ("... on Facebook ... people came together and raised more than $20 million in relief ... more than 70 million businesses - small businesses use Facebook to create jobs ...") in contrast to the bad acts of the other (" ... what Cambridge Analytica did ... improperly accessed some information ...they told us that they had deleted the data ... we heard new reports that suggested that wasn't true"). The strategy is adopted for providing a biased account of facts in favour of whom who speaks (van Dijk, 2006). Cambridge Analytica did things improperly and people were lax about what they share. Nevertheless, there is no telling that the users of Facebook intended for their data to be made public. According to Zuckerberg, "people everywhere have gotten a powerful new tool for staying connected to the people they care about most." It is well within the realm of possibility that their sharing frame-of-reference was with the people with whom they are friends with on Facebook, and not for the whole world to see. Also because the CEO has said on prior occasions, such as in a 2006 post, said that "nothing you do is being broadcast; rather, it is being shared with people who care about what you do - your friends." Users may have taken him up on his word.

Also, there was no mention of the Graph Application Programming Interface (API). Facebook launched the graph-based API on April 21, 2010 expressly to permit third-party developers to gain access to Facebook's software platform. The Graph API, version 1, was active until April 2014 when it was deprecated, and closed completely on April 30, 2015 (Albright, 2018). It was through this API that access could be gained to user data. The newer version, Version 2, though more restrictive regarding the pieces of information that it can access, does still provide access to a fair amount of personal information. Worryingly, the information that Cambridge Analytica and others had access

to also included the information of those who did not provide any consent to their information being harvested, just because they were friends to those who may have consented to their data accessed when using the third-party app. It is true that Cambridge Analytica bought information about millions of Facebook members. There is, however, less truth in the fact that the information accessed was that which people generally shared publicly on their Facebook pages. There was a privilege labelled as “read_mailbox" which was available to whichever app accessed the API, thus enabling the apps to read private messages.

Obscuring responsibility, at an organisational level was also evident in the speech. As an example, the CEO stated that “we need to make sure that the developer they [the users] share it [their personal information] with ...". This is problematic for a number of reasons, one being that the minimum age of people legally able to use Facebook is 13 years (Center, 2018a). A 13-year old cannot be expected to understand the gravity of sharing their information. Additionally, users interacting with external, third-party apps often could not tell the difference as the app webpages were seamless with Facebook’s, the URL (Universal Resource Language, or web address) also bore Facebook’s details. To the untrained eye, the app was safe and either official or endorsed by Facebook (Bogost, 2018).

5.2.3 Sincerity of the Senate Speech

To test this validity claim would entail attempting to infer the intentions of the speaker by examining differences between what things are said, how things are said and, what the speaker does (Cukier, Ngwenyama, et al., 2009). Sincerity is difficult to discern, as it can be assumed that the speaker is engaged in unconscious hegemony, operating on taken-for-granted assumptions and not necessarily being intentionally insincere (Cukier, Ryan, & Fornssler, 2009). Examining the choice of words uttered could reveal nuances that are not apparent when cursorily read (Cukier et al., 2004). The claim to sincerity can be examined by searching for metaphors and connotative words which could reveal vested interests due to, for example, the metaphor choice (Cukier et al., 2004; Koller, 2004). Similarly, van Dijk (van Dijk, 1995) finds that rhetorical devices such as hyperboles and metaphors often are used to emphasise “our" positive properties and “their" negative properties. Conversely, figures of mitigation often are used to decrease the significance of “our" negative properties and “their" positive properties. Questions that could be asked include “do the presence of rhetorical devices (such as metaphors, hyperboles, connotative words, emotionally charged adjectives and nouns) promote understanding or suppress understanding" and “at the organisational level are there rhetorical reassurances, false expressions of concerns or hiding of motives"?

The statement presents Facebook both as a company and as an artefact. Positive, human characteristics is used to describe a company as idealistic, optimistic, a being that exists, one that grows. The giving of human qualities to non-humans, based on people’s experiences of themselves, is termed *ontological* metaphors (Wyatt, 2004). On the other hand, the description of Facebook as a tool can be seen as objectification, an attempt to depersonalise an artefact that had in many other instances been referred to as a “community." The seeming effort at distancing was further accomplished with the use of the third-person form of “those tools" and “these tools". The imagery that the word “tool" suggests is an innate entity, an implement, an “it", albeit a powerful one. In the hands of good, idealistic and optimistic people, it is something that can be used to make positive

creations, that of connecting people, keeping people connected and staying connected. In the wrong hands, however, it is something being used to cause harm and hurt. Indeed Lindh (Lindh, 2016) speaks of technology sometimes being viewed as a neutral tool or object that can be used in different ways either positively or negatively. The author goes on to add that using utility metaphors in describing technology provide a cover to hide, or make less visible, political and social implications of the technological artefact.

A third metaphor was also adopted. One of Facebook being used as a weapon "... using it to hurt people ...", which must be prevented from "... being used for harm ...". A weapon that was also being used "to ... spread misinformation". It is possible that all three metaphors were selected to help shape the narrative. Taken together, the ontological metaphor (Wyatt, 2004) could have been selected perhaps to garner sympathy. A utility metaphor (Lindh, 2016) could have been adopted also to de-personalise Facebook and portray it as a tool that should be kept in the hands of the right people. Also, a war metaphor (Lakoff & Johnson, 1980) used could have been used in rallying support against "they, the villains", common enemies that must be fought together, thus reducing the narrative to a "simplistic contest of good versus evil" (Jayawardena, 2015). Indeed, the closing statement of "I realize the issues we're talking about today aren't just issues for Facebook and our community. They're issues and challenges for all of us as Americans" can be seen in a similar vein.

