Journal of Information Technology Management

Print ISSN: 2008-5893

Online ISSN: 2423-5059

The Impact of Digital Government on Whistleblowing and Whistle-blower Protection: Explanatory Study

Yelkal Mulualem Walle

College of Computer Science and Information Technology, Sudan University of Science and Technology, Khartoum, Sudan. ORCID: 0000-0003-4861-2682. E-mail: yelkal.mulualem@uog.edu.et

Received January 15, 2020; Accepted March 25, 2020

Abstract

This paper focuses on the contribution of digital government (DGOV) to Whistleblowing (WB). While considerable efforts have been devoted to DGOV and WB separately, research work at the intersection of these two domains is very scarce; hence and a systematic DGOV for WB (DGOV4WB) research framework has yet to emerge. This paper aims to identify the potential issues in whistleblowing and explore how digital government has been used to address these issues. To this end, this paper uses explanatory case study research methodology and analyses four case studies of existing DGOV initiatives with explicit WB dimensions. The result of the cross-case analysis shows that DGOV4WB initiatives contribute to address goals of the different dimensions of whistleblowing. The most common WB problems addressed are: easily accessible reporting and response whistleblowing channels (Whistleblowing Procedure), easy and timely communication channel with top management (Whistleblowing Organizational culture), and anonymous and confidential communication platforms (Whistleblower Protection). In addition, based on the analysis of the case studies, all the initiatives are classified as either engagement or contextualization stage of the digital government evolution model.

Keywords: Digital Government; E-government, Whistleblowing; Whistleblower Protection; Digital Technology.

DOI: 10.22059/jitm.2019.291003.2409

1. Introduction

Many organizations around the world are vulnerable to unethical behaviors such as fraud, bribery and abuse, negligence, bullying, harassment and that may cause financial and reputational harm to organizations if left unobserved and undetected (GFIR, 2018). The Annual Global Fraud Survey shows that fraud cases in 2015/16 increased by 14 percent from that of 2012/13 (GFR, 2016). Researchers like Barkemeyer, Preussb and Lee (2015), Alleyne and Watkins (2017) suggest that by developing a proactive approach and by incorporating stakeholders in fostering an ethical workplace, an organization can significantly reduce financial liability and loss and preserve its strong corporate image on the marketplace. Global Fraud Study of the Associations of Certified Fraud Examiners (ACFE) states that the most common method of detecting fraud was through whistleblowers disclosure –about 39.1 percent of the (ACFE, 2016).

Different international organizations (OECD, 2016; TI, 2013) and researchers (Figg, 2000; Apaza & Chang, 2011; Banisar, 2011) indicate the importance of whistleblowing –disclosure of information by an employee or contractor alleging wilful misconduct by an individual or individuals within an organization (Near & Miceli, 1985) –in the fighting against fraudulent activities within the organization (EY, 2016, Devine & Maassarani, 2011). However, whistleblowing suffers from a wide range of problems including the use of anonymous and confidential reporting mechanism, monitoring of the whistleblowing process, and practices of confidential communication between different whistleblowing stakeholders including direct communication and training with all involved stakeholders (Apaza & Chang, 2011; Near & Miceli, 1985). This indicates that whistleblowers need strong legal protections to protect them from retaliation and enable them to report offences safely and freely (TI, 2013; Rothschild & Miethe, 1994).

To deal with some of the issues of the whistleblowers and whistleblowing, government and organizations around the world work intensively through developing comprehensive whistleblowing policies with the aim of providing accessible and reliable channels to report wrongdoing and to encourage whistleblowers to report wrongdoing internally; and to provide strong protection for whistleblowers from any types of retaliation within the organization (TI, 2013; Apaza & Chang, 2011). A key question for governments and organizations is how to make the whistleblowing program effective. As per (TI-NL, 2017), effective whistleblowing program needs to i) provide a secured whistleblowing channel which can be accessible by 7/24/365; ii) promote whistleblowing programs; iii) build free and transparent whistleblowing organizational culture and iv) protect whistleblowers in their administration.

In order to address some of the whistleblowing and government challenges stated above, governments and organizations have started to develop and use different types of whistleblowing programs strategically relying on the use of digital technologies. Underpinning such responses is an assumption that digital government could help in providing secured whistleblowing reporting

channels which could substantially transform the whistleblowing process by reducing victimization (retaliation) for whistleblowers. This assumption is based on the basic features of digital government developed by international organizations (e.g. OECD, 2003; TI, 2016; Accenture, 2015; Corydon, Ganesan & Lundqvist, 2016), and researchers (e.g., Kraemer & King, 2006; Hoetker, 2002; Bertot, Jaeger & Grimes, 2010; Intuit, 2017). Digital government enables more effective and responsive delivery of public services, increases citizen participation, allows submitting reports anonymously (Emura et al., 2017), and provides greater access to information about whistleblowing laws, cases and decisions.

Increasingly, the use of digital technology to transform public administration organizations and their relationships with citizens, businesses and each other (i.e., digital government) (OECD, 2019) is recognized as a tool to help reinvent the public sector by transforming internal processes and systems of governments as well as their external ties with citizens and businesses (Fang, 2002; Seifert & Chung, 2008). This allows governments to provide services that meet the evolving expectations of citizens and businesses, and to become more accountable and transparent at global and national levels. It also helps provide secure online communications (Emura et al., 2017) that can have an impact on the protection of sources and whistleblowers. By applying the concept of Digital Government to whistleblowing domain (DGOV4WB), we redefine DGOV4WB as the use of digital technology to foster governance of Whistleblowing Process and Whistleblowing Protection. DGOV4WB involves the use of digital technologies to transform the public administration (and its relations with citizens and business) and to increase broad public sector modernizations (greater openness, transparency, engagement with and trust in government) while making possible citizens'/ employees' participation in exposing alleged wilful misconduct by an individual or individuals within an organization and protection of the whistleblowers from any form of retaliation. While considerable efforts have been devoted to studying DGOV and whistleblowing separately as depicted in Table 9, research work at the intersection of these domains is very scarce. Only a very few scholars investigated the possible contribution of technologies in whistleblowing and its side effects (Lam & Harcourt, 2019; Brevini, 2017; heemsbergen, 2013); therefore, a systematic DGOV4WB research framework is yet to emerge.

This article explores the contribution of digital government for whistleblowing and whistleblower protection. In particular, we identify potential issues in whistleblowing and explore how digital government has been used to address these issues. To achieve these targets, we analyse four DGOV4WB case studies that contain digital government initiatives with explicit whistleblowing objectives. Following explanatory case study research methodology, we characterize each of the case studies based on their background, problem/objective, types of DGOV solutions applied to the whistleblowing problems and finally make problem and solution analyses.

2. Literature Review

1.1. Whistleblower and Whistleblowing

The word whistleblowing emanates from sporting events in which a referee blows the whistle to stop an unethical or foul play (Qusqas & Kleiner, 2001). Near and Miceli (1985) define whistleblowing as "the disclosure by organization members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action". It has been regarded as a means of preserving honesty by expressing one's truth about what is right and what is wrong in an organization. This is also used as a strategy for asserting rights, protecting interests, influencing justice, and righting wrongs (Berry, 2004).

A whistleblower can be an employee, suppliers, contractors, clients or any individual who somehow becomes aware of illegal or unethical activities taking place in a business / organization, either through witnessing the behavior or reporting about it (Alleyne & Watkins, 2017; Courtland & Cohen, 2017). Rosenbloom (2003) indicate that as insiders, whistleblowers are the source of valuable information that neither the government nor the public can get from the oversight systems.

Whistleblowers can disclose the misconducts in an organization either internally or externally (Near & Miceli, 1985). Research suggests that almost all whistleblowers first attempt to expose wrongdoing via internal channels before using external channels (Near & Miceli, 1995). However, an employee's decision to report individual or organizational misconduct is a complex phenomenon that is based upon organizational, situational or personal factors (Miceli et al., 1987). Transparency International (2013) defines the whistleblowing domain in three dimensions: i) whistleblowing procedure; ii) whistleblowing organizational culture; and iii) whistleblower protection.

