U4 Helpdesk Answer

CMI | U4 ANTI-CORRUPTION RESOURCE CENTRE

TRANSPARENCY INTERNATIONAL
the global coalition against corruption

U4 Helpdesk Answer 2020:4

Overview of whistleblowing software

It can be daunting for anti-corruption agencies looking to set up a secure and anonymous whistleblowing mechanism. Yet there are various open-source and proprietary platforms they can deploy. This Helpdesk Answer lays out core principles and practical considerations for online reporting systems. It also highlights the chief digital threats, along with possible solutions. Open-source mechanisms tend to offer the greatest security for whistleblowers, while propriety software places greater emphasis on usability and integrated case management. Ultimately, organisations should be mindful of the context: their capacity, legal protections for whistleblowers, and the severity of physical and digital threats.

14 April 2020

AUTHOR
Matthew Jenkins (TI)
tihelpdesk@transparency.org

REVIEWED BY
Saul Mullard (U4)
saul.mullard@cmi.no

Marie Terracol (TI)
tihelpdesk@transparency.org

Helpdesk Answers are tailor-made research briefings compiled in ten working days.
The U4 Helpdesk is a free research service run in collaboration with Transparency International.

Query

Please provide an overview of the most common web-based whistleblower systems, exploring their respective advantages and disadvantages in terms of anonymity, security, accessibility, costs and so on. We are particularly interested in systems that would be appropriate for Anti-Corruption Agencies.

Contents

Caveat

The assessment of the corporate providers was based partly on research on publicly available information (predominantly that on their websites), as well as on their input to a questionnaire sent to them.

There is a forthcoming publication entitled *Digital Whistleblowing in Journalism* by Philip di Salvo due to appear in June 2020. Those interested in this topic may find additional relevant information in that book.

MAIN POINTS

- Whistleblowing can act as a crucial check on human rights abuses, corporate malfeasance and corruption. Despite this, many countries lack legal frameworks needed to protect whistleblowers, which deters people from reporting misconduct.
- Anonymity and ease-of-use are particularly important factors in people's decisions whether to come forward with evidence of wrongdoing.
- As such, providers of whistleblowing channels, whether analogue or digital, must make decisions as to the trade-off between security and usability.
- Open source software tends to prioritise security for the whistleblower, whereas many propriety solutions place greater emphasis on usability and case management functionality for compliance teams in client organisations.

Background

In recent years, policymakers have increasingly turned their attention to whistleblower protection as a crucial component of an effective integrity system in both the public and private sectors (G20

2019). Not only can whistleblowing alert relevant authorities to wrongdoing after the fact, but there is growing recognition of its potential as a preventative measure to reduce the costs of corruption to the state, businesses and private individuals.

A 2017 European Commission study, for instance, estimated that the lack of effective whistleblower protection across the European Union costs in the region of €5.8 to €9.6 billion annually in the misuse of public funds in the area of public procurement alone (Rossi, McGuinn and Fernandes 2017). Another study found that in Australia, employee whistleblowing was "the single most important way in which wrongdoing was brought to light in public sector organisations" (Brown 2008).

Nor is this a problem confined to the public sector; the Association of Certified Fraud Examiners (ACFE 2018) estimates that a typical firm loses approximately five percent of its annual revenues to fraud. At the same time, the ACFE found that while a typical fraudulent scheme went undiscovered for an average period of 16 months, over forty percent were eventually uncovered by whistleblower tips, a far higher percentage than any other detection method.1 Moreover, not only were organisations with reporting mechanisms more likely to detect fraud as the result of a tip, but their losses to fraud were 50% smaller than organisations without whistleblowing channels (ACFE 2018). Another study revealed that more than half of reports received via internal whistleblowing systems lead to the detection of "compliance-relevant abuses and misconduct" (Homann 2018).

With this growing emphasis on whistleblowing systems has come a concomitant focus on whether existing channels to blow the whistle on wrongdoing are fit for purpose, particularly when it comes to protecting the whistleblower from possible retaliation.

In addition to traditional reporting channels such as post, email, telephone and ombudspeople, there is a growing market for digital, web-based whistleblowing software intended to improve the efficacy of reporting. In fact, while the literature on whistleblowing tends to encourage organisations to provide a combination of different reporting channels to increase access to potential reporters in a manner suited to their individual needs (HTW Chur 2018), there is growing consensus that digital reporting systems offer clear advantages (EQS 2019a).

Advantages of digital reporting systems

Recent insights from behavioural economics suggest that there are a number of factors that influence an individual's decision whether to blow the whistle, including the perceived relevance, credibility, safety, accessibility and responsiveness of a given whistleblowing channel (Transparency International 2019).

Some of the features of digital whistleblowing platforms such as enhanced protection of identify and accessibility can encourage people to engage with anti-corruption mechanisms by lowering the

[1] The study also found that half of all corruption cases were detected as the result of a tip-off.

perceived cost of using them (Transparency International 2019). Traditional whistleblowing channels can be vulnerable to techniques employed to identify a whistleblower; voice recognition can trace hotline calls, private investigators can use handwriting analysis on anonymous letters, while e-mails can be relatively straightforward to trace (Hussein and Yamanaka, 2017).

While there is general consensus that the most effective means of protecting whistleblowing is ensuring that potential retaliators are not are of their identity, there are differing opinions on the relative merits of whistleblowing mechanisms that preserve *confidentiality* as opposed to allowing *anonymous* reporting (Transparency International 2018).