5.2.4 Comprehensibility of the Senate Speech

Achieving comprehensibility would require for there to be a shared system of meaning between the speaker and the hearer (Cukier et al., 2004). Although the testimony was presented to the U.S Senate, those listening were not only those physically present in Congress. The congressional hearing was shown live on television and the proceedings followed around the world. As said by Senator Thune in his opening address at the hearing "the hearing is an opportunity to speak ... We are listening. America is listening and quite possibly the world is listening, too." Questions which may be asked include "is there use of jargon?" or, "are there terms that are not explained?" Additionally, one might seek to know if there is evidence of obfuscation.

The first two questions need no answering as the prepared statement was devoid of jargon or any technical references. While the speech was free of technical jargon that could cause confusion, little was said regarding the severity of the harvesting of user data and, there was evidence of obfuscation that requires further analysis. Zuckerberg made mention in the speech said that "That information, this was information that people generally share publicly on their Facebook pages, like names and their profile picture and the pages they follow." He would subsequently add that "we are making sure that app developers can't access as much information now." If all the information retrieved was that which was generally shared and publicly available, the need to expressly deny access to developers would seem unnecessary.

5.3 Privacy Policy Statement Analysis

Privacy policies inform consumers about a company's privacy practices. They are, in turn, used by consumers for decision making and often serve as the only source of information about the

company's data gathering activities (Jensen & Potts, 2004). As mentioned earlier, Truecaller is a Swede-developed, globally-accessible, crowd-sourced telephone directory (Truecaller, 2018a). There are two versions of the Truecaller privacy policy statement, both with effective dates of 25 May, 2018 (Truecaller, 2018b). One version is for Switzerland and the EEA (European Economic Area, consisting of 28 European Union countries plus Iceland, Liechtenstein and Norway). A second version is for the rest of the world. The non-EU version of the policy statement was the primary document utilised for analysis with the EU version referenced when discrepancies were found between the two versions. The analysis of the policy follows.

5.3.1 Legitimacy of the Privacy Policy Statement

Legitimacy of a discourse is achieved by all parties being given an equal chance to be heard. In seeking to know whose interests are best served in a discourse, suggested questions for empirical testing include: who is allowed to speak? Who is considered an expert, and on what basis? Is there accountability, or a lack thereof? The format of privacy policy statements, however, does not permit the representation of all parties. As a one-way means of communication, users are unable to raise any real-time queries about the policies. As such, users are required to accept the statement in its entirety or not at all. The perceived lack of legitimacy was raised by interviewees who voiced concerns about policies being skewed in favour of the manufacturers.

To demonstrate the asymmetry of power, excerpts from Section 8 of Truecaller's privacy policy (PPS_Section 8) are reproduced in Table 1, page 21. This shows how the policy is drafted in the interest of the creators of Truecaller and not their consumers. In the document is reference to the fact that policy changes can be made for the non-EU market without necessarily notifying its users. Also of concern is the fact that users are meant to be bound by changes which they may not know about and which they may not have consented to. This approach is known as "browse-wrap" in which a user is assumed to have given assent without necessarily providing any affirmative action (Blanke, 2005). Furthermore, the non-specific, subjective nature of what constitutes as "substantial changes" further entrenches Truecaller's position of power. A comparison of the two versions shows a deference to the EU region, because of the recently-implemented General Data Protection Regulation (GDPR) law. The GDPR is an EU-based, data protection law that came into effect in May 2018. The law is based on the notion that privacy, as a fundamental human right, must be respected. Violations include sanctions levied against an organization to the tune of up to 100 million Euro (Commission, 2018). Perhaps due to such stringency, the EEA version of the policy explicitly states that users will be notified.

5.3.2 Truth of the Privacy Policy Statement

The search for truth within documentation would require perusing statements that affirm or deny something, and whether these statements can subsequently be proven to be true of false. In testing this validity claim, the following questions may be asked: "what is said about the technology"? "Are the issues and options clearly defined"? "Has relevant information been communicated without distortion, misrepresentation or omission"? "Are there ideological claims and, is the responsibility

Table 1: Comparing two versions of the privacy policy of Truecaller to illustrate lack of legitimacy

Rest of the World	**EEA and Switzerland**
Truecaller may at any time with or without a separate notice change this Privacy Policy and You are encouraged to review this Policy from time to time. In case of substantial changes, Truecaller will notify the Users by push notice or via notice in the Services. Your continued use of the Services after a notice of changes has been communicated to You or published on our Services shall constitute consent to the changed policy.	Truecaller may at any time change this Privacy Policy. Truecaller will notify the Users of such changes by push notice or via notice in the Services or by other means. If You object to any changes, You may uninstall the Truecaller applications and cease using the Services. Your continued use of the Services after Truecaller have communicated changes to this Privacy Policy, will mean that the collection, use, sharing and processing of Your personal information is subject to the new Privacy Policy. We may from time to time set out more detailed information on how we process your personal information in relation to particular Services in supplemental Privacy Notices which shall be incorporated into and form part of the Privacy Policy.

of any party obscured"? Very little was said about what Truecaller is. There are many references to “the Services" such as “When You install and use the Services ..." (PP_Section 1.2). The first and only reference to Truecaller being a mobile application is in Section 1.4 of the policy as shown below. Indeed, nothing is said about what Truecaller, as an app, does.