1.1.1. Whistleblowing Procedure

Whistleblowing procedures are formulated in an organization to encourage disclosure in good faith of unlawful incidents. These procedures can provide the utmost confidentiality and effective protection from any harassment or reprisals arising from whistleblowing (TI, 2013; Miceli et al., 1987). These procedures are a key element for an organizational integrity and facilitate combating practices that might damage its activities and reputation (Courtland & Cohen, 2017). According to TI (2013), the effectiveness of the internal reporting procedures includes several mechanisms. The reporting mechanisms should ensure the accessibility of whistleblowing reporting channels while the response mechanisms should put in place clear procedures to ensure thorough, timely and independent investigations of reports of misconduct. Moreover, there should be mechanisms for monitoring the investigation result –the key statistics on whistleblowing cases collected and reviewed on a regular basis (TI, 2013).

1.1.2. Whistleblowing Organizational Culture

Organisation's corporate culture determines to what extent potential whistleblowers feel safe and comfortable to report wrongdoing internally (Lachman, 2008). This has a direct influence on how whistleblowers react toward observed wrongdoings. The goodwill for internal reporting of wrongdoing is embedded in the corporate culture (Berry, 2004). Transparency International (2013) identifies two main factors that contribute to whistleblowing organizational culture. The first is the commitment of an organization's top management towards the whistleblowing –direct involvement of top officials and their effective engagement in the whistleblowing process. The second factor concerns the communication from the upper management –clear support of the organization's higher officials for its employees and customers to expose misconduct through the existing whistleblowing frameworks (TI, 2013).

1.1.3. Whistleblower protection

Whistleblowing has immense social value, but it usually comes at a very high professional or personal cost (OECD, 2012; TI, 2013). According to Berry (2004) those who report wrongdoings may be subject to retaliation, such as intimidation, harassment, dismissal or violence by their fellow colleagues or superiors. OECD (2016) on its convention on effective whistleblower protection states that "Whistleblower protection is integral to fostering transparency and promoting integrity". Encouraging and facilitating whistleblowing, in particular by providing effective legal protection and clear guidance on reporting procedures, can also help authorities monitor compliance and detect violations of anti-corruption laws (OECD, 2012). TI (2016) and (OECD, 2015) mentions the level of protection given to people reporting wrongdoing internally: level of anonymity, anti-retaliation measures, civil and criminal liability, and burden of proof.

1.2 Digital Government and Whistleblowing

The advent of digital technologies, from cloud computing to mobile to analytics, is fundamentally transforming both public and private sector organizations' operations (Deloitte, 2015) and it has been an important enabling tool for reforms (Katsonis & Botros, 2015). The pursuit of efficiency gains, effective delivery of program outcomes, improving services, increasing accountability and transparency, and facilitating consultation and engagement had been the main drivers of technology use in government (OECD, 2003). OECD (2016) defines Digital Government as "digital technologies and user preference integrated in the design and receipt of services and broad public sector reform which is the integral part of government's modernization strategies to create public value" (OECD, 2016). Digital Government has been considered as a driving force of administrative reforms around the world (Morgeson & Mithas, 2009; Scholl, 2006). It enables governments to create more public value and public sector transformation –greater accountability, transparency, engagement with and trust in government– by the integration of digital technologies and user preferences in service design and delivery of

direct personal services as well as in shaping public policy outcomes (Katsonis & Botros, 2015; OECD, 2016; Deloitte, 2015, Tweedie, 2010).

The technology landscape involved in whistleblowing has changed drastically over time. At its most basic level, writing and verbal speech could be used to convey information about wrongdoings. The printing press and radio eased the spread of news. Copiers allowed whistleblowers to copy documents and give them to press. Computers and the Internet make it easy to disseminate information and upload leaked documents. Easy uploading means the rise of leaking, i.e., mass release of millions of documents the whistleblower might not have even read. In the current digital world, there are a growing number of web publishing organizations dedicated to free online whistleblowing services such as WikiLeaks or afriLeaks. Social media sites, such as Facebook or Twitter, are also being used to facilitate the disclosure of organizational wrongdoing, although they are not specifically designed for whistle-blowing.

Digital technologies also pose challenges to the protection of whistleblowers and sources (TI, 2013). Vast amount of data is generated from internet connection records to communications data. The advancement of digital technology has resulted in increased data collection, storage, analysis and discovery capabilities as well as information use and disclosure of information (Katsonis & Botros, 2015). Integrating digital technology through transformation and modernization activities in the public sector, however, is a challenge. It means that technological interventions alone are not sufficient to protect whistleblowers, and whistleblower protection policies for digital technologies use in all areas and at all levels of the administration - digital government for whistleblowing and whistleblower protection - is required.

A few scholars investigated the possible contribution of technologies in whistleblowing and its side effects. Brevini (2017) has explored the rise and the legacy of the disclosure platform and whistle-blowing website WikiLeaks through the discussion of four scholars analyzing WikiLeaks's impact on the world. He explores the effect of WikiLeaks has had on traditional journalism which has to power in the realm of the balance between openness and secrecy in domestic and international politics; He also used WikiLeaks as a case study to understand the relationship between media and social movements and to study the platform's ethics and the legal consequences of its operations (Brevini, 2017). In his interview with interview with Suelette Dreyfus, Luke Heemsbergen (2013) explores the relationship between whistleblowing and digital technologies. He indicates that the technology involved in whistleblowing is more than just the technology used in whistleblowing systems, it's also online publishing technology, security and privacy technologies and, of course, mass eavesdropping technologies (Heemsbergen, 2013).

Despite the surge in online whistle-blowing systems implementations across the world and as shown in Table 9 (Scopus databases search publications result as of June 2019), the contribution

of digital government to whistleblowing domain is scarce. Based on the rationale above, the study in this paper focus on the identifying the possible contribution of digital government on whistleblowing and whistleblowing domain. In particular, we identify potential issues in whistleblowing and explore how digital government has been used to address these issues. This has been achieved by considering whistleblowing domain as problem domain and digital government as solution domain.

4. Conceptual Framework

The conceptual framework of DGOV4WB is developed by explaining both digital government (DGOV) domain and whistleblowing (WB) domain independently based on their definition and comprising elements. Near and Miceli defines whistleblowing as "the disclosure by organization members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action" (Near & Miceli, 1985). Whistleblowers enhance corporate and government accountability by being the first line of defense against wrongdoing, and it is recognized as one of the most effective and powerful tools for protecting the public interest (OECD, 2016).

According to Transparency International (2013), whistleblowing domain underpinned by three dimensions: 1) whistleblower protection, 2) whistleblowing procedure, and 3) whistleblowing organizational culture (TI, 2013). Following the above dimensions, the whistleblowing domain finds solutions to global problems including frauds, corruptions and any unlawful activities within the organizations. Whistleblowing Domain dimensions and its elements depicted as shown in Table 1.

There are numerous definitions of digital government provided by different organizations (OECD, 2016; Accenture, 2015). For this study, we adopted the definition of digital government from OECD (2016) – "Digital Government is digital technologies and user preference integrated in the design and receipt of services and broad public sector reform which is the integral part of government's modernization strategies to create public value".

Table 1. Whistleblowing Domain dimensions and its elements (TI, 2013; Near & Miceli, 1995; OECD, 2012)

Dimensions		
Whistleblower Protection	Whistleblowing Procedure	Whistleblowing Organizational Culture
Anti-retaliation	Reporting mechanism	Communication
Anonymity and confidentiality	Response mechanism	Commitment from top managers
Burden of proof	Monitoring	
Criminal and Civil Liability		

According to OECD (2019), DGOV is underpinned by six dimensions of DGOV: 1) User-driven (i.e. focus on user needs and citizens' expectations); 2) Government as a platform (i.e.