In confidential systems, only the recipient of the disclosure is aware of the whistleblower's identity, and this recipient must seek the explicit consent from the whistleblower to disclosure their identity. While confidentiality is the minimum requirement of any law that seeks to protect whistleblowers, the protection offered by confidentiality alone is not absolute, and the receiving body should make this clear to potential whistleblowers (Transparency International 2018).

In truly anonymous systems, no-one knows the identity of the whistleblower. The appropriateness of different system will depend on context. Confidential systems are better suited to jurisdictions where whistleblowers are required to disclose their name by law, particularly where the disclosure reveals a criminal offence and the whistleblower may eventually to called to testify as a witness.

Conversely, in countries with weak legal frameworks, low cultural acceptance of whistleblowing and high threat levels to would-be whistleblowers, anonymous reporting systems are preferable. Where anonymous whistleblowers' identities come to light, Transparency International (2018) states that these people should "be granted the same rights and protections as other whistleblowers."

Regardless of whether the intention is to encourage confidential or truly anonymous reporting, online platforms offer advantages over traditional channels. This is because although online platforms are not impervious to attempts to uncover a whistleblower's identity, many providers of digital whistleblowing systems offer software that receives, tracks and processes reports of wrongdoing without collecting data that could be used to identify the reporter. Instead, whistleblowers are typically assigned a personal incident number and password in order to facilitate encrypted access to their case files and allow confidential two-way communication with relevant authorities (EQS 2019a; Süsse 2014). This can be crucial in order to allow investigators – whether internal or external to an organisation – to follow up on initial reports where there is insufficient information for effective investigation, as well as to provide the whistleblower an opportunity to give feedback on how the case is being conducted (Kossow and Dykes 2018).

The possibility to disclosure wrongdoing confidentialy/anonymously is a pivotal feature of any effective whistleblowing system. This is because while whistleblower protection legislation can help stimulate the use of whistleblowing platforms, to date relatively few countries have adopted comprehensive measures to protect whistleblowers from retaliation (Kossow and Dykes 2018). Even where such laws exist, they often only protect whistleblowers who disclose their identity and thus offer no safeguards to anonymous whistleblowers should they be exposed later (The Tor Project 2018).

Therefore, when combined with greater round-the-clock accessibility from any location with an internet connection and local language customisation options, the anonymity guaranteed by many digital whistleblowing systems can tip potential reporters' cost/benefit assessment in favour of reporting wrongdoing they have witnessed.

In addition to lowering the inhibition threshold of potential whistleblowers, digital reporting systems offer a number of backend advantages over analogue channels in terms of improved case management functionality. Firstly, compared to whistleblowing channels that rely on post, email, telephone and ombudspeople, it is comparatively straightforward to ensure that incoming reports take the form of structured data. Web-based platforms can require reporters to provide their input via online forms and questionnaires with narrowly set parameters, which can help filter out spurious reports while ensuring that the information provided is actionable and minimising the risk that the reporter can be identified (EQS 2019a).

As many providers of digital whistleblowing software offer integrated case management options, the structured approach to data collection also simplifies the follow-up process. Generally, all anonymised reports are stored in a secure manner, and access to the whole report or parts thereof can be granted to relevant stakeholders as required to investigate the claims made in the whistleblower's disclosure (EQS 2019a). Moreover, by collating and aggregating anonymised reports, digital reporting systems can also be used to identify patterns and trends, such as where misconduct is prevalent. Some solutions include analytics tools to assist organisations to generate statistics on their whistleblowing reports (Homann 2018).

Growing markets of providers

Recent legislative changes in many jurisdictions have extended the requirement to establish whistleblowing channels to the private sector. This is most notably the case in the European Union, where the Directive on Whistleblower Protection entered force in December 2019. The Directive obliges all public entities[2] and enterprises with more than 50 employees to take measures to establish secure and confidential internal reporting channels, develop procedures to rigorously follow-up on reports of alleged wrongdoing and provide timely feedback to reporters (Official Journal of the European Union. 2019; EQS 2019b; Bacher and Popp 2019).

These kind of legislative reforms in the past few years have been accompanied by a considerable growth in the number and scope of digital whistleblowing platforms on the market, many of which are design to cater to the needs of private companies seeking to comply with their new whistleblowing obligations. These vendors offer packages that range from simply providing access to a secure web platform to an entirely outsourced service that receives, assesses, investigates and follows up on whistleblower reports (G2 2020). A recent comparative study of whistleblowing

[2] Member States can decide not to apply this obligation to municipalities with fewer than 10,000 inhabitants or fewer than 50 workers.

platforms in sport found that there was a great diversity in terms of how whistleblowing platforms are managed (whether they are internal or external to the organisation), the channels through which an informant could make disclosure (website, mobile apps and so on), the respective levels of digital security, and well as how much personal information a whistleblower had to disclose (Leeds Beckett University 2018).

For many organisations in both the private and public sectors looking to adopt digital whistleblowing platforms, the question therefore arises which of the many providers offers the most appropriate solution.

The answer to this question is, however, not straightforward. In general, the most appropriate reporting channel will depend on the legal environment and sector in which an organisation operates, as well as its size and structure.

While digital reporting platforms offer some significant comparative advantages over analogue channels, the decision which whistleblowing system to adopt should not be solely technologically driven. Organisations must consider their likely use cases; a sophisticated cloud-based digital reporting channel is likely to be of little use to a garment manufacturer employing hundreds of staff with limited literacy and little access to the internet. Likewise in contexts where repressive regimes conduct extensive internet surveillance and there is no legal protection for whistleblowers, a flashy web-based solution may initially look attractive. Yet, without robust digital security measures such as end-to-end encryption, such web platforms may have the perverse effect of encouraging whistleblowers to come forward without being able to ensure their anonymity or safety.