PP_Section 1.4: “*Where the Truecaller mobile applications (“Truecaller Apps") are obtained from other sources than Apple App Store or Google Play, You may share the names, numbers, Google ID’s and email addresses contained in Your address book (“Contact Information") with Truecaller by enabling the Truecaller Enhanced Search Functionality. Where the Truecaller Apps are obtained from Apple App Store or Google Play, we do not share any user Contact Information*".

There are two specific instances that will be addressed in this paper -– one of misrepresentation of information, and the other of the responsibility of Truecaller being obscured. For the former, misrepresentation of information, there is a reference in Section 2.2 of the privacy policy in which Truecaller states:

PP_Section 2.2: “*We do not consider personal information to include information that has been made*

anonymous or aggregated so that it can no longer be used to identify a specific person, whether in combination with other information or otherwise".

There is research to suggest that it is possible, and with surprising ease, that anonymised and aggregated data can be, and has been, used to re-identify individuals. Such research has been demonstrated as far back as the start of the previous decade, well before the development of Truecaller (Golle, 2010; Ohm, 2010).

Furthermore, in comparing both privacy policy versions, there would appear to be obscuring of responsibility of parties involved. In the Non-EU version, it is stated in the preamble:

PP_Section Preamble: "*If You provide us with personal information about someone else, You confirm that they are aware that You have provided their information and that they consent to our use of their information according to our Privacy Policy*".

There is the fact that one of the permissions associated with this app is access to the address book. This app comes pre-installed on some Android phones (Jonnalagadda, 2016), sometimes as the default dialling app. Accordingly, it is not necessarily true that a user will explicitly provide personal information of others. Glaringly, this onerous burden is omitted from the EEA-Switzerland version.

5.3.3 Sincerity of the Privacy Policy Statement

To test this validity claim requires checking the correspondence between an utterance and the speaker's intention. Sincerity must be inferred because intentions typically cannot be directly observed. This can be discerned by identifying discrepancies between what the speaker says, how the speaker says it and what the speaker does. The use of rhetorical devices such as metaphors can also be used to determine the sincerity of a discourse (Cukier & Eagen, 2003). Distortion of this validity claim will result in false assurance. The opening line of the app's policy states:

PP_Section Preamble: "*Truecaller is firmly committed to the security and protection of personal information of our Users and their contacts*".

By stating a commitment to ensuring privacy and security of a user's data from the onset, it would not be unreasonable for users to assume that every effort would be made in securing their data. Excerpts in Table 2 seemingly belie this.

Truecaller could ensure that data transfers are made to countries sharing the same level of protection offered by e.g. where the data was collected. Sincerity is also the quality of being open and truthful. In comparing both sets of policies, The EEA-Swiss version demonstrates this characteristic. There is an effort to be honest and about the nature of their business. This openness is missing from the Non-EU/rest-of-the-world version.

Additionally the use of rhetorical devices, such as metaphors, have been used in analysing the sincerity of statements. Metaphors can be used by people to comprehend new and unknown things. They can, however, also be used to mislead, sometimes deliberately, about the connections that

Table 2: Comparing two versions of the privacy policy of Truecaller to illustrate lack of sincerity

Rest of the World	**EEA and Switzerland**
In order to provide the Services, Truecaller will transfer, process and store personal information in a number of countries, including but not limited to India, and may also use cloud based services for this purpose. Truecaller may also subcontract storage or procession of Your information to third parties located in countries other than Your home country. Information collected within one country may, for example, be transferred to and processed in another country, which may not provide the same level of protection for personal data as the country in which it was collected.	The Truecaller services require by their very nature that Your personal information will be transferred to other Users across the globe. Truecaller may also use cloud based services and subcontract storage or processing of Your information to third parties located in countries other than Your home country in order to provide the Services, including e.g. the USA. Information collected within the Europe may, for example, be transferred to and processed in a country outside of Europe, which may not provide the same level of protection for personal data as within Europe.

they are being used in explaining (Fornaciari, 2014). Labour-is-a-resource is a metaphor central to capitalism (Wyatt, 2004). In the Truecaller privacy policy, the word “collect" was used, often in the phrase “collect, store and use ...". For example, in PP_Section 1.4, it is stated that “Truecaller may collect, store and use the list of identifiers associated with said services ...". There is a practice of employing the words like “harvest" and “use" as metaphors to transform data into tangible things. The transforming of data into a resource could possibly be seen in a similar light.

Computer terms are also rooted in metaphors (Lindh, 2016). Metaphors are often used to make technology comprehensible to non-specialists. While they can be used to help people to comprehend new concepts, they can also be misleading. Microsoft made use of metaphors such as “windows" and “menus" to make computing more accessible (Wyatt, 2004). Similarly, other references from the physical world and people’s experiences have been used in the world of IT, such as “cookies", “beacons", “servers", [search] “engine" and [IP] “address".

There is also connotative word-use in the policy with the word “share". The act of sharing, with the seemingly innocent suggestion of a joint, co-operative use of user’s data with known consent, belie the transactional or commercial aspect of the act. There is an attempt to underplay the economic focus. An excerpt from PP_Section 3 reads:

PP_Section 3: *"Truecaller may also share personal information with third party advertisers, agencies and networks. Such third parties may use this information for analytical and marketing purposes e.g. to provide measurement services and targeted ads and for improvement of products and services ...".*

Additionally, qualifiers are rhetorical devices sometimes used deliberately to introduce ambiguity in text. This is in order to mislead or withhold information or to water-down claims, but just enough to fulfil legal demands (Day, 1999). The word "may" is one such example, and it is used often in the policy document such as in PP_Section 1.2 in which was stated: "Truecaller may collect some of this information automatically through use of cookies ...", in PP_Section 2.2: "We may come to share such data with third parties." or in PP_Section 3: "Truecaller may also share personal information with third party advertisers, agencies and networks."

