Whistleblowing in the Software Industry: a Survey

Stefan Reijenga
VU Amsterdam
s.reijenga@student.vu.nl

Kousar Aslam
VU Amsterdam
k.aslam@vu.nl

Emitzá Guzmán
VU Amsterdam
e.guzmanortega@vu.nl

Abstract*—*Background: **Wrongdoings occurring within or in relation to software can have big implications on individuals, groups of people, or society as a whole. Whistleblowing is considered an effective tool to reveal and stop wrongdoing but is still a controversial topic that has been researched sparsely in the software industry.** ***Aim:*** **In this study we address this gap and research the current environment for whistleblowing (reporting wrongdoing) in the software industry.** ***Method:*** **We surveyed 147 software practitioners about their views on whistleblowing, the current means they have to report software-related wrongdoing, and the enabling and obstructing factors to whistleblow.**

Results: **Our study shows that software practitioners have a positive view towards whistleblowing. However, in practice whistleblowing is obstructed by the difficulty of proving the actual harm and fear of retaliation. Practitioners with more years of experience report more comfort using readily established mechanisms and procedures in their organization, are more willing to speak up and have more confidence that their report will lead to action than their less experienced peers. These differences are statistically significant.** ***Conclusion:*** **Through our results we conclude that the software industry needs to improve the environment for whistleblowers by providing more external reporting mechanisms, anonymity, and confidentiality, as well as support practitioners with less years of experience.**

***Index Terms*—whistleblowing, software industry, ethics in software engineering**

I. Introduction

From airports, to banks, healthcare, space crafts, and even social media, software is everywhere. Human lives increasingly depend on software products and, therefore, on the people responsible for its creation and maintenance. If wrongdoings occur within or in relation to software, they can have big implications on individuals, groups of people, or society as a whole. Whistleblowers are insiders who expose such wrongdoings— eventually stopping misconduct, such as fraud, endangerment to public health and safety, or damage to the environment. With famous examples unveiled by whistleblowers depicting serious issues in software applications, such as voter manipulation [1], failure to secure sensitive user data [2], negative mental health impact on teenage users [3] and emotion manipulation [3], it is not unthinkable that similar instances will occur in the future, increasing the reliance on whistleblowers for the exposure of wrongdoings in the software industry. With the growing entanglement of software in society, it is crucial to recognize that wrongdoings in software companies need to be discussed and corrected as they can lead to dangerous situations [4], and cause serious harm.

Whistleblowing is considered an effective tool to reveal and stop wrongdoing [5], and organizations are increasingly encouraged to embrace whistleblowers as a means to identify and eradicate issues within an organization [6]. Nevertheless, it is still a controversial topic as it presents a tradeoff between loyalty and justice or morality. Internal disclosure (reporting within organisation) is often insufficient to deal with serious wrongdoing [7]. Therefore, whistleblowers often choose external means to speak up about misconduct happening inside the company [8]. Publicly blowing the whistle after detecting some form of wrongdoing like fraud, endangerment of someone's health and safety, or damaging the environment would seem like a logical and even heroic thing to do, as serious consequences for many are expected, right? Well, not per se. It is common for whistleblowers to face retaliation from the same society they are protecting after conducting their actions [9]. This paradox is interesting as proper support for whistleblowers is deemed an essential factor in enabling disclosures about organizational wrongdoing [10], [11].

In words of Hunt and Ferrario [12] whistleblowing in context of the software industry is *"the responsible evidencing and disclosure of actions and artefacts perceived to be contrary to accepted ethical and professional standards [13] or software life-cycle standards (e.g. [14]), carried out to mitigate harm to self, others and wider society."*. This broad definition covers wrongdoings happening in all aspects of the software industry including the working environment, software development processes and the artefacts produced during software life cycle. In our work we particularly focus on *wrongdoings related to the software itself*, such as privacy and security breaches, discrimination happening within the software, enabling fraud or corruption, endangering someone's health or safety, and damaging the environment. Similar to other types of whistleblowing, reporting on software-related wrongdoing is not trivial and has received wide public attention and negative consequences to its reporters in the past, e.g., [15], [16].

While whistleblowing has been studied in different work sectors, research on whistleblowing in the software industry is sparse. We address this gap by examining the current state of whistleblowing about software-related wrongdoing in the software industry. For this purpose, we conducted a survey with 147 software professionals and explored practitioners' viewpoints on whistleblowing, current reporting practices, and

978-1-6654-5223-6/23/$31.00 ©2023 IEEE

the factors that enable and obstruct whistleblowing in the software industry. This is, to our best knowledge, the first study to use a questionnaire-based survey to study this topic. To allow for the replication and extension of our study, we make the collected data and survey instrument available[1].

The main contributions of this work are: (1) initial empirical evidence of the main viewpoints that software practitioners have on whistleblowing in the industry, (2) early empirical evidence about current obstructing and enabling factors of whistleblowing in the software industry and (3) a survey instrument, analysis scripts and data that can be used for further studies.

II. Background and Related work

A. Methods and incentives to whistleblow

Whistleblowing can be done internally [17] (for instance, reporting to a coworker, manager or counselor inside organization) or externally [17], [18] (report to entities outside the organization, for example, the media, an online platform, a regulator, law enforcement, or a representative of a union or external organization). Internal whistleblowing entails the risk that the concerned organization tries to cover up the wrongdoing. Previous research shows that external whistleblowing is a more effective approach for addressing wrongdoing and assigning the appropriate changes to an organization [19]. To facilitate and enable the act of reporting wrongdoing, an organization can implement various channels such as an internal hotline, a dedicated email, a web-based system, or in-person reporting [20].

When reporting wrongdoings, anonymity is considered to be an enabling factor for the whistleblowers [21]. Anonymity protects whistleblower from retaliation, however, it may reduce the effectiveness of whistleblowing as anonymous reports may be more difficult to investigate [22]. The personal traits of people also affect their intention to blow the whistle. Previous studies showed that the professional commitment of employees has a positive effect on whistleblowing intention as well as moral intensity [23], [24]. Although financial incentives are not common for whistleblowers, reward systems do increase the likelihood of whistleblowing [25], [26].

B. Facing obstacles and retaliation when whistleblowing

The lack of support from senior management [27] and the risk of any form of retaliation reduces an employee's willingness to report wrongdoing [28]–[30]. Whistleblowers pay a personal, psychological and financial price that often goes unnoticed by society [31]. Previous studies show that retaliation is still a common fate for many whistleblowers. Over half of the whistleblowers got fired after blowing the whistle in United States, and over 90% of the whistleblowers were subjected to some form of personal threats and reprisals [32]. Whistleblowers are seriously underprivileged when they apply for future jobs [33]. On average, a whistleblower is unemployed for 3.5 years after their disclosure, and 64% of the whistleblowers are formally blacklisted, which prevents them from working in their desired field [9].

C. Whistleblowing in relation to the software industry

Although software and technology have a strong influence on human lives, the number of cases reported by whistleblowers in this domain is lower than in other public sectors [34]. Literature regarding whistleblowing in the context of software industry is also scarce as of now. Hunt and Ferrario [12] recently provided a comprehensive overview of how whistleblowing has been researched in the software engineering research community. Their analysis of existing literature reveals that whistleblowing in the community is under-explored area and that the few available research presents whistleblowing as an individual's moral and ethical responsibility, rather than a collaborative effort.

The unwillingness of a project member to report issues within projects that have a software element has been focus of previous work [35]–[38]. A study among graduate business students following an information systems course found a strong connection between an individual's personal sense of responsibility and their willingness to report bad news [38]. Another study, conducted via an experiment encompassing hypothetical software project situations, suggests that an individual's willingness to report bad news is affected by personal factors like morality [37].