Before turning to consider the strengths and weaknesses of some of the major providers of digital reporting systems, it is therefore instructive to consider some of the core principles of an effective whistleblowing system that each potential solution should adhere to, regardless of how technologically advanced it is. Ultimately, technological needs should be defined in line with broader strategic considerations around accessibility and target audience. Moreover, institutional capacity in the areas of data protection and cyber risks should be assessed, including the resource requirements to establish and maintain these systems in the longer term (Transparency International 2016).

Core principles for an effective whistleblowing system

Whistleblowing mechanisms can be designed to facilitate three main types of reporting (UNODC 2020):

- internally within a given organisation,
- externally to regulators, law enforcement or anti-corruption agencies,
- public disclosure, particularly to the media and civil society organisations.

Regardless of its intended function, to be truly effective any whistleblowing mechanism must be aligned with the core principles of accessibility, relevance, credibility, safety and responsiveness (Transparency International 2019).

Accessibility

Prospective reporters should be able access the whistleblowing mechanism without difficulty or financial cost. Whether digital or analogue, whistleblowing channels must be “recognisable, reachable and understandable to people with different literacy levels” (Transparency International 2019). Ideally, each whistleblowing system should provide a range contact options (in-person, telephone, web-based) tailored to the needs of potential reporters. To the extent possible, data collection should be available offline and from remote locations to allow whistleblowers to report in areas with no or limited connectivity.

In terms of digital reporting systems, availability is a key component of accessibility. Uddholm (2016) stresses that the whistleblowing platform must not go offline in the event of system errors or determined denial-of-service attacks.

Usability is equally important. Potential whistleblowers should not be deterred from reporting wrongdoing because the processes is difficult or too technically challenging.

Relevance

Clear guidelines should be available to potential whistleblowers, including: who can submit a report, what rights and protections they are entitled to, how and where disclosures can be made, who has access to the information filed, what possible outcomes can be expected, and which other bodies they can make protected disclosures to. Potential whistleblowers should be advised of the possibility of filing a disclosure anonymously as well as the implications of this and the consequences for follow-up investigations (Transparency International 2016). Furthermore, each channel should provide information clearly stating the mandate of the body receiving the disclosure, specifying which kind of wrongdoing falls within the scope of protected disclosure, and outlining the process involved once a report has been lodged. Finally, bodies in charge of operating internal and external whistleblowing channels should publicly disclose anonymised statistics on the number and outcome of previous whistleblower disclosures, ideally in an open data format (Transparency International 2016).

Credibility

A whistleblowing channel has to be perceived as credible by prospective reporters. Credibility is likely to be higher in the eyes of potential whistleblowers where the mechanism is clearly fully autonomous and operates independently of external pressures, such as those from government or management. In this regard, information on who receives and processes whistleblowers’ disclosures should be made clear. This is vital, as the body charged with investigating whistleblower reports must be widely perceived as independent from the parties implicated in the whistleblower’s disclosure, so the case management system should provide for potential conflicts of interest to be avoided or mitigated (Transparency International 2016). Ensuring that at least two members of staff conduct independent reviews of the whistleblower’s report can help in this regard. A related point is that whistleblowing channels must also be adequately resourced to ensure that they are able to manage the inflow of disclosures and ensure effective follow-up.

In the private sector, many firms have resorted to simply outsourcing these compliance functions to a third party who is made responsible to handle the disclosure, maintain the whistleblower’s anonymity and in some cases to conduct follow-up investigations into the whistleblower’s claims (Hussein and Yamanaka 2017).

Security

Those adopting, implementing and operating whistleblowing channels have a duty of care to whistleblowers, whose needs should be at the centre of any whistleblowing system. Whistleblowers face a range of legal, physical, digital and social risks and a key mitigation measure is to ensure anonymity and/or confidentiality to the maximum possible extent. Data protection is therefore vital; and the following minimum standards should be in place:

- Control who is authorised to access data, establish distinct user roles and permissions, as well as identification and authentication procedures. Data submitted to the system should be immutable in that it is not able to be altered or deleted by any user.
- Implement measures to protect sensitive data from unsolicited access, such as hacks on databases stored in the cloud.
- Establish channels to share sensitive data in a secure fashion, using end-to-end encryption.
- Ensure regular security monitoring through audits, and develop incident management protocols in case of data security breaches, as well as procedures to recover data in case of security failures or mishandling incidents. An insecure application could itself become the host for attacks to compromise users' anonymity and/or confidentiality, as well as the availability of the service (Uddholm 2016).

According to Pfitzmann and Hansen (2010), those receiving whistleblower disclosures should be *unable* to identify the reporter; senders of information should be unobservable when interacting with the whistleblowing system. This is not always possible in practice as certain jurisdictions that require personal identifiers to be recorded when filing a whistleblowing report. Where this is the case, personal information should be split from the actual details of the case and the two elements handled by different agencies, so that one body records the identifying information, while a separate body charged with investigating the complaint receives the report and a dummy identity for the whistleblower.

Where anonymous reporting is either not possible or not desirable, the person handling the report should be aware of the whistleblower's identity to provide protection during the process of investigation to guard against retaliation (Transparency International 2018).