5.3.4 Comprehensibility of the Privacy Policy Statement

Comprehensibility, also known as clarity, is the quality of text being easy to understand. People in the technology and scientific fields are said to use jargon for obfuscation, rather than aiding understanding (Cukier et al., 2004). The indicators for a lack of comprehensibility include information overload, a level of detail that may be too burdensome for the reader and, the excessive use of language that a user may not be familiar with, as shown by some of the responses given by interviewee (earlier in Section 5.1) where the issue of technical competency was raised with interviewees.

The policy made use of technical terms and acronyms, of which only one was defined. A few of the terms are listed in Table 3. A hyperlink was provided in the privacy policy document that led to a separate "Cookie Policy" document where only the term 'cookie' was defined. Other terms used (e.g. web beacons, flash, HTML 5) were left unexplained either in the main policy statement, or in the linked cookie policy statement.

6 DISCUSSION

The intent of critical research is one which challenges accepted realities and seeks to promote resistance. Challenging reality and fostering resistance is done by identifying situations of power (which often are insidious and pervasive) and identifying those whom are dominated, to emancipate them by empowering them (Stahl, 2008). This definition is a classic example of the state of play with context-aware technologies. Long gone are the days in which the placement of cookies, on immobile computers, caused feelings of unease amongst desktop users. There is an attempt to develop an acceptance to the fact that one carries around what are essentially bugging devices, paid for by one's self. No longer can these devices be completely switched off. Consumers have come to accept the move from removable batteries to fused units based on explanations on aesthetics given by manufacturers. Apps are increasingly being preloaded unto smartphones with users unable to uninstall, or in some cases disable, the apps should they wish to. These new norms are being actively promoted by manufacturers of these technologies.

https://doi.org/10.18489/sacj.v31i2.694

Table 3: Unexplained technical terms in privacy policy of Truecaller to illustrate lack of comprehensibility

Section	Technical Term
1.2	Geo-location IP address Operating system IMSI Device log and event information Meta data Search engine Servers Cookies
1.4	Safety algorithm
2.1	Social graph algorithm Third party API
3	Bug testing
9	Web beacons Flash cookies HTML 5 cookies Pixel tags identifiers

Creators of modern, ubiquitous technologies often rely on inscrutable privacy policy documents to inform and confirm consent from the user on how their data will be used, stored and distributed. Additionally, the words of notable individuals have been shown not to be neutral forms of speech, but often are modes of persuasion which potentially could shape how consumers view these technological constructs. As communicative acts both of the policies and statements can and must be examined for their truth content, legitimacy, clarity and sincerity of motives.

The introduction of the new EU privacy-protection law demonstrates the ability of these manufacturers to be held accountable. It has been noted that Mr Zuckerberg has declined to accept invitations to attend a hearing with European legislators in a manner similar to his appearance in the United States Senate. Furthermore, the comparison of both versions of the privacy policy statement suggest privacy violation by design. There is no reason for the same policy not to be applicable the world over. Consumers should not be given the onerous task of tracking changes to these documents, which have been shown to be needlessly long, legalistic and vague, simply because their location is not protected by laws.

Truecaller is but one of many apps available for download, or pre-installed on phones. Similarly, Mr Zuckerberg is but only one of a number of influential decision makers of Information Technologies. Apps are but one component of the technological ecosystem which makes up context-aware computing, the foundation upon which the future of ubiquitous computing is being built. While the documentation of one app and the words of one CEO are being critically analysed, there is no intention to demonise either company. There is, however, an attempt to draw attention to the rampant data gathering

of which there is likely little or no informed consent. The exercise demonstrated also that there is justification to concerns raised by consumers of these technologies.

7 CONCLUSION

This study attempted to illustrate the increasing difficulty of users of context-aware technologies to manage and understand their privacy rights and privacy violations. To do so, the authors analysed the privacy policies of Truecaller, a popular caller ID service app, and the speech of Facebook's CEO using Critical Discourse Analysis (CDA) and Habermas' Theory of Communicative Action. In addition, twenty-five context-aware technology users from Nigeria were interviewed to obtain a better understanding of their privacy concerns.

By analysing and thematising interview responses, and reviewing a sample policy document, it was found that the privacy policy under review did not promote communication that was free from distortion, leading to alienated consumers. The further analysis of the Senate hearing speech by Facebook's CEO had the potential to provide false assurances to users regarding, for example, the control they have over their data as well as the visibility of their data. Whilst some components of a context-aware eco-system (for example, apps) are free, the devices upon which they run, and the connectivity required, typically are paid for by consumers. Consumers should be empowered to actively engage with the documents, truly inform themselves of their contents and implications of use and be encouraged to seek better alternatives if necessary.

Further work should be undertaken to critically analyse different public discourses on context-aware technologies for comparison analysis. Particularly, further research should especially be undertaken in Africa. Africa is a region in which the growth and use of these technologies is one of the fastest worldwide. It is also a region with ever-growing dependence on these technologies as a means of circumventing bad or failing infrastructure that characterise emerging economies. More importantly, however, it is a region with lagging privacy-enhancing legislation. There is therefore an even greater need to protect consumers from rampant data gathering.

References

Albright, J. (2018). The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle. https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747. [Online; accessed November 2018].

Analytica, C. (2018). https://cambridgeanalytica.org/. [Online; accessed April 2018]. Cambridge Analytica.