For demographic aspects, Keil et al. [39] found a positive association between whistleblowing intention, years of work experience and female gender when conducting a conjoint study with 159 IT managers. A general overview of the whistleblowing literature, however, shows an inconsistent effect of both of these factors on whistleblowing [40]. In the software industry, 71% of whistleblowers face some form of consequences which includes being fired, harassed, threatened, demoted, or suspended [41].

Duits et al. [42] studied whistleblowing as a socio-technical phenomenon by mining the communication of Twitter users to understand the sentiment of the general public towards whistleblowing in tech. Their results show that tweets expressing an opinion about whistleblowing in tech were mostly supportive and that mainly large companies such as Apple, Microsoft and Facebook are discussed in tweets regarding whistleblowing and tech.

The above-mentioned studies show the importance of reporting wrongdoing in the software industry and in creating a supportive environment for reporting these wrongdoings. However, there exists little understanding of the current environment for whistleblowing in the software industry across the globe. To the best of our knowledge, our work is the first attempt to explore this by directly surveying software practitioners, and broadening the scope in terms of exploring the enabling and obstructing factors for reporting wrongdoing related to software.

III. Scope and Research questions

The goal of this study is to explore the current environment for whistleblowing in the software industry. Our work is

[1] https://zenodo.org/record/7197878#.Y0ks5uxBx_k

guided by three research questions:

- **(RQ1) General views:** What are the general views and perceptions of software practitioners on reporting wrongdoing related to software?
- **(RQ2) Means of reporting:** What mechanisms and procedures are in place for software practitioners to report wrongdoing related to software?
- **(RQ3) Enabling and obstructing factors:** What enables or obstructs software practitioners from reporting wrongdoing related to software?

We define *wrongdoing* related to software as unethical or harmful behavior of the software such as privacy and security breaches, discrimination happening within the software (e.g., favoring certain users by an algorithm or allowing hate speech against specific user groups), enabling fraud or corruption, endangering someone's health and safety (e.g., motivating addictive behavior, triggering depressive thoughts), and damaging the environment (e.g., algorithms with high CO_2 emissions). Discrimination, (sexual-) harassment, physical violence, abuse of power, and any dynamics occurring within the development teams are out of the scope of this study. Wrongdoings can be reported internally (within the organization) or externally (outside the organization to a governing body, media or general public. We research both forms of reporting in this study. In this work we use the terms *reporting wrongdoing* and *whistleblowing* as synonyms. We do not make any differentiation between *intentional* and *unintentional wrongdoing*, as we consider that both need to be reported and addressed. Moreover, we use the term *software practitioners* or *software professionals* to refer to individuals working in the software industry in a large variety of roles and positions. This includes employees who analyze, design, develop, implement, operate, maintain, or manage software (for instance, software engineers, software testers, product owners, project managers, software consultants, and data scientists).

IV. Methodology

We used a positivist approach [43] and carried out a questionnaire-based survey, described below, to answer the research questions.

A. Target population

The target population of the survey is software practitioners. Therefore, we exclusively targeted people who work in tasks related to software development, regardless of their specific industry. The study does not limit to a particular role (technical or non-technical) or position, so programmers, testers, consultants, and (project-)managers were considered eligible to participate in the survey.

B. Survey design

We adapted, and in some cases directly adopted, questions from existing surveys that were helpful to answer our research questions [20], [44]–[50] researching whistleblowing in other industries when designing our survey. When needed, the wording of questions from other surveys was adapted to make them more relevant for the software engineering community or to make the question-style of our survey uniform. The survey contains 30 questions separated into four sections: demographics (DQ), general view (RQ1), means of reporting (RQ2) and, enabling and obstructing factors (RQ3). The format of the answers to the questions is either five-point Likert scale (LQ) [51], [52] or non-scaled choice(s) (MC). For some questions, respondents could also fill an open-text field, if they do not find a choice in the available options (e.g., MC1, MC3, MC4). Table I shows all questions in our survey, with exception of the demographic questions. One question (LQ2) did not stem from studying similar surveys but was manually added to get a better insight into the overall sentiment of software practitioners on the topic of whistleblowing in relation to software. An optional set of questions (MC9, MC10, MC11) could be accessed when respondents indicated that they have witnessed or suspected wrongdoing related to software in their organization. These questions are regarding whether they took action or not based on their observation(s), what type of action they took or why they did not, and what was the reaction from their organization. They are also shown in Table I. To avoid biasing participants, the survey uses the more neutral term *reporting wrongdoing* as a substitute for whistleblowing. The survey respondents were provided with a definition and examples of wrongdoing at the beginning of the survey. These definition and examples, which mirror the ones provided in Section III, still gave participants a degree of freedom in their interpretation of what is harmful or unethical when it comes to software[2]. To ensure that participants reported about *wrongdoing related to software*, we explicitly used this wording in our questions.

A trial run was held with five participants, all graduate students, three of whom were working as software practitioners in the industry at the time of the trial. Trial participants were asked to fill in the survey and give feedback regarding the formulation of the questions, the answer options, and the overall clarity of the survey. Based on the feedback from the trial run, the survey was refined. Changes included uniforming answer options for the multiple-choice questions and the overall formulation of the questions. Responses received from trial run were not included in the analysis of the results.

C. Survey Distribution

The survey was designed to be distributed online. We distributed the survey in our personal network and in software-related groups of LinkedIn, Facebook, and Reddit. This approach has the advantage that a large group of potential participants can be reached with relatively little effort. The survey was distributed between May and June of 2022.

D. Data analysis

We applied a mixed-methods approach for analyzing our results. In our analysis we inspected if answers among partic-

[2] This decision was intentional as we did not want to define wrongdoing in legal terms (a lot of wrongdoing is unregulated), and conceptions of what is ethical/unethical, harmful/unharmful can vary among individuals.