Responsiveness

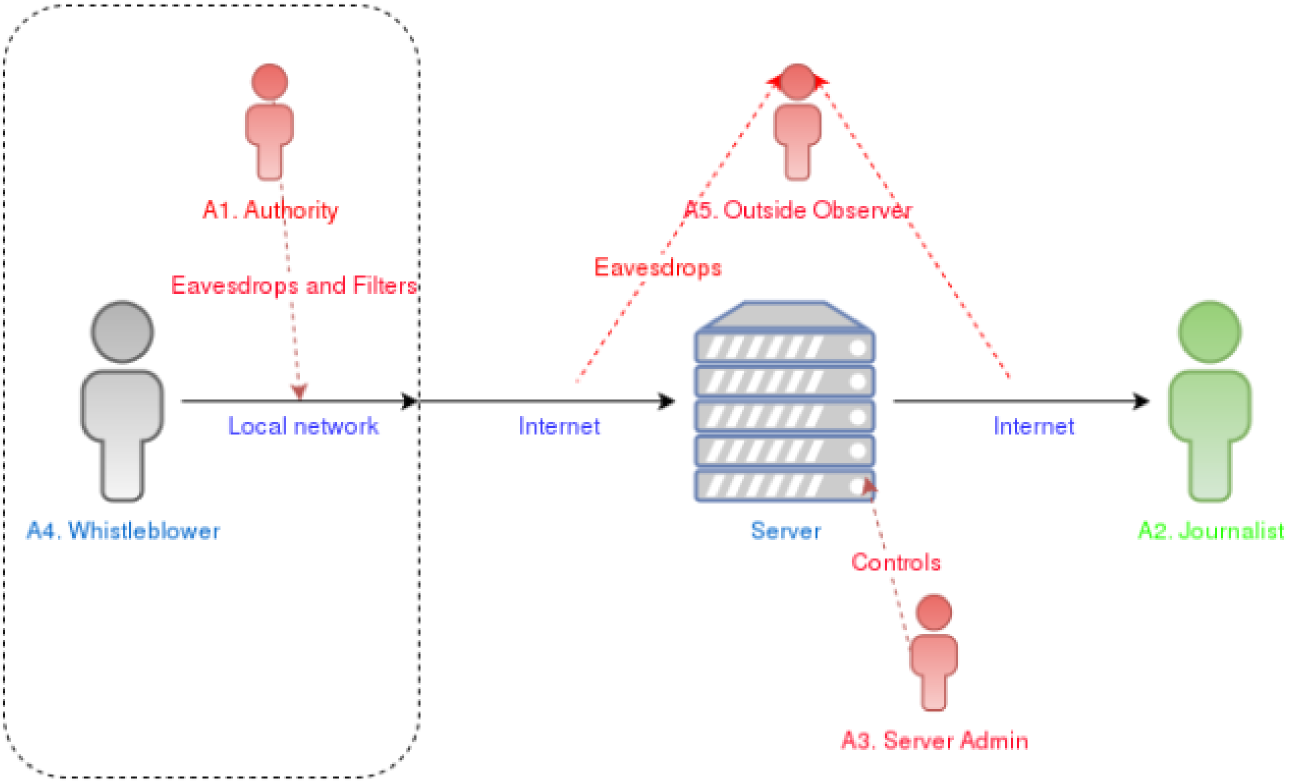
Once secure, encrypted two-way communication has been established between the whistleblower and the relevant authority, timely and forthright updates are important throughout the process so that the reporter can track the progress of the case. This may reduce the chance that the whistleblower escalates their report to other available channels, which could potentially be external to their organisation.

Practical considerations

In addition to these core principles, there are a number of practical functionalities that should feature in whistleblowing solutions that incorporate case management elements. These include the ability to (Transparency International 2016):

- Log all incoming reports with a unique identifier, date of disclosure and a timeline for response. Subsequently, record all relevant follow-up activities, correspondence and findings chronologically in order to track the progress of cases.

- Assess the disclosure against a checklist based on clear, predefined criteria to determine whether the reported wrongdoing falls within the scope of the whistleblowing mechanism.
- Establish two-way secure communication with the whistleblower to acknowledge receipt of the disclosure as soon as possible, and inform them as the case progresses. Where a decision is taken to close the case, this communication channel should be used to provide the whistleblower with a clear rationale for the decision and point them to alternative redress mechanisms where appropriate.
- Handle data in a secure manner, both online and, where relevant, offline information due to be synced to cloud storage.
- Refer cases to other organisational units (compliance, legal, finance) and, where relevant, competent external institutions such as law enforcement bodies.



Establishing a whistleblowing channel that adheres closely to the principles and incorporates the functionalities mentioned above can mean that whistleblowers are more likely to come forward with information about wrongdoing that can harm an organisation, and that the organisation itself can address such issues more efficiently (Transparency International 2016).

Having surveyed the core principles and practical considerations, it is instructive to consider the type of threats web-based whistleblowing systems are exposed to.

Nature of threats to the security of a digital whistleblowing platform

There are range of threats to whistleblower anonymity and/or confidentiality that can stem from one of five main sources in an interaction between a whistleblower and the recipient of a whistleblower's disclosure. These are termed by Uddholm (2016) the authority, the journalist (which could also be understood more broadly as the receiver), the server administrator, outside observers and the whistleblower themselves (see Figure 1).

Figure 1: the threat model (taken from Uddholm 2016)

The authority in control of the network from which the whistleblower connects may have the ability to monitor or interfere in outgoing traffic from that network.

The journalist/receiver may themselves identify whistleblower. This can be taking place unwittingly as a result of inadequate security protocols, as was the case for John McAfree, who was apprehend by police after the metadata in a picture taken by journalists revealed GPS coordinates (Wired 2012). Equally, recipients of whistleblower data may intentionally disclose their identity, as was the case when Adrian Lamo disclosed Chelsea Manning's identity to U.S. authorities (Pilkington 2013).