Andjelkovic, M. (2010). The Future is Mobile: Why Developing Country Entrepreneurs Can Drive Internet Innovation. *SAIS Review of International Affairs*, *30*(2), 121–133.

Baarslag, T., Alan, A. T., Gomer, R. C., Liccardi, I., Mareiros, H., Gerding, E. H., & Schraefel, M. C. (2016). Negotiation as an Interaction Mechanism for Deciding App Permissions. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16), San Jose, California, USA, May 07 — 12*. https://doi.org/10.1145/2851581.2892340

Balebako, R., Schaub, F., Adjerid, I., Acquisti, A., & Cranor, L. (2015). The Impact of Timing on the Salience of Smartphone App Privacy Notices. In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM '15), Colorado, USA, October 12*. https://doi.org/10.1145/2808117.2808119

Barrett, A. A., & Matthee, M. (2018). A Critical Analysis of Informed Use of Context-Aware Technologies. In *SAICSIT '18, Port Elizabeth, South Africa, 26 – 28 September*.

Bartholome, W. G. (1989). A New Understanding of Consent in Pediatric Practice: Consent, Parental Permission, and Child Assent. *Pediatric Annals*, *18*(4), 262–265. https://doi.org/10.1016/s0140-6736(02)11338-9

Beardsley, E., Jefford, M., & Mileshkin, L. (2007). Longer Consent Forms for Clinical Trials Compromise Patient Understanding: So Why are they Lengthening? *Journal of Clinical Oncology*, *25*(9), 13–14. https://doi.org/10.1200/jco.2006.10.3341

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International Differences in Information Privacy Concerns: A Global Survey of Information. *The Information Society*, *20*(5), 313–324. https://doi.org/10.1080/01972240490507956

Blanke, J. M. (2005). 'Robust Notice' and 'Informed Consent': The Keys to Successful Spyware Legislation. *Columbia Science and Technology Law Review*, *7*(2), 2–26.

Bogost, I. (2018). My Cow Game Extracted Your Facebook Data. https://www.theatlantic.com/technology/archive/2018/03/my-cow-game-extracted-your-facebook-data/556214/. [Online; accessed November 2018].

Boritz, E., & No, W. G. (2009). A Gap in Perceived Importance of Privacy Policies between Individuals and Companies. In *Proceedings of the 2009 World Congress on Privacy, Security, Trust and the Management of e-Business, New Brunswick, Canada, August 25 — 27*. https://doi.org/10.1109/congress.2009.32

Brummett, B. (2010). *Techniques of Close Reading*. SAGE Publishing, Los Angeles.

Cadwalladr, C. (2018). Cambridge Analytica's Ruthless Bid to Sway the Vote in Nigeria. https://www.theguardian.com/uk-news/2018/mar/21/cambridge-analyticas-ruthless-bid-to-sway-the-vote-in-Nigeria. [Online; accessed April 2018].

Center, F. H. (2018a). How Do I Report a Child Under the Age of 13 on Facebook? https://www.facebook.com/help/157793540954833. [Online; accessed November 2018]. Facebook Help Center.

Center, F. H. (2018b). Who Can See My Facebook Profile Picture and Cover Photo? https://www.facebook.com/help/193629617349922?helpref=uf_permalink. [Online; accessed May 2018]. Facebook Help Center.

Commission, E. (2018). 2018 Reform of EU Data Protection Rules. https://ec.europa.eu/commission/priorities/justice-and-fundament-rights/data-protection-rules_en/. [Online; accessed May 2018]. European Commission.

Confessore, N. (2018). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. [Online; accessed April 2018]. New York Times.

Crabtree, J. (2018). Here's how Cambridge Analytica Played a Dominant Role in Kenya's Chaotic 2017 Elections. https://cnbc.com/2018/-3/23/cambridge-analytica-and-its-role-in-kenya-2017-elections.html. [Online; accessed May 2018]. CNBC.

Cranor, L. F. (2012). Necessary but not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. *Journal on Telecommunications & High Technology Law*, *10*(2), 273–307.

Cukier, W., Bauer, R., & Middleton, C. (2004). Applying Habermas' Validity Claims as a Standard for Critical Discourse Analysis. In *Information Systems Research* (Vol. 143, pp. 233–258). IFIP International Federation for Information Processing. https://doi.org/10.1007/1-4020-8095-6_14

Cukier, W., & Eagen, W. (2003). Habermas's "Ideal Speech Act": A Standard for Critical Discourse Analysis. In *2nd European Conference on Research Methodology for Business and Management* (pp. 101–112).

Cukier, W., Ngwenyama, O., Bauer, R., & Middleton, C. (2009). A Critical Analysis of Media Discourse on Information Technology: Preliminary Results of a Proposed Method for Critical Discourse Analysis. *Information Systems Journal*, *19*(2), 175–196. https://doi.org/10.1111/j.1365-2575.2008.00296.x

Cukier, W., Ryan, P. M., & Fornssler, B. (2009). The Rhetoric of the "Information Highway" in the Media 1992-2008: Was the Hype Actually Trumped by the Reality? In *IEEE Toronto International Conference Science and Technology for Humanity (TIC-STH), Toronto, Ontario, September 26 – 27* (pp. 618–623). https://doi.org/10.1109/tic-sth.2009.5444426

Cullen, R. (2009). Culture, Identity and Information Privacy in the Age of Digital Government. *Online Information Review*, *33*(3), 405–421. https://doi.org/10.1108/14684520910969871

Day, N. R. (1999). *Advertising: Information or Manipulation?* Enslow Publishers, Inc., New Jersey, U.S.A.

Facebook. (2018). www.facebook.com. [Online; accessed April 2018]. Facebook.