#	Question	Response Options	Reference
RQ1 - General views			
LQ1	I am familiar with legislation aiming to protect people that report wrongdoing (whistleblowers)	[Strongly Disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree]	[49]
LQ2	It is important that IT professionals speak up when witnessing wrongdoing related to software	[Strongly Disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree]	
MC1	As an IT professional which one of these actions do you think is the most effective way to stop wrongdoing related to software? (Choose only one)	[By directly confronting the wrongdoer, By informally addressing the wrongdoing to coworkers or management (e.g., at the weekly status meeting or at the coffee machine), By formally reporting the wrongdoing within the organization via official channels (e.g., email, hotline, web-based system), By formally reporting the wrongdoing to a regulator outside the organization via official channels (e.g., email, hotline, web-based system), By reporting the wrongdoing to journalists or news organizations, By reporting the wrongdoing directly to the general public, via the internet, Twitter, Facebook, or on online blogs, None of the above – in my opinion, there is no effective way to stop wrongdoing, Don't know]	[20], [44]
MC4	As an IT professional when do you think it is appropriate to report wrongdoing related to software to journalists, media, or an online platform? (Choose only one)	[As the first option in any situation, Whenever there becomes a specific reason to do so, Only as a last resort, if all else fails, Never, Don't know]	[44], [46]
MC8	Have you ever witnessed or had suspicions that some form of wrongdoing related to software may have taken place within your current organization?	[Yes, No]	[46]
LQ3	It is in the interest of my organization for IT professionals to speak up about wrongdoing related to software	[Strongly Disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree]	[45], [46]
LQ4	If I observed wrongdoing related to software in my workplace, I would feel personally obliged to report it to someone in my organization	[Strongly Disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree]	[44]
RQ2 - Means for reporting			
LQ7	I am aware of the procedures/mechanisms to use when reporting wrongdoing related to software within my organization	[Strongly Disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree]	[48]
LQ8	I would be comfortable using the current procedures/mechanisms in place to formally report any wrongdoing related to software in my organization	[Strongly Disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree]	[48]
MC5	Which of the following channels are available to employees in your organization to formally report wrongdoing related to software? (Choose all relevant answers)	[Internal hotline, External hotline (outsourced to a third-party provider), Dedicated email, In-person reporting, Internal web-based system, External web-based system (outsourced to a third-party provider), Don't know, There are no formal channels available to report wrongdoing related to software]	[20], [47]
MC6	Is it possible for employees in your organization to report wrongdoing anonymously?	[Yes, No, Don't know]	[20]
RQ3 - Enabling and obstructing factors			
LQ5	If I reported wrongdoing related to software in my organization, I am confident something appropriate would be done about it	[Strongly Disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree]	[44]
LQ6	Management in my organization is serious about protecting people who report wrongdoing related to software	[Strongly Disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree]	[44]
MC2	As an IT professional which of the following factors would enable you to report wrongdoing related to software? (Choose all relevant answers)	[If I am guaranteed confidentiality (i.e., I share my name and know management or investigators would not share my identity with anyone), If I can report anonymously (i.e., my identity is not shared with anyone), If I know that I will be compensated for any harm I might suffer as a result of making my report, If I know that it will make a difference to those affected by the wrongdoing, If I know that my organization will act on my report, If I receive a financial reward for making a report, There are no enabling factors for me to report wrongdoing]	[46]
MC3	As an IT professional which of the following barriers would prevent you from reporting wrongdoing related to software? (Choose all relevant answers)	[Concern I could lose my job, Concern for my future career prospects, Concern that my report will make no difference, Concern that colleagues could lose their jobs, Concern I would be isolated by my colleagues, Difficulty to prove the threat or harm, Do not know how or where to report, Fear of financial consequences, Fear of legal consequences, It would be an act of disloyalty, Negative attitudes towards people reporting wrongdoing, There are no barriers for me to report wrongdoing]	[46], [47]
MC7	What obstacles would prevent you from using the current reporting procedures/mechanisms in your organization? (Choose all relevant answers)	[I am not confident that the current procedures/mechanisms will resolve the issue, Reporting may result in retaliation against me, Process may not be anonymous (i.e., my identity would be shared), Process may not be confidential (i.e., I shared my name with management or investigators and they shared my identity with anyone else), Procedures/mechanisms are not clear to me, No obstacles preventing me from using the current reporting mechanisms or procedures]	[47], [48]
MC9	In case you became aware of wrongdoing related to software in your workplace and you did not take action, what was the reason? (Choose all relevant answers)	[I decided the breach was not serious enough for me to report, I did not know who to address or where to report, I knew there would be no adequate response from my organization, I think reporting wrongdoing is not right, I wanted to protect the person who was committing the wrongdoing, I was afraid of legal or financial consequences against myself, I was afraid that my relationship with the management would be ruined, Such violations are usual practice in the organization I am employed at, The victim of the wrongdoing did not want me to report it, I did take action]	[47], [50]
MC10	In case you became aware of wrongdoing related to software in your workplace and you did take action, how did you act? (Choose all relevant answers)	[I informally addressed the wrongdoing to coworkers or management (e.g., at the weekly status meeting or at the coffee machine), I spoke directly to the person who committed the wrongdoing, I reported formally within the organization via an official channel (e.g., email, hotline, web-based system), I reported formally to a regulator outside the organization via an official channel (e.g., email, hotline, web-based system), I reported to journalists or news organizations, I reported directly to the general public, via the internet, Twitter, Facebook, or on online blogs, I did not take action]	[20], [50]
MC11	What was the reaction of your organization?	[The situation has been corrected, The organization did nothing, The action is still being processed, The organization took action against me, Not applicable]	[49]
OQ1	Any comments you would like to add?		

Table I: Survey questions per RQ (numbered in order of appearance in distributed survey).

ipants differed among genders, years of experience (in general and in current organization), the organization size and sector (public/private) in which they worked. This variable selection was performed considering existing literature [39].

We analyzed these differences with the Mann-Whitney U-test, for the Likert survey questions. For the multiple-choice survey questions, we used the Chi-square test and Fisher Exact test [53]. For some of the multiple-choice survey questions, answers were collapsed to analyze the data with the Chi-square test. For this step, we for example, put answer options that were only picked by a few respondents under ”other”. This was done to prevent violating the conventional rule of thumb that 80% of all expected values should be greater than five for the test [54]. The questions that could not be analyzed with the Chi-square test were analyzed with the Fisher Exact test.

Since we tested 5 variables for each question—gender, years of experience (in organization and overall), organization size and sector—we consider a statistically significant difference when the p-value is less than 0.01, thus ensuring an overall α of 0.05. While we performed this analysis among all four aforementioned variables, we only report on differences with statistical significance in the next section.

In total, 155 people responded to the survey. Five responses were removed from the survey because they came from

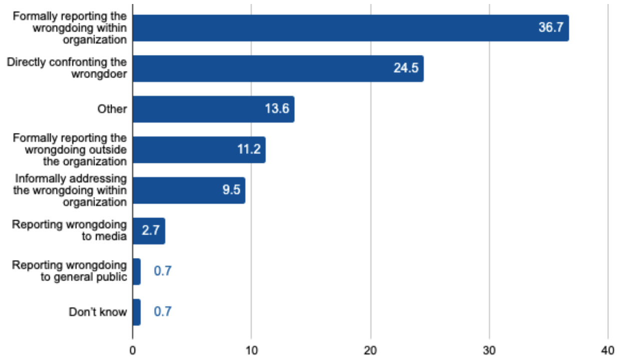


Figure 1: MC1 - Perceived most effective way to stop wrongdoing related to software.

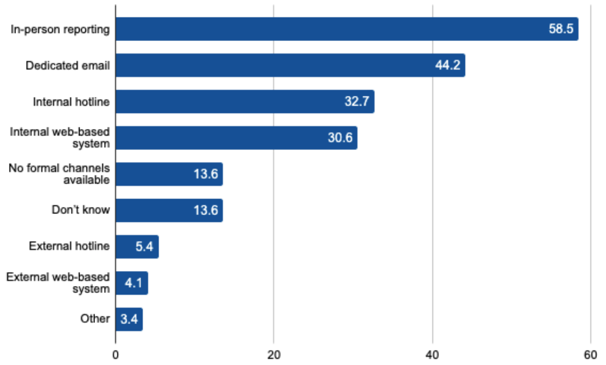


Figure 2: MC5 - Available mechanisms and procedures in the current organization.

individuals who are not *currently* working in software industry. Three more responses were removed because their answers to open-ended questions indicated that they did not fill the survey seriously (e.g., putting in non-informative jokes or meaningless text.) This resulted in a total of 147 responses for our analysis. We received 32 answers to open ended questions, we leave their analysis for the extended version of this paper due to lack of space.

V. Results

We highlight results with statistically significant differences with an * and only report on the statistical tests of these.

A. Demographics

Table II presents an overview of the demographic characteristics of our survey respondents. Noticeable results are highlighted in bold. Most of our respondents are men (86%), between 36 to 45 years of age (33%), with bachelors as their highest education degree (41%), working as software engineers (19%) with less than two years in their current organization (33%) but more than twenty years experience in the field (33%). Most respondents work in the private sector (73%), in organizations with 1001 - 100,000 employees (46%) that are located in Europe (59%).