Governments build supportive ecosystems - working together with the public to address common challenges); 3) Digital by design (i.e. rooting digital transformation within governments); 4) Data-driven (i.e. governments using data as a key strategic resources - uses data to predict needs, shape delivery, understand performance, and respond to change); 5) Pro-activeness (i.e. governments anticipating needs and delivery of services); and 6) Open by default (i.e. disclosing data in open formats - governments that are transparent and accountable). Following these dimensions cover the whole DGOV Solution space.

DGOV4WB –the use of digital technology to foster governance of Whistleblowing process and Whistleblowing protection. It is comprised of (see Figure 1) three primary domains namely Public Governance (GOV), Digital Technology (DT) and Whistleblowing (WB); and three secondary domains: i) Digital Government (DGOV) – intersection between public governance and digital technology; ii) Digital Technology for Whistleblowing (DT4WB) –intersection between Digital Technology for Whistleblowing; and iii) public Governance for Whistleblowing (GOV4WB) is the intersection of Governance and Whistleblowing. Figure 1 shows a mapping of three primary and three secondary domains contributing to DGOV4WB.

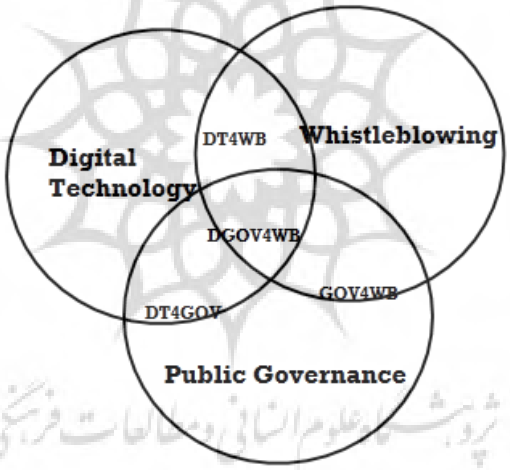

Figure 1. DGOV4WB comprising domains and its relationships

The relationships between the domains are based on the concept of customer service domain relation. According to customer service domain relation, one domain helps the other domain fulfil its goals. Considering the relationship between DT to WB and DT to GOV, Digital Technology is a service domain that helps to achieve the goal of Whistleblowing and Public Governance and they both are customer domain in this context. Whereas, governance is service domain in relation to whistleblowing. Based on the above definitions and list of dimensions the conceptual framework for DGOV4WB is shown in Figure 2.

The proposed approach aims to bridge the gap of the problem domain through the solution domains. The novelty of the framework emanates from the three characteristics – problem

domain, solution domain and mapping of WB. It shows the contribution of digital government in solving the issues/problems of the whistleblowing domain as discussed in the literature review. The mapping is necessary in order to provide a quick and efficient means for understanding the relationships between digital government solutions and whistleblowing problem.

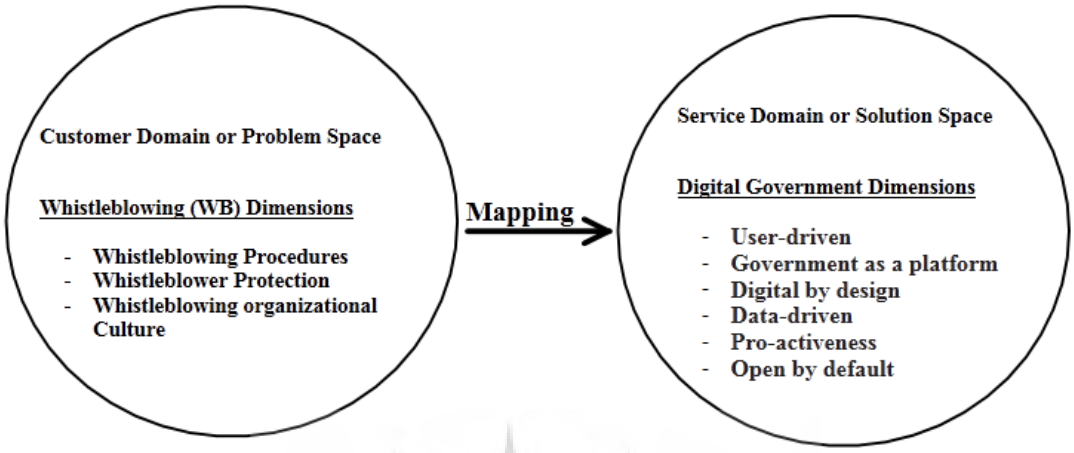

Figure 2. DGOV4WB Conceptual Framework

5. Methodology

The methodology used in this research paper is exploratory or formative research using the technique of formal qualitative research through multiple case studies using secondary data – digital government initiatives on whistleblowing and whistleblower protections. The researchers conducted an exploratory case study research to understand how the digital government contributes to solving the issues/problem of whistleblowing and whistleblower protection.

The case study was designed to be a preliminary investigation into various aspects of digital government use in whistleblowing. The researcher followed the following five steps to carry out the study: defining the assessment framework, defining the scope of the data collection, collecting and documenting case studies, analyzing case studies, and creating results. The assessment framework applies for this research paper is adopted from (Estevez, Janowski & Dzhusupova, 2014). To characterize each of the case studies (DGOV4WB initiatives), the assessment framework comprises four constructs - Background, Problem/Objective, Solution and Contribution. The assessment framework is depicted in Figure 3. Background is used to gather basic information about the initiative including the actors, launching place and time. Objective captures the ultimate goal of the initiative to address the problem of Whistleblowing. The third construct (solution) defines the digital government solution applied to solve whistleblowing problems, the outcome of the initiative such as policy, government tool, public service or capacity-building, and stages of Digital Government such as Digitization, Transformation, Engagement, and Contextualization (Janowski, 2015). The contribution construct defines how the DGOV solution addresses the WB problem.

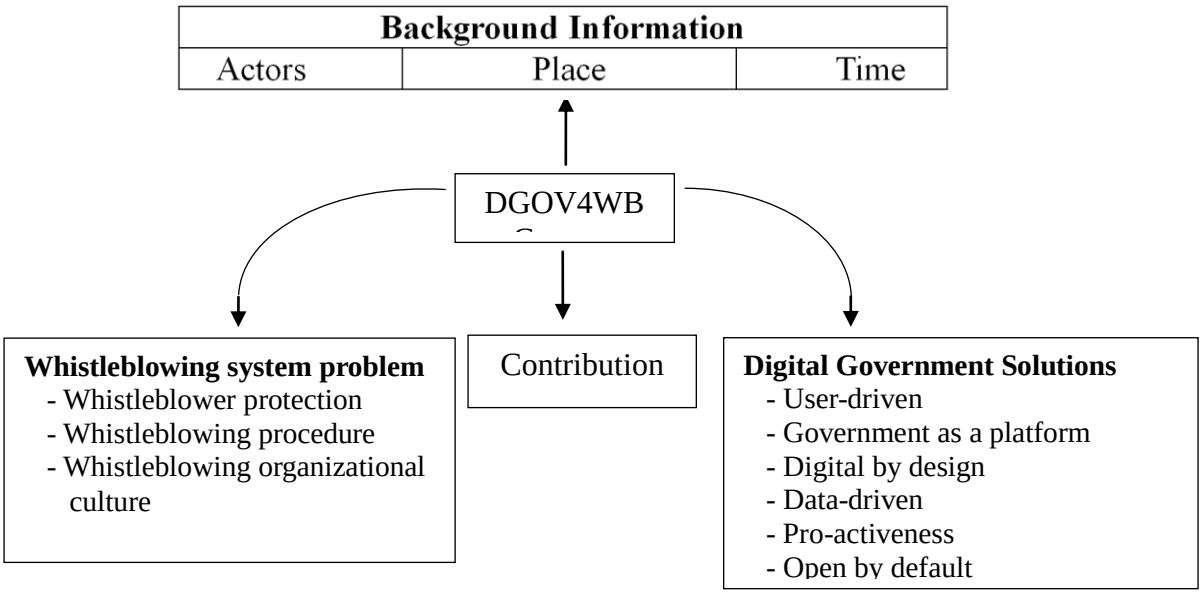

Figure 3. DGOV4WB Assessment framework

The data collection was done through internet searches using search engines. As the concern was about digital government initiatives with the objective of whistleblowing and whistleblower protection, the researchers used the search keys such as 'whistleblower protection', 'governance', 'digital technology', 'digital government', 'whistleblowing' and 'e-government'. The case studies were selected based on the availability of enough resources on the web for the analysis, based on their region and their relevance to the paper.