Fairclough, N. (1989). *Language and Power*. https://doi.org/10.1017/s0047404500016122

Fairclough, N. (2013). *Critical Discourse Analysis: The Critical Study of Language* (2nd ed.). https://doi.org/10.4324/9781315834368

Fitzgerald, D. W., Marotte, C., Verdier, R. I., Johnson, W. D., & Pape, J. W. (2002). Comprehension During Informed Consent in a Less-Developed Country. *The Lancet*, *360*(9342), 1301–1302. https://doi.org/10.1016/s0140-6736(02)11338-9

Fitzpatrick, T. (2002). Critical Theory, Information Society and Surveillance Technologies. *Information, Communication & Society*, *5*(3), 357–378.

Fjortoft, M. R. (2013). The Critical Element of Critical Discourse Analysis. *SYNAPS*, *28*, 67–75. https://doi.org/10.1080/17405904.2013.845373

Fornaciari, F. (2014). Pricey Privacy: Framing the Economy of Information in the Digital Age. *First Monday*, *19*(12), –. https://doi.org/10.5210/fm.v19i12.5008

Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for Characterizing the Form of Security Policies. *Journal of Strategic Information Systems*, *19*(4), 281–296. https://doi.org/10.1016/j.jsis.2010.10.002

Goh, J. P. L. (2015). Privacy, Security, and Wearable Technology. *Landslide*, *8*(2), 1–8.

Golle, P. (2010). Revisiting the Uniqueness of Simple Demographics in the US Population. In *WPES '06, Alexandria, Virginia, USA, October 20*. https://doi.org/10.1145/1179601.1179615

Habermas, J. (1976). What is Universal Pragmatics? In T. McCarthy (Ed.), *Communication and the Evolution of Society* (pp. 1–68). Boston, U.S.A.: Beacon Press.

Habermas, J. (1984). *The Theory of Communicative Action: Reason and the Rationalisation of Society (Vol. I)*. https://doi.org/10.2307/1955926

Hirschheim, R. A. (1992). Information Systems Epistemology: An Historical Perspective. In R. Galliers (Ed.), *Information Systems Research: Issues, Methods and Practical Guidelines* (pp. 28–60). London: Blackwell Scientific Publications.

Ho, D. G. E. (2013). Interviews. In C. A. Chapelle (Ed.), *The Encyclopedia of Applied Linguistics* (pp. 2–5). https://doi.org/10.1108/rr-08-2013-0204

Hoffmann, A. L., Proferes, N., & Zimmer, M. (2018). 'Making the World More Open and Connected': Mark Zuckerberg and the Discursive Construction of Facebook and Its Users. *New Media & Society*, *20*(1), 199–218. https://doi.org/10.1177/1461444816660784

Howarth, D. (2000). *Discourse*. https://doi.org/10.1177/03058298010300030928

Huckin, T. N. (1997). Critical Discourse Analysis. In T. Miller (Ed.), *Functional Approaches to Written Text* (pp. 78–92). Washington, CD: US Department of State.

Janson, M., & Cecez-Kecmanovic, D. (2005). Making Sense of e-Ccommerce as Social Action. *Information Technology & People*, *18*(4), 311–342. https://doi.org/10.1108/09593840510633301

Jayawardena, S. (2015). Metaphor as Weapon. http://harvardpolitics.com/books-arts/metaphor-weapon. [Online; accessed August 2018]. Harvard Political Review.

Jensen, C., & Potts, C. (2004). Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. In *CHI 2004, Vienna, Austria, April 24—29* (pp. 471–478). https://doi.org/10.1145/985692.985752

Johnson, J. (1991). Habermas on Strategic and Communicative Action. *Political Theory*, *19*(2), 181–201. https://doi.org/10.1177/0090591791019002003

Jonnalagadda, H. (2016). Huawei Phones to come with Truecaller Pre-installed, Starting with the Honor 8. https://www.androidcentral.com/huawei-phones-come-truecaller-pre-installed-starting-honor-8. [Online; accessed May 2018]. Android Central.

Kelley, P. G., Cesca, L., Bresee, J., & Cranor, L. F. (2010). Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10), Atlanta, Georgia, April 10 – 15* (pp. 1573–1582). https://doi.org/10.1145/1753326.1753561

Klein, H. K., & Huynh, M. Q. (2004). The Critical Social Theory of Jürgen Habermas and its Implications for IS Research. In J. Mingers & L. Willcocks (Eds.), *Social Theory and Philosophy for Information Systems* (pp. 157–237). John Wiley & Sons, Ltd., U.K.

Kok, K. F. (2018). Truecaller Appoints Zakaria Hersi as Director of Partnerships in Africa! https://truecaller.blog/2018/02/27/truecaller-appoints-zakaria-hersi-as-director-of-partnerships-in-africa/. [Online; accessed May 2018]. Truecaller.

Koller, V. (2004). *Metaphor and Gender in Business Media Discourse: A Critical Cognitive Study* (1st ed.). https://doi.org/10.1558/genl.v3i1.127

Krasnova, H., Eling, N., Schneider, O., Wenninger, H., Widjaja, T., & Buxmann, P. (2013). Does This App Ask For Too Much Data? The Role of Privacy Perceptions in User Behavior Towards Facebook Applications and Permission Dialogs. In *Proceeding of the 21st European Conference on Information Systems (ECIS 2013), Utrecht, Netherlands, 6 -– 8 June*.