B. RQ1: General views

Familiarity with legislation (LQ1) regarding whistleblowing strongly varies among software practitioners. Answers are

Demographics	#	%
IT role/position		
Software engineer	**28**	19%
IT manager	17	12%
Consultants	13	9%
Project managers	10	7%
Others	79	54%
Gender		
Women	17	12%
Men	**126**	86%
Did not disclose	4	3%
Age		
25 or younger	13	9%
26-35	41	28%
36-45	**49**	33%
46-55	28	19%
56-65	16	11%
Education		
High school	27	18%
Bachelors	**60**	41%
Masters	42	29%
Doctorate	10	7%
Other	8	5%
Experience at current organization		
0-2 years	**49**	33%
3-5 years	42	29%
6-10 years	25	17%
more than 10 years	31	21%
Experience as software professional		
0-2 years	14	10%
3-5 years	19	13%
6-10 years	26	18%
11-20 years	40	27%
more than 20 years	**48**	33%
Industry		
Medical and Healthcare services	17	12%
Education	9	6%
Financial services	13	9%
Industrial and Manufacturing services	9	6%
Public and Social services	11	8%
Media and Creative industry	9	6%
IT products and services	**55**	37%
Other	24	16%
Type of organization		
Private	**108**	74%
Public	39	26%
Organization size		
1 - 9 employees	8	5%
10 - 100 employees	30	20%
101 - 500 employees	21	14%
501 - 1000 employees	10	7%
1001 - 100.000 employees	**67**	46%
more than 100.000 employees	11	8%
Location		
Africa	2	1%
Asia	10	7%
Europe	**87**	59%
Middle East	3	2%
North America	42	29%
Oceania	3	2%

Table II: Respondents' demographic characteristics (n=147).

Possible answer	Percentage
As the first option in any situation	5.4%
Whenever there becomes a specific reason to do so	30.6%
Only as a last resort, if all else fails	49.7%
Never	11.6%
Don't know	2.7%

Table III: MC4 - Respondents perception on reporting wrongdoing to media.

evenly distributed over all answer options, with 19% of all the respondents strongly disagreeing and 14% strongly agreeing that they are familiar with legislation concerning reporting wrongdoing about software. Almost all software practitioners were positive (65% strongly agree, 29% respondents agree) about the *importance of speaking up (LQ2)* when witnessing wrongdoings related to software.

As Figure 1 shows, most participants (37%) consider formally reporting the wrongdoing within the organization via official channels (e.g., email, hotline, web-based system), as the most *effective way to stop wrongdoing (MC1)*. The second most effective way is to directly confront the wrongdoer (25%). Fewer participants consider reporting to regulators outside the organization (12%), and informally addressing wrongdoing to coworkers and management (10%) as the most effective actions. Some practitioners (14%) could not find themselves in the predefined answers and gave custom responses. Most of these answers pointed out that the most effective action depends on the specific situation. For example, one respondent wrote: *"It depends on the software- If it's a large company that has a good image, working internally with them is preferred until I'm sure the bad behavior is intentional. Then, going to regulators or the public is preferable."* None of the software practitioners indicated that there is no effective way to stop wrongdoing

The majority of respondents need strong evidence to *report a wrongdoing to the media (MC4)* (cf. Table III). This is inline with the perception on reporting to the general public; software practitioners do not want to be considered disloyal or bring a bad name to their organization. A small proportion of respondents (12%) would not report to the media at all.

Of the 147 respondents, 22% (33 software practitioners) *witnessed or suspected some form of wrongdoing (MC8)* within their current organization, as opposed to 78% who did not. A vast majority of respondents (61% strongly agree, 23% agree) indicated that it is in the *interest of their organization that they report wrongdoing (LQ3)*. Only 3% of software practitioners disagree and 2% strongly disagree. Most software practitioners (31% agree and 57% strongly agree) *feel personally obliged to report wrongdoing (LQ4)* to someone within their organization. A small percentage of respondents are neutral on the topic (10%), while a handful of software practitioners opposes the idea (0.7% disagrees and 2% strongly disagrees). Figure 3 shows the results for the Likert-scale questions about general views (LQ1, LQ2, LQ3 and LQ4) on whistleblowing.

Finding 1: The majority of software practitioners agree that it is important to speak up against software wrongdoing, prefer reporting within the organization via official channels and do not consider blowing the whistle through media or to the general public as the first option. Almost a quarter of participants have witnessed wrongdoing in their organizations.

C. RQ2: Means of reporting

Most software practitioners (61%) report that they are *aware of the procedures and mechanisms to report wrongdoing (LQ7)* related to software in their organization (see Figure 3). A considerable percentage (20%) neither agreed nor disagreed, showing that some respondents are unsure if they are really aware of reporting means. Moreover, another considerable proportion of respondents (18%) were not aware of current procedures and mechanisms to report wrongdoing.

The majority of software practitioners (59%) would *feel comfortable using current available procedures/mechanisms* (LQ8)* in their organization to report wrongdoing, with 27% being neutral on the topic and 15% (strongly) disagreeing (see Figure 3). Software practitioners having more than ten years of experience (strongly) agreed more (69%) than those with ten or less years of experience as software practitioners (42%). This difference was statistically significant (Mann Whitney: U= 1917.5, p= 0.007).

Figure 2 shows the *availability of different procedures and mechanisms for reporting wrongdoing* (MC5)* in respondents' organizations. In-person reporting (59%), dedicated email address (44%), internal hotline (33%) and internal web-based systems (31%) are the most frequently used means of reporting wrongdoing. Only a very small amount of software practitioners have access to an externally regulated mechanism, being it an external hotline (5%) or an external web-based system (4%). A notable group of software practitioners reported on the absence of formal mechanisms or procedures in their organizations to report wrongdoing related to software (14%) and a group of a similar size (14%) does not know what mechanisms and procedures are present in their organization. For this question, we only tested on organizational characteristics, as personal characteristics do not influence the available mechanisms and procedures in an organization. A statistically significant difference was found in the size of the organization that respondents work for. 23% of software practitioners working in an organization with 1000 or less employees indicate that there are no formal mechanisms or procedures to report wrongdoing related to software. For software practitioners working in an organization with more than 1000 employees, this is 5%. A dedicated email is present in 56% of organizations with more than 1000 employees as opposed to being present in 30% of organizations with 1000 or less employees. An internal web-based system is present in 39% of organizations with more than 1000 employees as opposed to being present in 22% of organizations with 1000 employees or less. The answers among respondents belonging

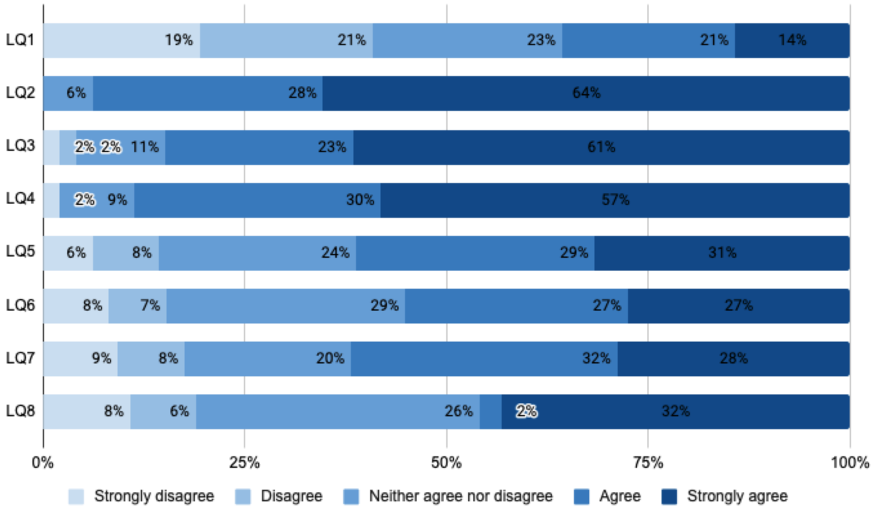


Figure 3: Overview of Likert-scale Questions – General views (LQ1, LQ2, LQ3, LQ4), Means for reporting (LQ7, LQ8) and Enabling and obstructing factors (LQ5, LQ6). Percentages rounded.

to different organization sizes differ significantly (Chi-square: χ^2= 18.65, *df* = 7, *p*= 0.009).