6. Case Studies

In this section, we present four case studies of DGOV4WB initiatives and each of them evaluated based on the conceptual framework defined in Section 4.

Case 1 - Platform to Protect Whistleblowers in Africa (PPLAAF) - Senegal

Background:

PPLAAF initiative is a Senegalese NGO launched in Dakar 2017 by lawyers, anti-corruption activists and investigative journalists with the mission to help whistleblowers and leaks through legal strategy, financing, research, legislation, and technology (PPLAAF, 2019).

Problem / Objective:

The initiative aims to reduce whistleblowing risks and costs to the point that they are insignificant – primarily for the teacher, the accountant, the soldier, the attorney on the African continent where their disclosures speak to African citizens ' public interest. The founder of the initiative, William Bourdon, states, "We have decided to protect whistleblowers here in Africa, the continent where they take the greatest of risks and are the least protected" (PPLAAF, 2019).

The initiative seeks to protect whistleblowers, and to strategically litigate and advocate on their behalf where their disclosures speak to the public interest of African citizens. Generally speaking, PPLAAF was established to assist whistleblowers whose revelations are related to Africa.

Solution:

The initiative PPLAAF plays the intermediary role by providing a community of in-house and external experts to ensure the process of 'blowing the whistle' is removed from the immediate danger and threats. PPLAAF provides the all the necessary services for whistleblowers, NGOs, media and governments. Among other things, PPLAAF provides Secure Communication, Legal assistance, Media assistant - Connection to credible investigative partners, and Advocacy and research (PPLAAF, 2019). Secure Communication includes: i) Telephonic support (Hotline) 24x7 service which offers the opportunity to an individual to open a dialog by contacting PPLAAF team either English or French language; ii) A secure GlobaLeaks platform – It provides Technological platform which guarantees confidentiality and anonymity all along the communication process through Tor Technology where connection goes through a number of encrypted channels which makes it difficult to trace the source of the information and the identification of the person is more protected. The Legal assistant offers Pro bono legal advice and/or defense. The platform provides guidance on how to approach journalists and which ones to contact for whistleblowing and it will look forward for any assistance.; 3) Media assistant - Connection to credible investigative partners; and 4) Advocacy and research (PPLAAF, 2019).

The Initiative provides whistleblowing information through its website and based on the needs of the whistleblower, it provides a way of reporting wrongdoings through a secure website, encrypted messaging service, and hotlines. PPLAAF provides a secure web portal for sending information and documents, as well as secure hotlines at the disposal of whistleblowers in both French and English. PPLAAF's website operates through the GlobaLeaks platform. It can be accessed through the TOR browser separating PPLAAF's website and the GlobaLeaks platform. The initiative provides two types of technological elements to disclose sensitive information submitted through communication channels. These are: 1) PPLAAF's hotline and 2) GlobaLeaks (submission of a report/ TIP through a webform) as well as the website. No sensitive information should be shared through the hotline (Voice) and web channels while Deep-web GlobaLeaks platform used only for sensitive information which is available through the TOR network allowing for individuals to safely connect and share any sensitive content. Case Management Tool is used to securely centralize, document and manage all cases. Since July 2017, PPLAAF delivered training on security and communication for more than one hundred stakeholders including activists, journalists, and bloggers with a West African network called Africtivistes to avoiding surveillance (PPLAAF, 2019).

Problem / Objective Analysis:

The whistleblowing dimensions problem addressed includes Whistleblowing Procedure and Whistleblowing Protection. The whistleblowing procedure is a reporting channel which can be easily accessed at any time. The whistleblowing protection, on the other hand, provides secured reporting channel that makes anonymity and confidentiality.

Solution Analysis

The solution is related to Local and Regional Governance and Stakeholder participation. The digital government evolution model is engagement. The following Digital Government elements were applied: 1) Digital by design – Publishing information on the portal, providing secured communication using digital tools GlobaLeak and tor technology, and use of Case Management Tool; Providing interface through website channel and telephonic support (Hotline) accessible 24 hours a week and it provides different platforms accessible through different channels; 2) Data-Driven – provide training for 100 stakeholders and it uses data as a key strategic asset; 3) User-Driven - addresses citizen demand on who wants reporting wrongdoing and providing enhanced service; 4) Government – providing legal and media assistant to whistleblowers.

Case 2 - XNET (Xnet – Internet Freedoms) Barcelona, Spain

Background:

Xnet, an activist project which has been working on and for networked democracy and digital rights since 2008, launches in the Barcelona City Hall. It is considered as the first public Anti-Corruption Complaint Box using anonymity protection technology like TOR and GlobaLeaks (Xnet, 2019).

Problem /Objective:

The ultimate goal is to create access to the citizens of the Barcelona city to send information safely, confidentially and anonymous, and to enable civil societies to be an active participant in fighting against corruption in supporting freedom of expression (Xnet, 2019).

Solution:

Xnet is a non-profit activist platform operates in various fields related to digital rights, networked democracy and freedom of expression. Xnet provides a Whistleblowing Platform against corruption for the City Hall of Barcelona – powered by GlobaLeaks and TOR friendly. Xnext launches this Anti-Corruption Complaint Box (XnetLeaks mailbox). The Box uses GlobaLeaks platform and the reporter can access through the Tor network which enables people to maintain the anonymity of communications (Xnet, 2019). There is no possibility to learn the identity of the person sending information even the City Hall itself. The Anti-Corruption Complaint Box is a means of which citizens can fight corruption and other practices that are damaging for good governance in the city of Barcelona. Utilizing the Box, citizens can send their

complaints, suspicions, and evidence of cases that they believe the City Hall should investigate in a way that secures and permits total anonymity. The City Hall responds to every single compline and inquiries into those that are deemed plausible, or send them on to the appropriate institution. The initiative has a capability for the whistleblower reserves the right whether or not to reveal his or her identity. Besides, the reporter can check the status and process of his complain. Xnet provides for journalists and citizens a FAQ service regarding the Box. One notable example is *the Blesa emails* (whistleblowing channel) which reveal Spain's biggest ever leak on banking corruption in 2012. It exposes thousands of corporate emails related to cases of corruption from the former president of Caja Madrid. It now considered one of the best whistleblowing systems in a fight against corruption that provides a safe and secure anonymous mailbox in addition to protecting whistleblowers from reprisals (Xnet, 2019).

Problem / Objective Analysis:

The whistleblowing System dimensions problem addressed includes Whistleblowing Procedure and Whistleblowing Protection. Whistleblowing Procedure is clear and understandable procedures to report wrongdoings and to communicate in response, and channels available for reporting the wrongdoing. The Whistleblowing Protection, on the other hand, provides anonymous and confidential communicating digital tool, Protection of whistleblower identity at all stages of the investigation process.