Lakoff, G., & Johnson, M. (1980). Conceptual Metaphor in Everyday Language. *The Journal of Philosophy*, *77*(8), 453–486. https://doi.org/10.2307/2025464

Lindh, M. (2016). As a Utility: Metaphors of Information Technologies. *Human IT*, *13*(2), 47–80.

Luger, E., Moran, S., & Rodden, T. (2013). Consent for All: Revealing the Hidden Complexity of Terms and Conditions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'13), Paris, France, April 27 – May 02*. https://doi.org/10.1145/2470654.2481371

Luger, E., & Rodden, T. (2013). Terms of Agreement: Rethinking Consent for Pervasive Computing. *Interacting with Computers*, *25*(3), 229–241. https://doi.org/10.1093/iwc/iws017

Lynch, G., Willis, J., & Cheeseman, N. (2018). Cambridge Analytica's Role in African Elections was Real but Overstated. https://qz.com/1242223/cambridge-analytica-facebook-had-little-impact-on-kenya-nigeria-elections/. [Online; accessed April 2018].

Lyytinen, K. J. (1985). The Critical Theory of Jurgen Habermas as a Basis for a Theory of Information Systems. In E. Mumford, R. Hirschheim, G. Fitzgerald, & A. T. Wood-Harper (Eds.), *Research Methods in Information Systems* (pp. 219–236). New York, NY: Elsevier Publishing.

Makulilo, A. B. (2016). The Context of Data Privacy in Africa. In A. B. Makulilo (Ed.), *African Data Privacy Laws* (pp. 3–25). https://doi.org/10.1007/978-3-319-47317-8_1

McDonald, A. M., & Cranor, L. F. (2008). The Cost of Reading Privacy Policies. *A Journal of Law and Policy for the Information Society*, *4*(3), 543–568.

Meinert, D. B., Peterson, D. K., Criswell, J. R., & Martin D, C. (2006). Would Regulation of Web Site Privacy Policy Statement Increase Consumer Trust? *Informing Science Journal*, *9*(15), 123–142. https://doi.org/10.28945/2952

Milne, G. R., Culnan, M. J., & Greene, H. (2006). A Longitudinal Assessment of Online Privacy Notice Readability. *Journal of Public Policy and Marketing*, *25*(23), 238–249. https://doi.org/10.1509/jppm.25.2.238

Murray, P. M. (1990). The History of Informed Consent. *The Iowa Orthopaedic Journal*, *10*, 104–109.

Myers, M. D., & Klein, H. K. (2011). A Set of Principles for Conducting Critical Research in Information Systems. *MIS Quarterly*, *35*(1), 17–36. https://doi.org/10.2307/23043487

Myers, M. D., & Newman, M. (2007). The Qualitative Interview in IS Research: Examining the Craft. *Information and Organization*, *17*, 2–36. https://doi.org/10.1016/j.infoandorg.2006.11.001

Naidoo, A. (2010). The UmNyango Project: Using SMS for Political Participation in Rural KwaZulu Natal. In S. Ekine (Ed.), *SMS Uprising: Mobile Phone Activism in Africa* (pp. 71–85). https://doi.org/10.1080/15405702.2011.562106

News, C. 4. (2018). Cambridge Analytica Uncovered: Secret Filming Reveals Election Tricks. https://www.youtube.com/watch?v=mpbeOCKZFfQ. [Online; accessed May 2018]. Channel 4 News.

Nwankwo, I. S. (2016). Information Privacy in Nigeria. In A. B. Makulilo (Ed.), *African Data Privacy Laws* (pp. 45–76). https://doi.org/10.1007/978-3-319-47317-8_3

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymizationt. *UCLA Law Review*, *57*(6), 1701–1777.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research*, *2*(1), 1–28. https://doi.org/10.1287/isre.2.1.1

Ponelis, S. R., & Holmner, M. A. (2015). ICT in Africa: Enabling a Better Life for All (Editorial). *Information Technology for Development*, *21*(1), 1–11. https://doi.org/10.1080/02681102.2014.985521

Ponterotto, J. G. (2005). Qualitative Research in Counseling Psychology: A Primer on Research Paradigms and Philosophy of Science. *Journal of Counseling Psychology*, *52*(2), 126–136. https://doi.org/10.1037/0022-0167.52.2.126

Post, T. W. (2018). Transcript of Zuckerberg's Appearance before House Committee. https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/transcript-of-zuckerbergs-appearance-before-house-committee/?utm_term=.c730d2115f56. [Online; accessed April 2018]. Washington Post.

Press, H. K. F. (2016). 3 Billion Phone Numbers and Identities Exposed by Mobile Apps, Investigation Finds. https://hongkongfp.com/2016/11/20/3-billion-phone-numbers-and-identities-are-being-exposed-by-mobile-apps-investigation-finds/. [Online; accessed April 2018]. Hong Kong Free Press.

Rashidi, N., & Souzandehfar, M. (2010). A Critical Discourse Analysis of the Debates Between Republicans and Democrats over the Continuation of War in Iraq. *Journal of Linguistic Intercultural Education*, *3*, 55–82.

Richardson, H., Tapia, A., & Kvasny, L. (2006). Introduction: Applying Critical Theory to the Study of ICT. *Social Science Computer Review*, *24*(3), 267–273.

Roztocki, N., & Weistroffer, H. R. (2008). Information Technology Investments in Emerging Economies. *Information Technology for Development*, *14*(1), 1–10. https://doi.org/10.1002/itdj.20084

Sane, I., & Traore, M. B. (2009). Mobile Phones in a Time of Modernity: The Quest for Increased Self-Sufficiency Among Women Fishmongers and Fish Processors in Dakar. In I. Busken & A. Webb (Eds.), *African Women and ICTs: Investigating Technology, Gender and Empowerment* (pp. 107–118). London, UK: Zed Books.