According to our survey participants, it is possible to *anonymously report wrongdoings (MC6)* in 32% of the respondents' organizations and not possible in 31% of the organizations. Moreover, 37% of the respondents do not know if this possibility exists.

Finding 2: Most software practitioners are aware of the procedures and mechanisms for reporting in their organizations. The respondents with more years of experience are found to be significantly more comfortable in using available procedures and mechanisms. The organizations with more than 1000 employees have significantly more explicit mechanisms and procedures for reporting.

D. RQ3: Enabling and obstructing factors

Questions MC9, MC10, and MC11 have only been answered by the 33 software practitioners (22% of the total respondents) who reported witnessing or suspecting wrongdoing within their organization.

The majority of respondents (61%) are *confident that their reports about wrongdoing will lead to action by their organizations* (LQ5)*. Moreover, 25% of the respondents neither agreed nor disagreed with the statement. A small but notable group, 15%, (strongly) disagreed with this statement.

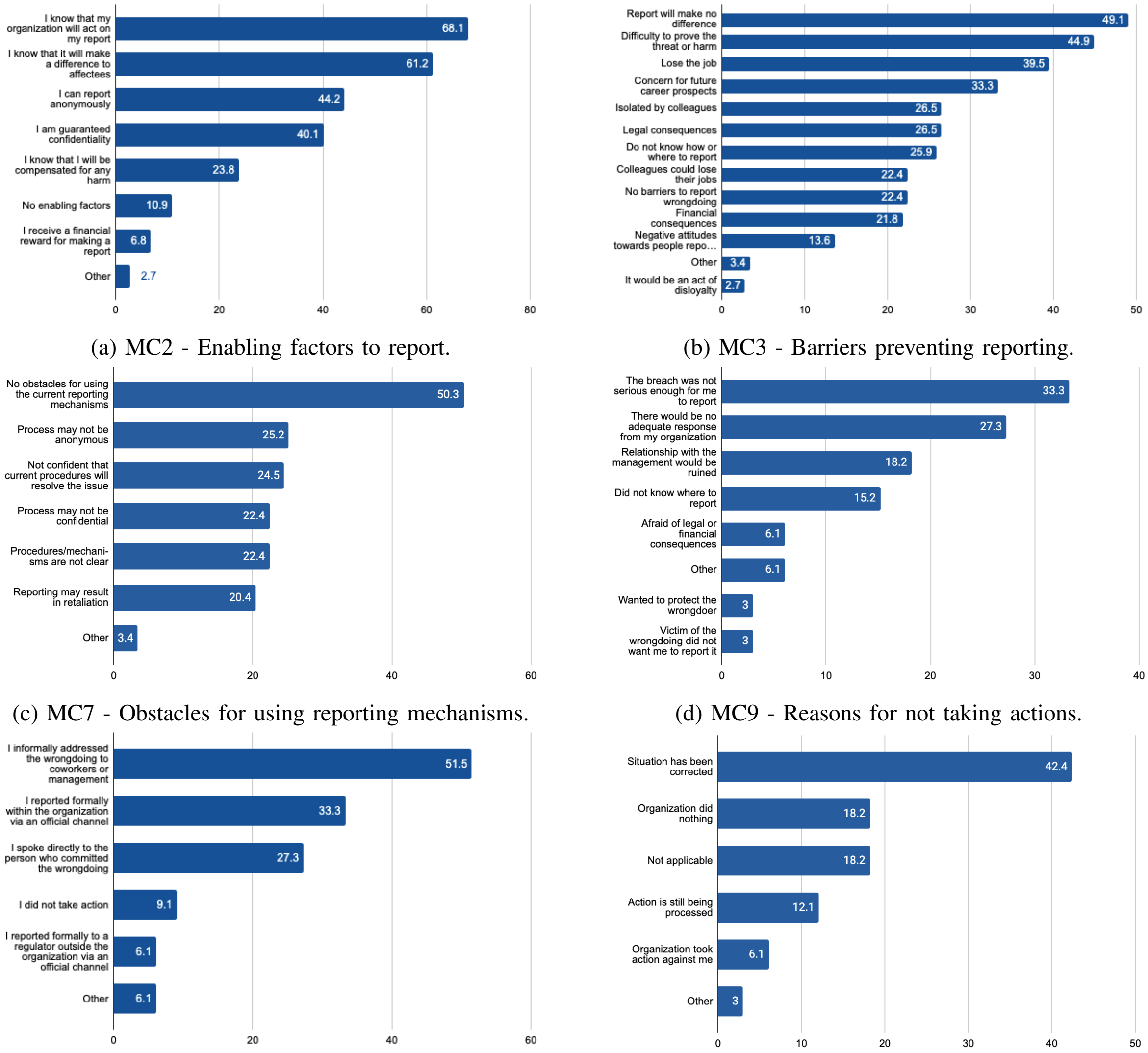
The group of software practitioners having more than ten years of experience (strongly) agreed more (71%) than those with ten years or less experience as software practitioners (46%). The answers between these groups differ significantly (Mann Whitney: *U*= 1875.5, *p*= 0.004).

More than half of the surveyed software practitioners (55%) indicate that *management is serious about protecting people reporting wrongdoing (LQ6)*[3], a small proportion (16%) of practitioners hold the opposite opinion.

Figure 4a shows that for software practitioners the most important *enabling factor to report wrongdoing (MC2)* related to software is knowing that their organization will act on their report (68%) and perceiving that their report would make a difference to those affected by the wrongdoing (61%). Confidentiality (40%) and anonymization (44%) are also important contributing factors. Only 7% of the respondents regard financial rewards for making a report as an enabling factor. However, compensation for any harm resulting from reporting is considerably more important (24%).

Figure 4b shows the *obstructing factors for reporting wrongdoing (MC3)* about software. As shown, responses are quite dispersed over several factors. The obstructing factors for reporting wrongdoings include fear that the report will not make any difference (49%), the difficulty in proving the threat or harm (45%), fear of losing the job (40%), negative impact on future career prospects (33%), isolation by colleagues (27%), unawareness of the means to report wrongdoing related to software (26%), concern that their colleagues would lose their jobs (22%), fear of financial (22%) and legal consequences (22%). Few software practitioners feel that the overall negative attitude towards whistleblowing forms a barrier for them to report (14%). Only a small percentage of software practitioners would not report because they consider reporting an act of disloyalty to their organization or colleagues (3%). Interestingly, a group of respondents also indicated that they have no obstructing factors preventing them from reporting wrongdoing (22%). The majority of the software practitioners feel that they have no *obstacles preventing them from using their organization's current reporting mechanisms and procedures* (MC7)* (50%). The obstacles preventing software prac-

[3] To remove any potential bias, the answers of all software practitioners with managerial roles have been excluded from the analysis of this question.



(a) MC2 - Enabling factors to report.

(b) MC3 - Barriers preventing reporting.

(c) MC7 - Obstacles for using reporting mechanisms.

(d) MC9 - Reasons for not taking actions.

(e) MC10 - Actions taken by software practitioners.