The administrator of a server may additionally monitor usage of the server to track IP addresses and related information, and may disclose this information to third parties.

Outside observers, such as law enforcement agencies or security services may attempt to hack the system in order to uncover the identity of the whistleblower.

Finally, whistleblowers themselves may be malicious, in the sense that they could submit malware to try to gain access to the system in order to identify other whistleblowers who have used the service or at least read the reports submitted by other whistleblowers.

In terms of the technical nature of the security threats a web-based whistleblowing application faces, some of the most common include an IP leak, DNS leak, URL leak, lookup leak, software usage anonymity leak, HTTP confidentiality and integrity risks, third-part services, server confidentiality and integrity risks, traffic analysis leaks and who-had-access leaks (Uddholm 2016). The assessment of this technical security threats goes beyond the scope of this Helpdesk answer, but a good overview is provided in Uddholm (2016), and individual digital reporting systems should be assessed against all of these threats as part of a security audit.

It is worth noting that the two open source whistleblowing applications covered in this Helpdesk Answer (GlobaLeaks and SecureDrop) have measures in place to address most of these types of security threat (Uddholm 2016).

Criteria to assess and select a suitable digital reporting system

Before turning to an overview of different web-based whistleblowing platforms, it is worth reflecting on a number of preferences for digital reporting systems identified by experts consulted for this Helpdesk answer. The following could be considered as criteria to help select a software solution appropriate to an organisation's needs and use cases.

- Is the software open source or proprietary? If an organisation cannot see the underlying code, it cannot be entirely sure what it is doing.
- Is there a vibrant community developing, updating and patching the software? This is an important consideration when evaluating sustainability and longevity.
- Is the software centrally controlled or delocalised?
- Has the software been subjected to security audits?
- Is the software new on the market or is it an established product? Newer software is more likely to be faulty as it is comparatively untested.
- Is the software an off-the-shelf package or a bespoke solution? Boilerplate software may be more reliable but less sensitive to the specific needs of a given organisation.
- How customisable is the software? For instance, can the data input fields whistleblowers fill in in order to make a disclosure be adjusted to suit different operational contexts?

Overview of providers

Web-based whistleblowing systems can be divided into three broad categories: open source software, for-profit packages marketed at private firms, and custom-built bespoke platforms. The following section provides an overview of the various options, before assessing which would be most suited to the needs of Anti-Corruption Agencies.

Open source software

There are a number of open source software solutions designed to enable anonymous and secure communication between whistleblowers and those they want to inform of wrongdoing. Two of the most prominent are SecureDrop and GlobaLeaks, which share many common features but in practice have served two slightly different use cases. Whereas, SecureDrop focuses primarily on facilitating investigative journalism by bringing new, confidential or otherwise sensitive stories to light, GlobaLeaks has been more broadly applied, including in the field of anti-corruption.3

Although neither exclude the possibility that the whistleblower's disclosure will make it into the public domain, either in its entirety or in part, both are intended to first of all bring wrongdoing to the attention of specific individuals or organisations, be these investigate journalists or public officials.

In addition, to SecureDrop and GlobaLeaks, which both rely on intermediaries between the whistleblower and the broader public to review the disclosure, there are a range of dedicated leaking platforms that operate more in line with the notion of "radical transparency." Radical transparency is the notion that potentially sensitive and compromising information should be available to the public without being first screened and curated by moderators (Gilsinan 2018), which translates into a strategy that critics allege simply amounts to

[3] GlobaLeaks has also been adopted by some media outlets, including by fifteen news organisations in the Netherlands who collectively support an instance of GlobaLeaks call PubLeaks.

"leak, publish, and wait for the inevitable outrage" (Roberts 2012).

Like SecureDrop and GlobaLeaks, these platforms seek to ensure the complete anonymity of the whistleblower. Unlike those options, they seek to ensure that the full, uncensored versions are archived and available for everyone to view online. The most famous of these is WikiLeaks, but there have been numerous spin-offs, with both geographic and thematic focus.4

As these leaking platforms tend to operate on the basis of publishing all information received by default, they are less suited to forming part of a coherent whistleblowing system operated by an organisation. For this reason, this section on open source software concentrates on GlobaLeaks and SecureDrop.

Yet before turning to consider each of them in detail, it is instructive to look at their many shared features and qualities. Both are free, open source projects that offer a secure web interface that whistleblowers, journalists and others can use to communicate. Both systems work primarily over the Tor network, a free and open source software design to enable anonymous communication, and they rely on the anonymity provided by Tor (Uddholm 2016).

Both systems are regularly audited by independent software security companies and publish the findings of these audits, also known as penetration tests (Berret 2016). In response to the results of these tests, both require frequent administration and updates to maintain security (Yawnbox 2016).

Users are not required to register or otherwise disclose information that could be used to identify them. Once a document or other tip has been submitted anonymously, an automatically generated passphrase can be used by the whistleblower to add additional information or look for correspondence from the journalist or other receiver (Schwartz 2020).

Another advantage when it comes to ensuring anonymity is that unlike other messaging apps and whistleblowing channels that may store metadata on servers owned by the messaging system, GlobaLeaks and SecureDrop collect hardly any metadata. What little metadata is collected is itself encrypted and in the case of SecureDrop it is then stored on a server on the organisation's premises, making interception by authorities more difficult (Schwartz 2020).