Solution Analysis:

The solution is related to Local and Regional Governance and Stakeholder participation. The output is public service. The digital government evolution model is Contextualization. The following Digital Government elements were applied: 1) Digital by design – Publishing information on the portal, Anti-Corruption Complaint Box powered by GlobaLeak and tor technology; providing interface through website channel accessible 24 hours a week and *the Blesa emails,* and 2) User-Driven – provides active participation through civil society in combating corruption. 3) |Government – providing a platform for reporting suspicious corruption activities for the citizens.

Case 3 - Vale Whistleblowing Channel (VWC), Indonesia

Background:

Vale Whistleblower Channel (VWC) was launched on January 1, 2016, by PT Vale Indonesia Tbk Company. It is a whistleblowing service that is managed independently and professionally by a violation reporting service provider in Indonesia - PT Deloitte Konsultan Indonesia. The VWC is directly linked to the Vale S.A Code of Ethics and Conduct (VWC, 2019).

Problem/ Objective:

The mission of PT Vale Indonesia Tbk ("PT Vale") is to transform natural resources into prosperity and to commit to sustainable development. To be increasingly competitive in the

business environment, Val implements good corporate governance ("GCG") by continuously improving its performance, transparency, accountability, and responsibility in the eyes of its stakeholders. VWC aims to provide reporting mechanisms for the customers and employees to any illegal activities in a company with at most secured systems and to train all employees on its whistleblowing system (VWC, 2019).

Solution:

In achieving the Mission and the Vision, PT Vale conducts its operational activities, guided by a set of values that reflects high ethical and moral standards. This leads to raising credibility, and maintaining the positive image of the Company in markets, both in the short and long term. The company introduces a violation reporting mechanism, called Vale Whistleblower Channel (VWC), which is managed independently by third parties where its existence thinks the violations can be prevented or detected earlier.

The VWC mechanism contains a reporting system that includes various types of violation, including Fraud, Corruption, Theft, Breach of policy, Conflict of interest, Financial Statement Fraud, Bribery and other types of Harassment, Discrimination, Environment, Health and safety in PT Vale included in the scope. Violation reports may be submitted in Bahasa Indonesia or English, through the channels provided. VWC is equipped with stringent follow-up procedures, therefore PT Vale expects that prospective offenders are reluctant to conduct fraud (VWC, 2019).

Vale Whistleblower Channel includes: 1) 24 hour a week accessible Toll free number, SMS, fax, website, email, and PO Box provided for whistleblower to report suspected incidents of misconduct; 2) Employee education and training on policies and procedures to prevent misconduct; 3) Comprehensive awareness-raising of PT Vale employees of the Whistleblower system; 4) Specialist call center operators with knowledge of PT Vale; 4) Expert forensic investigators to analyze reports 5) Timely reporting of incidences to PT Vale WB team. 6) Recommendations on corrective action.

Problem / Objective Analysis:

The whistleblowing System dimensions problem addressed includes Whistleblowing Procedure, Whistleblowing organizational culture and Whistleblowing Protection. Whistleblowing Procedure is free channels reporting wrongdoing accessible 24x7. Whistleblowing organizational culture is regular training for employees responsible for receiving and investigating reports – Whistleblowing System Team and Regular training for employees on whistleblowing frameworks. Whistleblowing Protection, on the other hand, provides secured reporting channel.

Solution Analysis:

The solution is related to Local and Regional Governance and Stakeholder participation. The output is public service and capacity building. The digital government evolution model is

Engagement. The following Digital Government elements were applied: 1) Government-Providing services to enhance public services and providing informational services; 2) Digital by design – promoting digital technologies to support service delivery and providing digital tools to report wrongdoings; forensic investigators to analyze reports; Providing interface through website channel and email application to its customers and employees. 3) User-Driven –capacity building through training based on the need of the society.

Case 4 – WildLeaks, First Wildlife Crime Whistleblowing initiative (VWC), USA

Background:

WildLeaks is a nonprofit collaborative project created, funded and managed by the Elephant Action League (EAL) based in the United State of America. WildLeaks launched on February 7th, 2014 and it is considered as the first whistleblower initiative dedicated to Wildlife and Forest Crime in the world (WildLeaks, 2019).

Problem / Objective:

According to the founder of the project "The mission of the project is to receive and evaluate anonymous information and tips regarding wildlife crime, including corruption, and to transform them into concrete actions." This includes "preventing wildlife crimes through by facilitate the identification, arrest, and prosecution of criminals, traffickers, businessmen, and corrupt governmental officials behind the poaching of endangered species and the trafficking of wildlife and forest products, including ivory, rhino horn, big cats, apes, pangolins, birds, illegal fishing and illegal timber all over the world". The initiative was developed to expose the key players in the international crime networks, not the low-level operatives on the ground around the world (WildLeaks, 2019).

Solution:

The initiative starts with a target group of any person in the world who witnessed any wildlife crimes. The project consists of the WildLeaks website which has 16 different language versions and smartphone applications. WildLeaks has implemented a very secure online platform built on the Tor technology in order to allow the sources to stay anonymous and to submit 'sensitive' information in the most secure way possible, always encrypted, with respect to data transmission and management. All leaked information through WildLeaks is reviewed, evaluated, and filtered before releasing any of the data to outside parties. It is an extremely very pro-active initiative with a solid investigative component and a diverse of intelligence gathering assets in target countries (WildLeaks, 2019). The online portal allows the whistleblower unique receipt number to connect once again in a secure and anonymous way which enables them to add more information about your original submission, to send us a message, and to interact in an anonymous way.

The initiative protects whistleblowers by providing both on a state-of-the-art secure anonymous system and by managing and using the information professionally. WildLeaks does NOT dump unfiltered data and information onto the web and does NOT pander for media headlines.

For any whistleblowers WildLeaks provides two possible options to send information and files in a very secure platform: 1) Confidential – without the use of Tor Browser, it uses the usual web browsers (Firefox, explorer and google chrome) and the connection to WildLeaks will be automatically completed via HTTPS, which encrypts and secures data as it travels between whistleblower and secure servers where the transmission of the information is secured and encrypted but entities like employers or governmental agencies, may still be able to understand where you are and to see that you are uploading documents. or 2) Anonymous - If whistleblowers want total anonymity, Using Tor Browser submit information to WidlLeaks where the connection is not only secure but also anonymous, leaving no traces behind. Tor technology is considered the best technology for digital anonymity available to Internet users and academics. Tor guarantees that no personal traces remain in WildLeaks systems. To assess the information and decide what to do, WildLeaks uses intelligence methodologies, a vast network of contacts and the latest technologies (WildLeaks, 2019).

Problem / Objective Analysis:

The whistleblowing system dimensions problem addressed includes whistleblowing procedure and whistleblowing protection. Whistleblowing procedure receives and evaluates anonymous information, reporting channel for whistleblowers. Whistleblowing protection, on the other hand, provides secured communication channel with total anonymity and confidentiality.

Solution Analysis:

The solution is related to local and regional governance and stakeholder participation. The output is public service. The digital government evolution model is contextualization. The following Digital Government elements were applied: 1) Digital by design –online portal to report wrongdoings. Allows the whistleblower unique receipt number, providing secured communication using digital tools WildLeaks website and Tor technology; Providing interface through website channel and mobile application and it provides service through 16 different language versions and smartphone applications; 2) User-driven –gaining the accessibility of the public service. 3) Government –providing informational services.

7. Cross Case analysis

The cross-case analysis is a method that involves the in-depth exploration of similarities and differences across cases. This section presents the finding of the analysis of the case studies

(digital government for whistleblowing initiatives) based on the conceptual framework of DGOV4WB described in Section 4.

In whistleblowing analysis, we managed to identify a total of 8, 4 and 2 problems/issues for whistleblowing procedure, whistleblower protection and whistleblowing organizational culture respectively as shown in Tables 2, 3 and 4. The solution analysis of the case studies identifies 10, 6 and 10 types of solutions related to government as a platform, digital by design and user-driven respectively. The DGOV solutions are listed in Tables 5, 6 and 7 respectively as government as a platform, user-driven and digital by design.