(f) MC11 - Management reaction.

Figure 4: MC questions on enabling and obstructing factors for reporting wrongdoing.

titioners from reporting wrongdoing are quite evenly spread. Noticeably, the mechanisms or procedures to report are unclear to 22% of the respondents. Figure 4c shows the main results of this question. 64% of software practitioners with more than ten years of experience, indicate they have no obstacles preventing them from using the current mechanisms and procedures to report wrongdoing related to software. In contrast, only 30% of practitioners with ten years or less of experience indicate that there is no obstacle which prevents them from making a report. Furthermore, 36% of practitioners with ten years or less experience indicate they are not confident that the current mechanisms and procedures would resolve the issue, while for practitioners with more than ten years of experience, this is 17%. These differences are statistically significant (Chi-square: χ^2= 22, *df* = 6, *p*= 0.001).

With respect to *reasons for not taking action* (MC9)*: Of those who witnessed or suspected wrongdoing in their organization and decided not to take action, 33% thought that the breach was not serious enough for them to report. A large group of respondents (27%) also indicated a lack of trust in whether the organization will take up the matter with seriousness, 18% indicated that they feared their relationship with the management would be ruined, and 15% did not know where to report the wrongdoing. Those with ten or less years of experience indicated more often that they did not take action as they knew their organization would not respond adequately (23%). In contrast, for practitioners with more than ten years of experience, this was an obstructing factor only in 5% of the cases. Of the software practitioners with ten years or less experience, 14% did not take action because they did not know where to address it in their organization. None of the software practitioners with more than ten years of experience selected this as the reason for not taking action. The answers between these groups differ significantly (Fisher Exact, *p*= 0.01).

Out of 33 software practitioners who witnessed wrongdoing in their organizations, 16 *took some action (MC10)* and 17 did not. Figure 4e shows that the software practitioners who took action mostly reported this informally to coworkers or management (52%). Other frequent actions include formally reporting wrongdoing within the organization via an official channel (33%) and speaking to the person who committed the wrongdoing (27%).

With respect to *management reaction (MC11)*, it is encouraging to observe that for 42% of the cases where software practitioners witnessed or suspected wrongdoing in their organization, the situation was corrected. In contrast, in 6% of the cases, the organization took action against the software professional reporting the wrongdoing (see Figure 4f). There was no action in 18% of the cases.

Finding 3: The majority of respondents are confident that management is serious about taking action on reported wrongdoings and protecting reporters. Practitioners are also motivated to report if they know the organization will act on their report and are demotivated by the feeling that their report will make no difference. Practitioners with more years of experience think that they have no obstacles for reporting. Only half of the practitioners that witnessed wrongdoings, took action. Among those that did, most reported internally.

VI. Discussion

Our results show that **(RQ1)** overall software practitioners have a positive view towards whistleblowing, **(RQ2)** current means and channels of reporting in organizations are not supportive enough, and **(RQ3)** software practitioners are mostly motivated to report wrongdoing by the confidence that the concerned organization will take action and demotivated by the feeling that their report will not make any difference.

The vast majority of software practitioners (93%) think that speaking up against software-related wrongdoing is important. An also predominant majority (84%) agreed that it is in the interest of their organization that they speak up. Similarly, the leading majority (88%) agreed that they would feel personally obliged to report wrongdoing within their organization. These might seem like encouraging results. However, a quarter of practitioners reported that they have witnessed or been suspicious of software-related wrongdoing in their current organizations[4] and one out of every five software practitioners indicated that they do not dare to blow the whistle and are unaware of their organization's reporting mechanisms. The comfort of reporting wrongdoings outside the organization or to the media is still extremely low (3%). This is disturbing as recent well known examples of whistleblowing cases [1]–[3] show that when unheard within the concerned organizations, whistleblowing demands the extra courage of reaching out directly to regulators, activists, media or the general public.

While half of the practitioners in our study (∼55%) are aware of mechanisms for reporting wrongdoing in their organization and with using those mechanisms, a still considerable amount (∼15%) do not know which reporting mechanisms are in place. A similar proportion is uncomfortable using the available mechanisms. Moreover, nearly 20% of the respondents are unsure if they are really aware of reporting means. This could indicate that in their organizations, the mechanisms for reporting wrongdoing have not been explicitly discussed. Software practitioners in our study mostly have in-person reporting and a dedicated email address at their disposal. There is very low occurrence of external channels, i.e., an external hotline or an external web-based system. This issue should be addressed as research [19] suggests that when whistleblowing involves external investigations and correction, it is deemed a more effective approach to address wrongdoing and assign the appropriate changes to the concerned organization as opposed to internal whistleblowing. A follow-up study should investigate the effectiveness of different reporting mechanisms in the software industry. Larger-sized organizations (>1000 employees) tend to have internal reporting mechanisms significantly more in place than smaller organizations.

Of the quarter of practitioners that had witnessed or suspected wrongdoing, only half eventually took action and reported the wrongdoing. Less than half of these actions lead to actual responses from the management.

Software practitioners gain confidence and encouragement to report wrongdoings, if the organization takes actions against wrongdoings and facilitates anonymity, confidentiality and future protection. Previous research has shown that anonymity is a good tool for protecting whistleblowers against retaliation [21]. However, anonymous reports may be more difficult to investigate [22].

A statistically significant difference was found for software practitioners with more than ten years of experience in believing that reporting wrongdoing is in favor of their organization, feeling confident that reports will lead to actions, showing comfort in using existing reporting mechanisms and indicating there are no obstructing factors for reporting wrongdoing. Years of work have also shown a positive association with whistleblowing intentions for IT managers [39]. Due to the large number of less experienced software practitioners, it is important to better support them so that they are less vulnerable to the consequences of reporting wrongdoings. In this direction, future research can analyze how to better support less experienced software practitioners and how to motivate and regulate companies, so that they establish official whistleblowing mechanisms and procedures.

Due to the knowledge of the internal procedures and processes of an organization, whistleblowing has historically been proven to be better in detecting wrongdoings and frauds than other mechanisms such as external audits and measurement reviews [55]–[57]. Despite their valuable contributions, whistleblowers are often called out by the society as traitors or snitches. In our study, software practitioners reported being obstructed from disclosing wrongdoing by fear

[4] This number could be higher for previous organizations as it could be a potential reason for them to leave.

of being ignored, perpetual job loss, financial instability and legal consequences. Unfortunately, these fears are not unreal or self-created—71% of whistleblowers face some form of consequences which includes being fired, harassed, threatened, demoted, or suspended [41]. This makes choosing to become a whistleblower an uphill battle, as evidenced by the open-ended answers of some respondents: *"I took action, I paid the price. The wrongdoers live happily ever after."*, similarly, another mentioned: *The person who reports it gets punished. The wrongdoer never does.* Primarily, it is the responsibility of organizations to provide trustworthy mechanisms to their employees for reporting wrongdoing and to react without retaliation. If unheard by internal or external official channels, software practitioners should take additional steps, such as reporting to public media or activists. These steps are not easy ones to take as repercussions are often strong. It is therefore important, that as a software engineering community we support, encourage and protect whistleblowers as they contribute to a safer and healthier society.

VII. Threats to validity

A large threat in our study is self-selection bias. The topic of whistleblowing is still controversial, so people with strong opinions could be more likely to respond the survey and skew the results. We addressed this threat by replacing the term "whistleblowing" with "reporting wrongdoing" throughout the questions and introductory text of the survey. This term was chosen as it embodies the act of whistleblowing but does not carry the stigma that whistleblowing entails. With this change we aimed to enhance the participation of software professionals in the survey.