Sloan, R. H., & Warner, R. (2013). Beyond Notice and Choice: Privacy, Norms, and Consent. *Journal of High Technology Law*, *16*, 1–34. https://doi.org/10.2139/ssrn.2239099

Stahl, B. C. (2008). Empowerment Through ICT: A Critical Discourse Analysis of the Egyptian ICT Policy. In C. Avgerou, M. L. Smith, & P. van der Besselaar (Eds.), *Social Dimensions Of Information And Communication Technology Policy* (Vol. 282, pp. 161–177). IFIP International Federation for Information Processing. https://doi.org/10.1007/978-0-387-84822-8_11

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information Security Policies in the UK Healthcare Sector: A Critical Evaluation. *Information Systems Journal*, *22*, 77–94. https://doi.org/10.1111/j.1365-2575.2011.00378.x

Stahl, B. C., Tremblay, M. C., & LeRouge, C. M. (2011). Focus Groups and Critical Social IS Research: How the Choice of Method can Promote Emancipation of Respondents and Researchers. *European Journal of Information Systems*, *20*(1), 378–394. https://doi.org/10.1057/ejis.2011.21

Statista. (2019). Most Popular Social Networks Worldwide as of January 2019, Ranked by Number of Active Users (In Millions). https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/. [Online; accessed January 2019]. Statista.

Steijn, W. M. P., Scouten, A. P., & Vedder, A. H. (2016). Why Concern Regarding Privacy Differs: The Influence of Age and (Non-) Participation on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(1), 1–12. https://doi.org/10.5817/cp2016-1-3

Trauth, E. M., & Howcroft, D. (2006). Critical Empirical Research in IS: An Example of Gender and the IT Workforce. *International Technology & People*, *19*(3), 272–292. https://doi.org/10.1108/09593840610689859

Trauth, E. M., & Jessup, L. M. (2000). Understanding Computer-Mediated Discussions: Positivist and Interpretive Analyses of Group Support System Use. *MIS Quarterly*, *24*(1), 43–79. https://doi.org/10.2307/3250979

Truecaller. (2018a). https://www.truecaller.com. [Online; accessed May 2018]. Truecaller.

Truecaller. (2018b). Truecaller Privacy Policy. https://privacy.truecaller.com/privacy-policy. [Online; accessed May 2018]. Truecaller.

van Dijk, T. A. (1985). Introduction: Discourse Analysis as a New Cross-Discipline. In T. A. van Dijk (Ed.), *Handbook of Discourse Analysis* (Vol. 1, pp. 1–10). https://doi.org/10.1525/aa.1986.88.4.02a00760

van Dijk, T. A. (1986). *Racism in the Press*. Arnold.

van Dijk, T. A. (1995). Aims of Critical Discourse Analysis. *Japanese Discourse*, *1*, 17–27.

van Dijk, T. A. (2001). Critical Discourse Analysis. In D. Tannen, D. Schiffrin, & H. E. Hamilton (Eds.), *Handbook of Discourse Analysis* (pp. 352–371). https://doi.org/10.1111/b.9780631205968.2003.x

van Dijk, T. A. (2006). Discourse and Manipulation. *Discourse and Society*, *17*(2), 359–383. https://doi.org/10.1007/978-1-137-07299-3_9

Walsham, G. (1995). Interpretive Case Studies in IS Research: Nature and Method. *European Journal of Information Systems*, *4*(2), 74–81. https://doi.org/10.1057/ejis.1995.9

Watkins, J. O. T. A., Goudge, J., Gomez-Olive, F. X., & Griffiths, F. (2018). Mobile Phone Use Among Patients and Health Workers to Enhance Primary Healthcare: A Qualitative Study in Rural

South Africa. *Social Science & Medicine*, *198*, 139–147. https://doi.org/10.1016/j.socscimed.2018.01.011

Watson, S. L., & Watson, W. R. (2011). Critical Emancipatory, and Pluralistic Research for Education: A Review of Critical Systems Theory. *Journal of Thought*, *46*(3), 63–77. https://doi.org/10.2307/jthought.46.3-4.63

Weiser, M. (1991). The Computer for the 21st Century. *Scientific American*, *265*(3), 94–104. https://doi.org/10.1038/scientificamerican0991-94

Wodak, R. (1989). Introduction. In R. Wodak (Ed.), *Language, Power and ideology: Studies in Political Discourse* (pp. xii–xx). https://doi.org/10.1017/s0047404500016134

Wodak, R., & Meyer, M. (2009). Critical Discourse Analysis: History, Agenda, Theory, and Methodology. In R. Wodak & M. Meyer (Eds.), *Methods for Critical Discourse Analysis* (pp. 1–33). https://doi.org/10.1075/z.184.79dij

Wyatt, S. (2004). Danger! Metaphor at Work in Economics, Geophysiology, and the Internet. *Science, Technology & Human Values*, *29*(2), 242–261. https://doi.org/10.1177/0162243903261947

Zinkin, M. (1998). Habermas on Intelligibility. *The Southern Journal of Philosophy*, *36*, 453–472. https://doi.org/10.1111/j.2041-6962.1998.tb01765.x

Zukowski, T., & Brown, I. (2007). Examining the Influence of Demographic Factors on Internet Users' Information Privacy Concerns. In *Proceedings of the 2007 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists (SAICSIT 2007), Port Elizabeth, South Africa, October 2 – 3*. https://doi.org/10.1145/1292491.1292514