Table 2. Whistleblowing Dimensions - Whistleblowing Procedure

S. No.	Whistleblowing Procedure related problems / objectives	Case No.
1	Providing easily accessible reporting channel	1,4
2	Providing reporting channels available at all-time 24x7	1,2,3,4
3	Providing secured channel to communicate in response – to receive feedback	2
4	Providing clear and understandable procedures for internal reporting.	1,2,4
5	Providing digital tool (Case Management System) for recording, investigating and monitoring reports.	2
6	Receive and evaluate anonymous information	1
7	Providing FAQ for the society	2
8	Providing access for status and process of the complain	2

Table 3. Whistleblowing Dimensions - Whistleblowing Protection

S. No.	Whistleblowing Protection related problems/objectives	Case No
1	Providing secured reporting channel (secured communication)	1,2,3,4
2	Providing anonyms connection	1,2,4
3	Providing confidential connection	1,2,4
4	Providing Protection of whistleblower identity ensured throughout all stages of the investigation process	2, 4

Table 4. Whistleblowing Dimensions - Whistleblowing Organizational Culture

S. No.	Whistleblowing Organizational Culture related problems/objectives	Case No.
1	Providing regular trainings for WB team	2
2	Providing regular trainings for employees on whistleblowing frameworks	2

Table 5. Digital Government Dimensions – Government as a platform

S. No.	Digital Government Dimensions – Government as a platform	Case No
1	Providing service through different language versions	4
2	Providing user friendly interfaces website channel	2,4
3	Providing user friendly mobile application.	4
4	Providing simple interfaces	1
5	Providing unified identity for each complain	2
6	Providing telephonic support (Hotline)	1
7	Providing interaction through email	3
8	Providing service through smartphone applications	4
9	providing different platforms accessible through different forms of channels	1
10	Promoting digital technologies to support service delivery	3

Table 6. Digital Government Dimensions - User driven (societal)

S. No.	Digital Government Dimensions – User driven related solutions	Case No.
1	Developing human capacity through training	2
2	Delivering enhanced public service	4
3	Empowering citizens	1
4	Empowering citizens through civil society	2
5	Enhancing citizen participation	2
6	Addresses citizen demand on who wants reporting wrongdoing and providing enhanced service.	2

Table 7. Digital Government Dimensions – Digital by design

S. No.	Digital Government Dimensions – Digital by design related solutions	Case No.
1	Providing online portal to report wrongdoings	1,2,4
2	Providing digital tools to report wrong doings	3
3	Providing mobile based platform for service delivery	2,3
4	Providing secured communication using digital tools WildLeaks website and Tor technology	1,4
5	Provide digital tools to analyze reports	2
6	Publishing information on the portal	1,2
7	Providing Case Management Tool	1
8	Promoting Anti-Corruption Complaint Box powered by GlobaLeak and Tor technology	2
9	Applying secured technologies	1,2,4
10	Providing digital forensic investigators service to analyze reports	3

8. Finding and Discussion

Considering the DGOV4WB conceptual and assessment frameworks described in Section 4, we started to analyze all the case studies in Section 5. In our analysis, the themes are identified through the iterative process of identifying WB problems and DGOV solutions based on case studies.

Our case study analysis showed that DGOV4WB initiatives/projects positively contributed to solving a variety of whistleblowing (WB) issues/problems. Specifically, WB problems addressed by the WB dimensions includes whisleblowing procedure, whistleblowing organizational structure, and whistleblower protection. Whistleblowing Procedure is concerned with whistleblowing reporting mechanism and monitoring the process; Whistleblowing Organizational culture is about communication (training all involved stakeholders); Whistleblower Protection aims at anonymity and confidentiality of communication. The analysis also showed that DGOV4WB initiatives applied to a variety of DGOV solutions in different DGOV dimensions: supportive ecosystems which are an easy and interactive interface of communicating channels to report the wrongdoing activities (government), ICT-enabled services and government ICT infrastructure based on user preference, and enabling the citizens/customers or any stakeholders to involve in the process through different languages and platforms and active citizen participation and civil societies contribution (User-driven), Digital transformation within the government and secured communication channel and Case Management Tools for recording and managing the complaints (Digital by design). The correlation between the dimensions of WB problems and the dimensions of DGOV solutions, problem to solution relation, as they occur within the case studies are presented in Table 8. For each problem-solution pair, the table lists all case studies that apply the solution to address the problem. Figures 5 and 6 depicts the distribution of the problems and solution across the WB and DGOV dimensions.

Table 8. Correlation between DGOV solutions to WB Problems through code words

Code Word	Case Numbers	Code Word	Case Numbers
M1	All cases	M7	1
M2	All cases	M8	3,4
M3	1,4	M9	1,3,4
M4	All cases		
M5	2,3		
M6	4		

As indicated in Figure 6, whistleblowing procedure is the highest-ranked categories of whistleblowing dimensions in problem description while according to Figure 5 the highest-ranked categories of DGOV solutions belong to digital by design and Government as a platform. While DGOV4WB solutions may be expected to holistically address all whistleblowing dimensions, this expectation is also the main challenge facing such initiatives.

The case study evidence indicates that digitally-enabled whistleblowing reporting channels, both electronic platforms and hotlines, used to facilitate individual disclosures. It eases the disclosure of organizational wrongdoing for protection against fraud and any wrongdoing activities. All the four cases provide a dedicated channel to whistle-blowing. An electronic platform whistleblowing channel exists in all of the case studies and except Xnet the other three whistleblowing initiatives provide dedicated hotlines. These reporting channels are open to

receive reports for 24 hours of a day for all 365 days of the year. Both whistleblowing electronic platforms and whistleblowing hotlines enable the individuals to report unlawful activities through different language in either of whistleblowing disclosure methods –oral or written. The finding identified Tor technologies have been used to provide whistleblower protection – anonymity and confidentiality. Our finding also shows that Case Management Tool has been used in two of our cases to manage the reported cases for recording, investigating, and monitoring reports. This case management tool provides a mechanism for notifications, analysis, and reporting management for each reported case. This enables the whistleblowers to track their whistleblowing reports at every stage of the whistleblowing process. This enables the whistleblowers to track their whistleblowing reports at every stage of the whistleblowing process and to communicate with the government/organization officials for further information. This capability of the whistleblowing system enables the active participation of employees in the whistleblowing process.

From the case studies, all the initiatives were classified either engagement (Electronic Governance) or contextualization (Policy-Driven Electronic Governance) stage of the digital government evolution model. Engagement stage enables engaging citizens and other nonstate actors in government decision making and trust building. It aims to transform relationships between government and citizens through the use of digital channels to build trust (Janowski, 2015). This digitally whistleblowing systems smooths the relationship between the government and its citizens in combating misconduct and frauds in an organization. According to Janowski (2015) Contextualization stage involves "the choice of locally-relevant and/or sector-specific goals, locally-acceptable and sectorally-feasible ways of pursuing such goals, and managing the impact on the local environment and sector involved". It enables sectors, territories, communities, citizens, etc. to pursue development action by themselves. It aims to create better conditions through digital technology to pursue public policy and development goals. Whistleblowing systems allow the citizen to participate in tackling corrupt, unlawful activities within the organization.

The three case studies/initiatives: Xnet, Wildleaks, and PPLAAF are all developed by non-governmental organizations or individuals who are an active activist and lowers. VWC is a VAL company whistleblowing channel to support its good corporate governance (GCO) principles that could help to achieve accountability and transparency in the VAL Company. Interestingly, the result of the study indicates whistleblowing systems developed by non-governmental organizations are more user-driven (language and whistleblowing methods varieties) compared to governmental whistleblowing.