We distributed our survey online. In this setting, respondents could misinterpret questions and give inaccurate answers. To ensure that questions were clear and misunderstandings were reduced, we held a trial run with 5 graduate students in Computer Science related fields. Additionally, to make sure that questions and answer options were as neutral as possible, we considered related surveys from previous work—reducing the threat of biasing respondents through our used language.

We collected 147 responses in our study. The survey respondents were mainly men and located in Europe and North America. Due to the size and demographics of our respondents, we cannot claim that the survey participants are representative of the whole software industry. This study serves as a starting point to capture the general views of software practitioners about whistleblowing. Additional research is needed to understand in depth the motivations, barriers and support/retaliation received by whistleblowers in the software industry. Further studies with larger and representative populations, and other data collection methods e.g., interviews and focus groups can complement the current study to gain a more comprehensive understanding of the topic. In this direction, we have already mined communication of twitter users to investigate the general public sentiment about whistleblowing in tech [42].

The survey partially consists of statements for which respondents gave answers based on a five-point Likert scale. A limitation of this choice is that respondents might avoid giving extreme ratings and go for answers that are more centrally located. This central tendency bias can skew the data [58].

We analyzed if our results varied among genders, years of experience working in the software industry and in respondents' current company, organization size and type of organization (public/private). Other personal or organizational characteristics may influence the view of software professionals or organization's reporting mechanisms, for example. This could include variables like age, education, specific industry, organization's location and team size. Future work could study the influence of these variables as it was impossible to do so in this study because the distributions of these variables were too dispersed.

A limitation of this study is that it assumes that wrongdoing related to software should always be reported to someone else. However, it could also be possible that a practitioner witnesses wrongdoing in software and fixes it themselves without notifying anybody. The assumption made for this study is that software-related wrongdoing is not completely solvable alone by the software practitioner who witnesses or suspects it.

Respondents were partially asked to answer questions on behalf of their organization, such as what kind of reporting mechanisms and procedures are available to them. It is possible that respondents of the survey are not familiar with all reporting mechanisms due to their shorter work experience in their organization or its larger size.

Whistleblowing can be a sensitive topic for many. To encourage more respondents to fill out the survey and mitigate the threat of desirability bias, respondents filled out the survey anonymously. By offering anonymity, we expect that respondents were more comfortable answering the questions regarding their work environment and sharing their views on whistleblowing in the software industry.

VIII. Conclusion

Whistleblowing has emerged as a powerful form to unveil serious wrongdoings in the software industry in the last fifteen years. We report on the current environment for whistleblowing in the software industry by surveying 147 software practitioners. Our study shows that despite positive views from software practitioners about whistleblowing in general, about 1/4 of the surveyed practitioners have witnessed or suspected wrongdoing in their organization and only half of those has reported the (eventual) wrongdoing. More experienced software practitioners are significantly more willing to report wrongdoings, are more confident about existing reporting mechanisms in their organizations and believe that their report will lead to some action more frequently than practitioners with less experience. In this context, our study can be seen as exploratory and preliminary work, which draws attention to the need for a more encouraging and supportive environment for whistleblowing in the software community.

References

[1] C. Wylie, “How i helped hack democracy,” 2019. [Online]. Available: https://nymag.com/intelligencer/2019/10/book-excerpt-mindf-ck-by-christopher-wylie.html

[2] Z. C., M. J., S. F., and L. C., “Twitter whistleblower says security holes cause ‘real harm to real people’,” 2022. [Online]. Available: https://www.washingtonpost.com/technology/2022/09/13/twitter-whistleblower-peiter-zatko-testifies/

[3] S. D. Wells G., Horwitz J., “The facebook files: A wall street journal investigation,” 2021. [Online]. Available: https://www.wsj.com/articles/the-facebook-files-11631713039

[4] D. Birsch, “Moral responsibility for harm caused by computer system failures,” *Ethics and Information Technology*, vol. 6, pp. 233–245, 2004.

[5] ACFE, “Report to the nations: 2018 global study on occupational fraud and abuse,” 2018. [Online]. Available: https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf

[6] ACCA, “Effective speak-up arrangements for whistle-blowers a multi-case study on the role of responsiveness, trust and culture,” 2016. [Online]. Available: https://www.accaglobal.com/lk/en/technical-activities/technical-resources-search/2016/may/effective-speak-up-arrangements-for-whistle-blowers1.html

[7] S. Dawson, “Whistleblowing: A broad definition and some issues for australia,” 2000.

[8] M. Kaptein, “From inaction to external whistleblowing: The influence of the ethical culture of organizations on employee responses to observed wrongdoing,” *Journal of Business Ethics*, vol. 98, no. 3, pp. 513–530, 2011.

[9] K. Kenny and M. Fotaki, “The costs and labour of whistleblowing: Bodily vulnerability and post-disclosure survival,” *Journal of Business Ethics*, 12 2021.

[10] M. V. Portfliet and K. Kenny, “Whistleblowing advocacy: Solidarity and fascinance,” *Organization*, vol. 29, pp. 345–366, 2022.

[11] A. H. Pulungan, K. J. A. T. Sari, S. Maharsi, and A. Hasudungan, “Authentic leadership and whistleblowing: The mediating roles of trust and moral courage,” *Jurnal Kajian Akuntansi*, vol. 5, pp. 2579–9975, 2021.

[12] L. Hunt and M. A. Ferrario, “A review of how whistleblowing is studied in software engineering, and the implications for research and practice,” in *Proceedings of the 2022 ACM/IEEE 44th International Conference on Software Engineering: Software Engineering in Society*, 2022, pp. 12–23.

[13] ACM, “Acm code of ethics and professional conduct,” 2018. [Online]. Available: https://www.acm.org/code-of-ethics

[14] I. O. for Standardization, “Systems and software engineering: Software life cycle processes,” 2017.

[15] K. Hao, “We read the paper that forced timnit gebru out of google. here’s what it says.” *MIT Technology Review*, 2020. [Online]. Available: https://www.technologyreview.com/2020/12/04/1013294/google-ai-ethics-research-paper-forced-out-timnit-gebru/

[16] B. Perrigo, “Inside frances haugen’s decision to take on facebook,” 2021. [Online]. Available: https://time.com/6121931/frances-haugen-facebook-whistleblower-profile/

[17] H. Park, J. Blenkinsopp, M. K. Oktem, and U. Omurgonulsen, “Cultural orientation and attitudes toward different forms of whistleblowing: A comparison of south korea, turkey, and the u.k.” *Journal of Business Ethics*, vol. 82, pp. 929–939, 2008.

[18] M. P. Miceli and J. P. Near, “The relationships among beliefs, organizational position, and whistle-blowing status: A discriminant analysis,” *The Academy of Management Journal*, vol. 27, pp. 687–705, 1984.

[19] T. M. Dworkin and M. S. Baucus, “Internal vs. external whistleblowers: A comparison of whistleblowering processes,” *Journal of Business Ethics*, vol. 17, pp. 1281–1298, 1998.

[20] transparency international Nederland, “Whistleblowing frameworks 2019, assessing companies in trade, industry, finance, and energy in the netherlands,” 2019. [Online]. Available: https://www.transparency.nl/wp-content/uploads/2020/05/Whistleblowing-Frameworks-2019-TI-NL.pdf

[21] R. G. Thomas, “Whistleblowing and power: A network perspective,” *Business Ethics*, vol. 29, pp. 842–855, 10 2020.

[22] J. P. Near and M. P. Miceli, “Effective whistle-blowing, academy of management,” *The Academy of Management Review*, vol. 20, pp. 679–708, 1995.