Overall, the security features of GobaLeaks and SecureDrop mean that most of the technical threats and security risks described earlier that confront whistleblowers are avoided by running either of these applications correctly (Uddholm 2016). A comparative assessment of both systems concluded that whereas SecureDrop was a more appropriate solution for those looking to "defend legally privileged work, or when utmost security is needed", GlobaLeaks was a more viable option for organisations who need "internal auditing and/or whistleblowing platform, a survey/questionnaire platform, or a file submission platform" and does

[4] Geographic: AfriLeaks (Africa), MexicoLeaks (Mexico) SwissWhistleblower (Switzerland), balkanleaks (Balkan countries), MagyarLeaks (Hungary), pirateleaks.cz (Czechia) ,Leakymails (Argentina), RuLeaks (Russia), TunisLeaks (Tunisia), IsraeliLink (Israel), PinoyLeaks (The Phillipines), IndoLeaks (Indonesia).
Thematic: ArtLeaks, UniLeaks.
For further details, see UNODC 2015.

not possess the necessary dedicated technical support to set-up and maintain SecureDrop (Yawnbox 2016).

Nonetheless, as stressed above, technology alone cannot address all of the fraught issues blowing the whistle entails. Both options necessitate careful consideration about the broader legal and policy environment, as well as physical security and organisation use cases and procedures (Yawnbox 2016).

Globaleaks

GlobaLeaks is an increasingly dominant player in the world of open source whistleblowing platforms. Launched as a project in 2012 by the Hermes Center for Transparency and Digital Human Rights, it has been widely adopted by both private and public organisations. Since 2014, GlobaLeaks has been deployed in various anti-corruption projects in order to encourage those aware of corruption to come forward and report it to relevant authorities in a secure and anonymous manner (Kossow and Dykes 2018). GlobaLeaks has been broadly acclaimed as offering users (both whistleblowers and receivers) a good balance of security, usability, and customisation options (Yawnbox 2016).

Security

GlobaLeaks has sought to embed security features in the technological design of the website framework itself, which is written in Python and JavaScript (Uddholm 2016). The platform itself is fully geared to preserving user anonymity, as its design makes it impossible to trace the IP addresses of whistleblowers. Moreover, data ownership is left to the organisation operating the specific instance of GlobaLeaks, and no data transfer occurs between that organisation and the Hermes Center (Kossow and Dykes 2018).

The software encrypts all incoming submissions by default, thereby protecting all elements of the whistleblower's disclosure, from answers to the initial questionnaire, comments, attachments, and related metadata, as well as any eventual correspondence between receiver and whistleblower (GlobaLeaks 2020b). In this way, GlobaLeaks attempts to prevent any instances of plaintext data being stored (Uddholm 2016). Each GlobaLeaks instance includes a default data retention policy that automatically securely deletes submissions after a certain period of time to further minimise the risk of security being compromised (GlobaLeaks 2020a).

GlobaLeaks has been subjected to regular security audits (GitHub 2020a), the most recent of which in 2018 identified no high impact security issues, and one medium impact issue that has since been resolved (GitHub 2020b). Encouragingly, there is evidence of an active community of developers on github dedicated to continuously refining and improving the software (GitHub 2020c).

While an administrator can decide to install their instance of GlobaLeaks in a cloud computing system, observers note that using shared virtual hosting environments can bring additional security and legal risks, as it often means that a third party manages the service (Yawnbox 2016).

Usability

GlobaLeaks is considered easier than SecureDrop for less technical users to operate. It is more straightforward to install (Berret 2016), and the interface itself is more advanced as it permits whistleblowers to choose who should receive their disclosures (Uddholm 2016). The software then encrypts the whistleblower's disclosure using the chosen recipient's keys, meaning the whistleblower has more control over who reads their data than in SecureDrop (Uddholm 2016).

While GlobaLeaks previously operated exclusively on Tor (Uddholm 2016), in 2017 HTTPS was integrated into the platform, making it accessible to many more organisations for whom configuring the Tor browser presented an additional hurdle (Open Technology Fund 2019). The Open Technology Fund notes that using HTTPS can often be less risky that employing Tor to protect anonymity in countries with low internet penetration or advanced surveillance (Open Technology Fund 2019). For its part, GlobaLeaks differentiates between "anonymous submissions" made via Tor and "confidential submissions" made via HTTPs (GlobaLeaks 2020c), and displays a warning to users access the site without using Tor in order to safeguard non-technical users who might not otherwise comprehend the security risks (Uddholm 2016).

Unlike SecureDrop, GlobaLeaks also offers some basic case management functions to record cases and track their status. Recipients can define their own taxonomy for disclosures they have received; by default the system includes New/Open/Closed as submission statuses (GlobaLeaks 2020a). GlobaLeaks reportedly also has the capacity to integrate with other case management systems, such as the one used by Transparency International's Advocacy and Legal Advice Centre network, which is due to operate on SalesForce.

Customisation

Another advantage of GlobaLeaks over SecureDrop is that it is highly adaptable, and each organisation can customise the free, open source software to suit their own needs while receiving technical support from the Hermes Center (Kossow and Dykes 2018; Schwartz 2020). Driven by the concern that "whistleblowing should be as local as possible to give a voice to concerned citizens in their local context" (GlobaLeaks 2020d), each installation can be tailored to suit a specific audience and subject matter by customising the questionnaire into which whistleblowers enter their disclosures (Open Technology Fund 2019). In addition, software has been fully translated into twenty-two different languages (Transifex 2020). Different forms of attachments, from documents to audio and video recordings can be submitted via the platform (SportsLeaks 2020).

GlobaLeaks has been customised by journalists both working with a geographic focus, as is the case in the Netherlands where fifteen news organisations collectively support an instance of GlobaLeaks call PubLeaks (Berret 2016), as well as thematically, such as the journalists running SportLeaks.