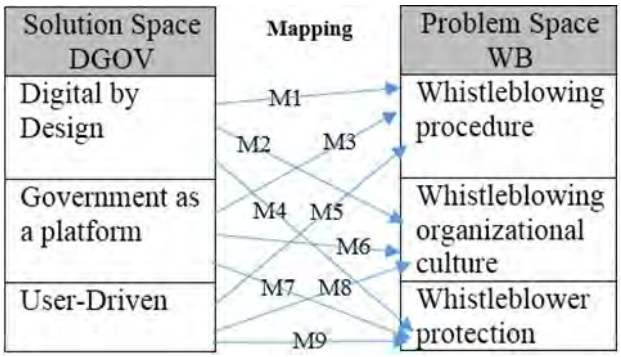

Figure 4. WB problems and DGOV solutions code mapping

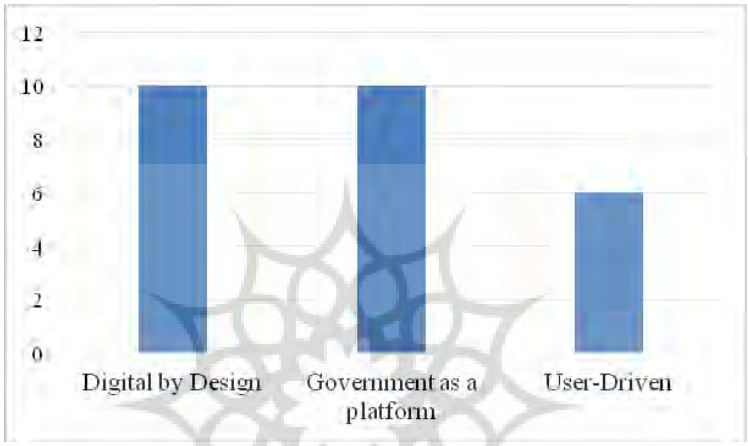

Figure 5. Distribution of DGOV Solution

Figure 6. Distribution of WB Problems

9. Conclusion

This paper serves as an introduction to the new research area Digital Governance for whistleblowing (DGOV4WB). It was set out to achieve three main objectives: 1) to offer a conceptual framework for DGOV4WB, 2) to identify the potential issues in whistleblowing and 3) to explore how digital government has been used to address these issues. The following

procedures were followed to meet these objectives. First, Section 3 presented a conceptual framework for DGOV4WB. The framework identified six dimensions (OECD, 2019) in the DGOV perspective –Government as a platform, Digital by design, Data-driven, User-driven, Open by default and Pro-activeness; three dimensions in the WB perspective –whistleblower protection, whistleblowing procedure and whistleblowing organizational culture (TI, 2013); and six underlying domains — Governance (GOV), Whistleblowing (WB), Digital Technologies (DT), Digital Governance (DGOV), Governance for WB (GOV4WB), and DT for WB (DT4WB). Second, Section 5 and 6 documented and analyzed four case studies (DGOV4WB initiatives) through exploratory or formative research methodology - to demonstrate how DGOV solutions are contributing to solve the problems of WB dimensions. We managed to identify the WB problems based on their dimensions and the correlation to the possible DGOV solution is mapped. Brevini (2017) has examined the rise and the legacy of the disclosure platform in the whistleblowing domain (Brevini, 2017). Lam and Harcourt (2019) explored Virtual whistle-blowing which also has implications for general surveillance and the rights and freedoms. However, both studies don't show how the digital government could make an impact on the whistleblowing domain. Besides, the stages of digitally enabled whistleblowing initiative in the digital government evolution model (Janowski, 2015) did not indicate ways the digital government could make an impact on the whistleblowing domain.

This paper makes an important contribution to identifying potential issues in whistleblowing and to exploring how digital government has been used to address these issues. A conceptual framework, exhibiting how DGOV solutions are contributing to WB problems, was developed to show the importance of digitally enabled whistleblowing initiatives. In addition, this paper establishes a foundation for further DGOV4WB research.

The paper also revealed that despite the growing interest in DGOV and WB research and a strong potential for applying DGOV research to further WB objectives, research at the intersection of both domains is scarce and almost utterly practiced within the contributing domains. We are aware of several limitations of this research. First, the case studies were small in number and were not evenly distributed across the continent. Second, this research indicates that the digitally enabled whistleblowing initiatives are classified as either engagement or contextualization stage of the digital government evolution model. However, this paper is limited in analyzing at what stage of digital government is required for each whistleblowing dimensions based on Janowski (2015) articles analysis published between 1992 and 2014 in government information quarterly (GIQ) that classified digital government initiatives in four stages, from digitization (technology in government), transformation (electronic government), and engagement (electronic governance), to contextualization (policy-driven electronic governance). Additionally, issues related to the identification of all the relevant stakeholders in whistleblowing and its new business models due to the implementation of the digital government need to be analyzed.

Table 9. Scopus Databases Search Publications result

	Publication Year														
Key words	**< 2000**	**2004**	**2005**	**2006**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**Total**
Digital Government & Whistleblower	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Digital Government & Whistleblowing	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
E-government & Whistleblowing	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
E-government & Whistleblower	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Digital Technologies & Whistleblower	0	0	1	0	0	0	0	0	0	0	0	0	1	0	2
Digital Technologies & Whistleblowing	0	2	1	0	0	0	0	0	0	0	0	0	0	0	3
Technology & Whistleblowing	13	2	1	1	1	4	1	2	5	3	1	3	2	3	42
Technology & Whistleblower	2	0	2	1	0	1	1	1	2	1	5	3	1	2	22
ICT & Whistleblowing	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ICT & Whistleblower	0	0	0	0	0	0	0	0	0	0	2	1	0	0	3

References

ACFE. (2016). *Report to the Nations on Occupational Fraud and Abuse*: 2016 Global Fraud Study. Association of Certified Fraud Examiner (ACEF) publishing. Retrieved January 10, 2020, from https://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf

Accenture. (2015). *Digital government pathways to delivering public services for the Future: A comparative study of digital government Performance across 10 countries*. 2015 Accenture Report, Accenture publishing. Retrieved January 10, 2020, from https://www.accenture.com

Alleyne, P., & Watkins, A. (2017). Whistleblowing as a corporate governance mechanism in the Caribbean. In Snapshots in Governance: *The Caribbean Experience* (2nd ed., pp. 176–198). University of the West Indies.

Apaza, C. R., & Chang, Y. (2011). What makes whistleblowing effective?. *Public Integrity*, 13(2), 113–130. DOI: 10.2753/pin1099-9922130202

Banisar, D. (2011). Whistleblowing: International standards and developments. In *Corruption and Transparency: Debating the Frontiers between State, Market and Society*. Washington, DC: World Bank-Institute for Social Research.

Barkemeyer, R., Preuss, L., & Lee, L. (2015). Corporate reporting on corruption: An international comparison. *Accounting Forum*, 39(4), 349–365. DOI: 10.1016/j.accfor.2015.10.001

Berry, B. (2004). Organizational culture: A framework and strategies for facilitating employee whistleblowing. *Employee Responsibilities and Rights Journal*, 16(1), 1–11. DOI: 10.1023/b:errj.0000017516.40437.b1

Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly*, 27(3), 264–271. DOI: 10.1016/j.giq.2010.03.001

Brevini, B. (2017). WikiLeaks: Between disclosure and whistle-blowing in digital times. Sociology Compass, 11(3). DOI: 10.1111/soc4.12457

Corydon, B., Ganesan, V., & Lundqvist, M. (2016). *Transforming government through digitization*. *Transforming government through digitization*. McKinsey & Company publishing. Retrieved January 10, 2020, from https://www.mckinsey.com/

Courtland, C. C., & Cohen, M. C. (2017). Whistleblower laws in the financial markets: Lessons for emerging markets. *Arizona Journal of International & Comparative Law*, *34*(2).