[23] F. Pangestu and D. K. Rahajeng, “The effect of power distance, moral intensity, and professional commitment on whistleblowing decisions,” *Journal of Indonesian Economy and Business*, vol. 35, pp. 144–162, 2020.

[24] D. Nurdianawati and R. Rachmawati, “The effect of moral intensity, ethical decision making, professional commitment, and anticipatory socialization on whistleblowing intention,” *Proceedings of the 6th Annual International Conference on Management Research (AICMaR 2019)*, pp. 195–201, 2020.

[25] T. Nyreröd and G. Spagnolo, “Myths and numbers on whistleblower rewards,” *Regulation and Governance*, vol. 15, pp. 82–97, 2021.

[26] J. V. Butler, D. S., and G. Spagnolo, “Motivating whistleblowers,” *Management Science*, vol. 66, pp. 605–621, 2017.

[27] F. B. Deringer, “Whistleblowing in the spotlight; worrying signs for speak-up culture,” 2020. [Online]. Available: https://www.freshfields.com/49bbe1/globalassets/imported/documents/cec04aa0-7813-4318-bb5c-cfcca86f66e5.pdf

[28] J. Zhang, R. Chiu, and L. Wei, “Decision-making process of internal whistleblowing behavior in china: Empirical evidence and implications,” *Journal of Business Ethics*, vol. 88, pp. 25–41, 2009.

[29] M. P. Miceli and J. P. Near, “An international comparison of the incidence of public sector whistle-blowing and the prediction of retaliation: Australia, norway, and the us,” *Australian Journal of Public Administration*, vol. 72, pp. 433–446, 2013.

[30] D. Finn, “Ethical decision-making in organizations: A management employee organization whistle-blowing model,” *Research on Accounting Ethics*, vol. 1, pp. 291–313, 1995.

[31] R. Goodson, “The adequacy of whistleblower protection: Is the cost to the individual whistleblower too high,” *Hous. Bus. & Tax LJ*, vol. 12, p. 161, 2011.

[32] K. F. Brickey, “From enron to worldcom and beyond: Life and crime after from enron to worldcom and beyond: Life and crime after sarbanes-oxley sarbanes-oxley,” vol. 81, pp. 357–401, 2003.

[33] L. F. Eisenstadt and J. M. Pacella, “Whistleblowers need not apply,” *American Business Law Journal*, vol. 55, no. 4, pp. 665–719, 2018.

[34] W. Vandekerckhove, C. James, and F. West, “Whistleblowing: the inside story-a study of the experiences of 1,000 whistleblowers,” 2013.

[35] M. Keil and D. Robey, “Turning around troubled software projects: An exploratory study of the deescalation of commitment to failing courses of action,” *Journal of Management Information Systems*, vol. 15, pp. 63–87, 1999.

[36] M. Keil and M. Robey, “Blowing the whistle on troubled software projects,” *Communications of the ACM*, vol. 44, pp. 87–93, 2001.

[37] C. W. Park, M. Keil, and J. W. Kim, “The effect of it failure impact and personal morality on it project reporting behavior,” *IEEE Transactions on Engineering Management*, vol. 56, pp. 45–60, 2009.

[38] M. Keil, H. J. Smith, S. Pawlowski, and L. Jin, “’why didn’t somebody tell me?’: Climate, information asymmetry, and bad news about troubled projects,” *The DATABASE for Advances in Information Systems*, vol. 35, pp. 65–84, 2004.

[39] M. Keil, A. Tiwana, R. Sainsbury, and S. Sneha, “Toward a theory of whistleblowing intentions: A benefit-to-cost differential perspective,” *Decision Sciences*, vol. 41, pp. 787–812, 2010.

[40] A. K. Vadera, R. V. Aguilera, and B. B. Caza, “Making sense of whistleblowing’s antecedents: Learning from research on identity and ethics programs.” *Business Ethics Quarterly*, vol. 19, pp. 553–586, 2009.

[41] A. Dey, J. Heese, and G. Pérez-Cavazos, “Cash-for-information whistleblower programs: Effects on whistleblowing and consequences for whistleblowers,” *Journal of accounting research*, vol. 59, pp. 1689–1740, 2021.

[42] L. Duits, I. Kashyap, J. Bekkink, K. Aslam, and E. Guzmán, “Whistleblowing and tech on twitter,” in *20th International Conference on Mining Software Repositories (MSR 2023)*, 2023.

[43] S. Easterbrook, J. Singer, M. Storey, and D. Damian, “Selecting empirical methods for software engineering research,” *In: Shull, F., Singer, J., Sjøberg, D.I.K. (eds) Guide to Advanced Empirical Software Engineering*, pp. 285–311, 2008.

[44] R. C. Council, “Public attitudes to whistleblowing in south east europe,” 2017. [Online]. Available: https://www.rcc.int/pubs/44/public-attitudes-to-whistleblowing-in-south-east-europe--data-analysis\-of-opinion-survey-about-whistleblowing-and-the-protection-of-\whistleblowers

[45] T. I. Ireland, “First national survey on whistleblowing points to positive attitudes but need for action by employers,”

2016. [Online]. Available: https://transparency.ie/news_events/first-national-survey-whistleblowing-points-positive-attitudes-need-\action-employers

[46] ——, “Speak up report 2017,” 2017. [Online]. Available: https://transparency.ie/resources/whistleblowing/speak-report-2017

[47] ICF, “Study on the need for horizontal or further sectorial action at eu level to strengthen the protection of whistleblowers - final report,” 2017. [Online]. Available: https://ec.europa.eu/info/sites/default/files/14_annex_-_icfs_study_whistleblower_report_-_vol_i_-_principal_report.pdf

[48] AccountableNow, “Member accountability and whistleblower survey 2020/21,” 2021. [Online]. Available: https://accountablenow.org/member-accountability-and-whistleblower-survey-2020-21/

[49] T. B. P. Alleyne, W. Charles-Soverall and A. Pierce, “Perceptions, predictors and consequences of whistleblowing among accounting employees in barbados,” *Meditari Accountancy Research*, vol. 25, pp. 241–267, 2017.

[50] institute for development of freedom of information, “Challenges of whistleblowing in georgia; legislation and practice,” 2020. [Online]. Available: https://idfi.ge/en/challenges_of_whistleblowing_in_georgia-legislation_and_practice

[51] A. Joshi, S. Kale, S. Chandel, and D. Pal, “Likert scale: Explored and explained,” *British Journal of Applied Science and Technology*, vol. 7, pp. 396–403, 1 2015.

[52] H. Taherdoost, “What is the best response scale for survey and questionnaire design; review of different lengths of rating scale / attitude scale / likert scale,” *International Journal of Academic Research in Management (IJARM)*, vol. 8, pp. 1–10, 2019.

[53] E. McCrum-Gardner, “Which is the correct statistical test to use?” *British Journal of Oral and Maxillofacial Surgery*, vol. 46, pp. 38–41, 1 2008.

[54] M. L. McHugh, “The chi-square test of independence.” *Biochemia medica*, vol. 23, pp. 143–149, 2013.

[55] D. A. Ritchie, “Investigating the watergate scandal,” *OAH Magazine of History*, vol. 12, no. 4, pp. 49–53, 1998.

[56] T. F. Sterling, *The Enron Scandal*. Nova Publishers, 2002.

[57] M. Azim and M. S. Azam, “Bernard madoff’s’ ponzi scheme’: Fraudulent behaviour and the role of auditors,” *Accountancy Business and the Public interest*, vol. 15, pp. 122–137, 2016.

[58] I. Douven, “A bayesian perspective on likert scales and central tendency,” *Psychonomic Bulletin & Review*, vol. 25, pp. 1203–1211, 2018.