Yet the flexibility of the GlobaLeaks system has enabled it to be adopted not only by media outlets and non-governmental organisations but also by public authorities such as the Barcelona City Council and the Italian Anti-Corruption Agency as well as private firms like Edison (GlobaLeaks 2020e). The software is now in operation as places as diverse as Ukraine, Angola, and Madagascar, while the International Criminal Court is using GlobaLeaks to uncover crimes against humanity in the Central African Republic (Open Technology Fund 2019).

Perhaps most notably, GlobaLeaks' recent introduction of a so-called "multitenancy feature" enables the creation of a single platform that provides every public agency with their own bespoke anti-corruption whistleblowing channel

(Open Technology Fund 2019). An Italian initiative, whistleblowing.it, has taken this approach and currently over 600 public institutions have adopted this whistleblowing platform. (Transparency International Italia 2020). The Open Technology Fund, which has funded GlobaLeaks, argues that the "streamlined encryption model and multitenancy capability has resulted in massive, organic scaling" and notes that more than 60% of GlobaLeaks current projects are created by external users without the support of the GlobaLeaks team (Open Technology Fund 2019).

SecureDrop

SecureDrop is an open-source whistleblower submission system that is designed primarily to allow journalists to securely and anonymously receive documents from and communicate with sources. Managed by the Freedom of the Press Foundation since 2013, it is primarily used by media outlets including the *New York Times* and *the Guardian*, though some public accountability organisations such as the Project on Government Oversight and ExposeFacts also run it (Schwartz 2020).

Security

In comparison to GlobaLeaks, SecureDrop emphasises security above usability (Uddholm 2016). The system works using two physical servers, one public server to store, receive and encrypt messages using PGP and a second server to monitor the security of the public server. The public server is a web application coded in Python that is only accessible using Tor, thereby hiding whistleblowers' identities from both the SecureDrop server itself as well as any other (potentially hostile) third-parties (SecureDrop 2020a). The SecureDrop application itself is designed to be part of a larger system architecture, which includes so-called "air-gaps" in which data is physically transferred from a computer linked the SecureDrop application to a "secure viewing station." A secure viewing station is a computer with no access to the internet and no hard drive on which data could be stored. Journalists or other recipients use the secure viewing station to decrypt and read the disclosure, creating an additional layer of security intended to prevent hackers who have gained access to the network from being able to access the data included in the disclosure itself (Uddholm 2016).

In addition, SecureDrop features mandatory two-factor authentication for the journalists in the form of TOTP and uses additional application to further enhance security of the application itself, including GRSecurity, OSSEC, iptables and AppArmor (Uddholm 2016). Like GlobaLeaks, the software is frequently audited by security firms. The most recent audit in 2018 did not find any critical or high-severity issues in the system (Softwerx 2018).