Deloitte. (2015). *How are digital trends reshaping government financial organizations? Findings from Deloitte NASACT 2015 Digital Government Transformation Survey*. Deloitte Development LLC Publishing. Retrieved January 10, 2020, from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-state-nasact-survey.pdf

Devine, T., & Maassarani, T. F. (2011). *The corporate whistleblower's survival guide*. Berrett-Koehler publishing.

Emura, K., Kanaoka, A., Ohta, S., & Takahashi, T. (2017). Establishing secure and anonymous communication channel: KEM/DEM-based construction and its implementation. *Journal of Information Security and Applications*, 34, 84–91. DOI: 10.1016/j.jisa.2016.12.001

Estevez, E., Janowski, T., & Dzhusupova, Z. (2014). Electronic Governance for Sustainable Development – How EGOV Solutions Contribute to SD Goals? *The Proceedings of the 14th Annual International Conference on Digital Government Research*.

EY. (2016). *Whistle-blowing: The pillar of sound corporate governance, building better government.* Ernst & Young LLP. Publishing, India. Retrieved January 10, 2020, from www.ey.com/in

Fang, Z. (2002). E-Government in Digital Era: Concept, Practice, and Development. *International Journal of The Computer, The Internet and Management*, *10*(2), 1–22.

Figg, J. (2000). Whistleblowing. *Internal Auditor*, 30–37.

Hoetker, G. (2002). Building the virtual state: information technology and institutional change building the virtual state: Information Technology and institutional change, by Fountain Jane E. Washington, DC: Brookings Institution Press, 2001. *Academy of Management Review*, 27(4), 619–622. DOI: 10.5465/amr.2002.7566114

GFIR. (2018). *Exploring the links between customer recognition, convenience, trust and fraud risk.* The 2018 Global Fraud and Identity Report. Experian Information Solutions Publishing. Retrieved January 10, 2020, from https://www.experian.com/assets/decision-analytics/reports/global-fraud-report-2018.pdf

GFR. (2015). *Vulnerabilities on the rise annual edition:* 2015/2016 Global Fraud Report, Kroll and the Economist Intelligence Unit Ltd Publishing. Retrieved January 10, 2020, from http://anticorruzione.eu/wp-content/uploads/2015/09/Kroll_Global_Fraud_Report_2015low-copia.pdf

Intuit. (2017). *The path to digital governance: An agenda for public service innovation and excellence*. Intuit Publishing, Canada. Retrieved January 10, 2020, from https://iog.ca/docs/The-Path-to-Digital-Governance.pdf

Heemsbergen, L. (2013). Whistleblowing and digital technologies: An interview with Suelette Dreyfus. *Journal of Media and Communication*, *5*(1), 67–71.

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly*, 32(3), 221–236. DOI: 10.1016/j.giq.2015.07.001

Katsonis, M., & Botros, A. (2015). Digital government: A primer and professional perspectives. *Australian Journal of Public Administration*, *74*(1), 42–52. DOI: 10.1111/1467-8500.12144

Kraemer, K., & King, J. L. (2006). Information technology and administrative reform. *International Journal of Electronic Government Research*, *2*(1), 1–20. DOI: 10.4018/jegr.2006010101

Lachman, V. D. (2008). Whistleblowing: Role of organizational culture in prevention and management. *Dermatology Nursing / Dermatology Nurses' Association (Dermatol Nurs)*, *20*(5), 394-396.

Lam, H., & Harcourt, M. (2019). Whistle-blowing in the digital era: motives, issues and recommendations. *New Technology, Work and Employment*. DOI: 10.1111/ntwe.12139

Miceli, M. P., Dozier, J. B., & Near, J. P. (1987). Personal and Situational Determinants of Whistleblowing. *Paper presented at the meeting of the Academy of Management*, New Orleans, LA.

Morgeson, F. V., & Mithas, S. (2009). Does e-government measure up to e-business? Comparing end user perceptions of U.S. federal government and e-business web sites. *Public Administration Review*, *69*(4), 740–752. DOI: 10.1111/j.1540-6210.2009.02021.x

Near, J. P., & Miceli, M. P. (1995). Effective-whistle blowing. *Academy of Management Review*, *20*(3), 679–708. DOI: 10.5465/amr.1995.9508080334

Near, J. P., & Miceli, M. P. (1985). Organizational dissidence: The case of whistle-blowing. *Journal of Business Ethics*, *4*(1), 1–16. DOI: 10.1007/bf00382668

OECD. (2003). *The e-government imperative.* OECD Publishing, Paris. DOI; 10.1787/9789264101197-en

OECD. (2012). *Whistleblower protection: Encouraging reporting. CleanGovBiz Integrity Practice*. OECD Publishing, Paris.

OECD. (2015). *G20/OECD Principles of Corporate Governance*. OECD Publishing, Paris. DOI: 10.1787/9789264236882-en

OECD. (2016). *Digital Government Strategies for Transforming Public Services in the Welfare Areas: OECD COMPARATIVE STUDY*. OECD Publishing, Paris. Retrieved January 10, 2020, from http://www.oecd.org/gov/digital-government/Digital-Government-Strategies-Welfare-Service.pdf

OECD. (2019). *Strengthening digital government*. OECD Going Digital Policy Note, OECD Publishing, Paris. Retrieved January 10, 2020, from http://www.oecd.org/goingdigital/strengthening-digital-government.pdf

PPLAAF. (2017). *Platform to protect whistleblowers in Africa*, first year activity report. PPLAAF Publishing. Retrieved January 10, 2020, from https://pplaaf.org/downloads/annual_report.pdf

Qusqas, F., & Kleiner, B. H. (2001). The difficulties of whistleblowers finding employment. *Management Research News*, *24*(3/4), 97–100. DOI: 10.1108/01409170110782702

Rosenbloom, T. (2003). Risk evaluation and risky behavior of high and low sensation seekers. *Social Behavior and Personality: An International Journal*, *31*(4), 375–386. DOI: 10.2224/sbp.2003.31.4.375

Rothschild, J., & Miethe, T. D. (1999). Whistle-blower disclosures and management retaliation. *Work and Occupations*, *26*(1), 107–128. DOI: 10.1177/0730888499026001006

Scholl, H. J. (2006). What can e-commerce and e-government learn from each other? *Proceedings of the 2006 National Conference on Digital Government Research - DG.O 06*. DOI: 10.1145/1146598.1146746

Seifert, J. W., & Chung, J. (2008). Using e-government to reinforce government—citizen relationships. *Social Science Computer Review*, *27*(1), 3–23. DOI: 10.1177/0894439308316404

TI. (2013). *Whistleblower protection and the UN convention against corruption*. Transparency International Publishing. Retrieved January 10, 2020, from http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/ti_report_/ti_report_en.pdf

TI-NL. (2017). *Whistleblowing frameworks. Assessing Dutch publicly listed companies.* Transparency International Nederland Publication. Retrieved January 10, 2020, from https://www.transparency.nl/wp-content/uploads/2017/12/Whistleblowing-Frameworks-TI-NL-final-report-13-12-2017.pdf

Tweedie, B. (2010). Whistle Stop: the Suppression of whistleblowers in the Canadian. *Government. Electronic Theses and Dissertations*, 7. Retrieved January 10, 2020, from https://scholar.uwindsor.ca/etd/7

VWC. (2019). Whistleblowing system. Retrieved January 10, 2020, from http://www.vale.com/indonesia/EN/investors/corporate-governance_id/whistleblower-system/Pages/default.aspx

WildLeaks. (2019). Retrieved January 10, 2020, from https://wildleaks.org/

Xnet. (2019). Internet freedoms & digital rights. Retrieved January 10, 2020, from https://xnet-x.net/en/

Bibliographic information of this paper for citing:

Walle, Y. M. (2020). The impact of digital government on whistleblowing and whistle-blower protection: Explanatory study. *Journal of Information Technology Management*, 12(1), 1-26.