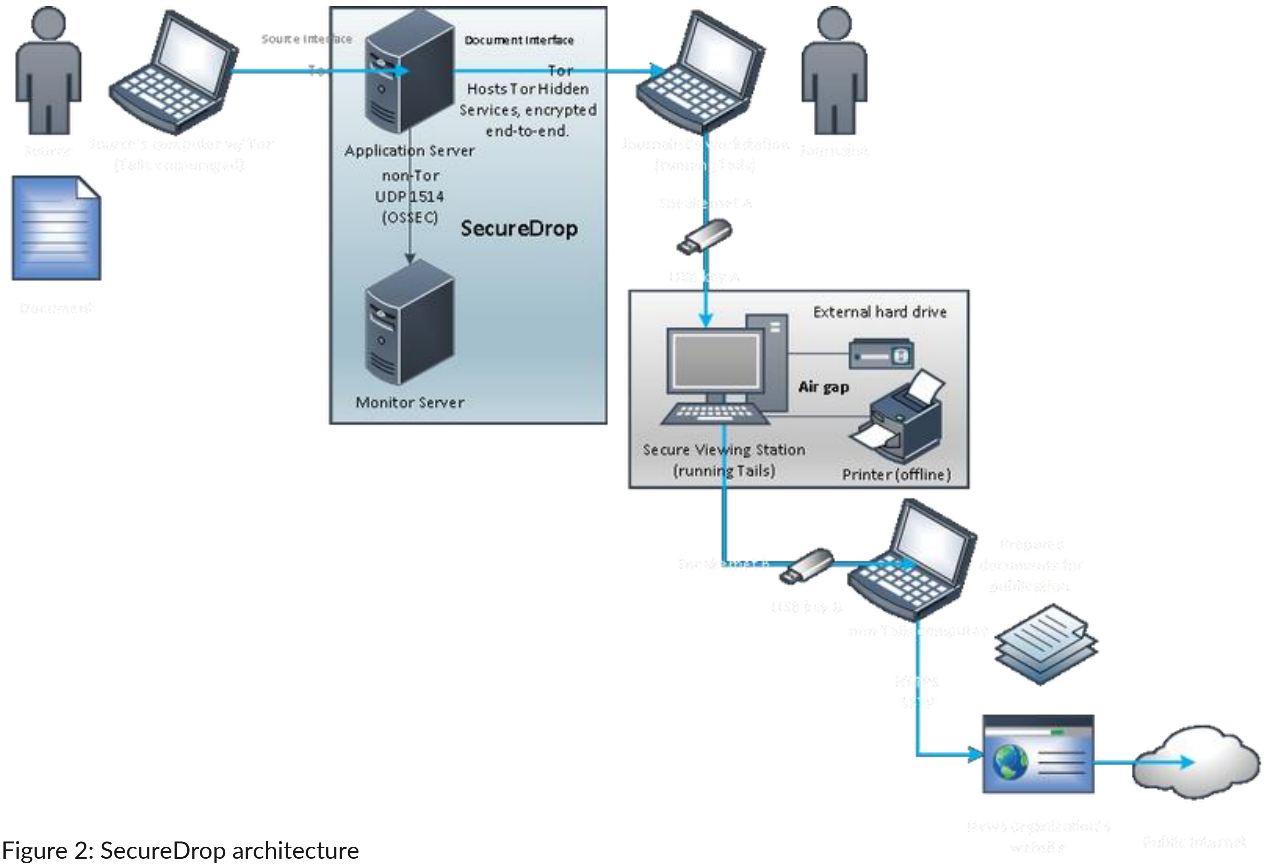


Figure 2: SecureDrop architecture

Usability

Although also available in around twenty languages (SecureDrop 2020b), SecureDrop is more complex to use than GlobaLeaks. Operating the system requires some Linux system administration expertise, and once it has been deployed, only local administration is possible and is command line only (Yawnbox 2016).

Disclosures are less targeted than those made via GlobaLeaks. From the whistleblower side, a user is granted access to a form to upload files and leave a message, but it is not possible to specify which journalist or other recipient should have access to the disclosure (Uddholm 2016).

Recipients such as journalists are then presented with a list of all anonymised sources and their submissions, each of which displays a thread of downloadable messages and files encrypted with GPG. To read the contents of the disclosure, recipients of disclosures are obliged to download each encrypted message separately, then manually transfer it to a secure viewing station in order to decrypt and verify the contents. Observers point out that this process is labour intensive and prone to abuse by spammers (Uddholm 2016). For an organisation that expects to receive large numbers of whistleblower disclosures, this could be an unwieldy or even unmanageable system. Studies of whistleblowing mechanisms run by Anti-Corruption Agencies in Kenya and Indonesia found that they average several thousand submissions per year (Kossow and Dykes 2018).

Corporate

The second category of digital reporting systems are those primarily designed for the private sector, which often feature as part of a broader governance, risk and compliance system (G2 2020). As opposed to the open-source systems offered above, these solutions are proprietary and many of them are intended to be fully-outsourced systems that manage whistleblower disclosure from secure receipt of the initial report to case management and follow-up investigations.

As alluded to above, there has been a rapid growth in the market for these systems to keep pace with the changing regulatory environment in many jurisdictions that increasingly require companies to adopt whistleblowing protection into corporate governance standards and risk management measures (Sillaman and Bernadi 2018). Notably in 2016, the International Standards Organisation introduced a new standard on Anti-Bribery Management Systems that obliges companies to enable anonymous reporting (International Standards Organisation 2020).

Consequentially to meet this growing demand, various vendors have emerged offering differentiated solutions for whistleblowing ethics and reporting management (O'Leary and Pike 2018).

For this Helpdesk answer thirteen private sector providers5 were contacted and asked to complete a self-assessment questionnaire against some criteria developed in consultation with whistleblowing and IT specialists at Transparency International. Not all of the vendors replied, in which case the author of this Helpdesk answer collected as much information as possible in the public domain, chiefly drawing on the companies' own websites.

A review of these providers' solutions found that unlike the two open source solutions mentioned above, many of the corporate providers place less emphasis on security in favour of greater usability.

For instance, a number of providers primarily offered whistleblowing channels such as mobile apps and SMS that are inherently less secure than web-based platforms. In certain contexts they can compromise a whistleblower's anonymity; merely the fact of having the app on one's mobile could be grounds for suspicion. In addition, email addresses are often needed in order to download mobile apps. Thus while vendors of many of the mobile apps are at pains to stress that their software does not itself IP addresses or require personal information to download the app, it often is unclear what security protocols they have put in place to prevent potentially hostile third parties from tracking this information.

In addition, the corporate providers place greater emphasis on integrated case management functionalities than their open source counterparts. However, in order to generate the aggregated statistics and assess trends, data analytics tools rely on data retention, which could constitute both a security risk and a legal risk from a data protection

[5] Alethia, BKMS, Canary Whistleblowing, Convercent, Ethics Global, Ethicontrol, ExpoLink, Got Ethics, People Intouch, RedFlag Group, Whispli, WhistleB and WhistleblowerSecurity

point of view. For this reason, GlobaLeaks includes a default data retention setting that wipes disclosures after fixed period of time.

Moreover, some of these corporate solutions rely on third party services, such as the use of Amazon, Microsoft or IBM cloud computing, or external translation services. Again, this renders whistleblowers' disclosures more vulnerable to interception.

Finally, while a system that provides anonymous means of communication might appear to be secure on the surface, a whistleblower's identity can nonetheless be compromised unless the solution provides clear instructions and protocols for less technical users.

For instance, systems that require a prospective whistleblower to download a specific client or application should first of all communicate clearly that these activities should also be conducted on secure channels, otherwise a user that viewed instructions on how to file a report could be correlated to the disclosure itself due to DNS, IP or URL leaks that reveal when and from where a user viewed this information (Uddholm 2016). This is not always the case with some of the corporate providers.

Custom-built platforms

In addition to the open source and corporate solution, some organisations choose to custom build their own whistleblowing platforms. The World Anti-Doping Agency (2020), for instance, launched its own doping-specific whistleblowing platform, Speak Up!

Whistleblowers to the Speak Up! platform submit their disclosure through a secure online post box through which they can communicate with WADA while remaining anonymous. Although WADA offers advice to help whistleblowers remain anonymous such as filing reports from personal computers, there is little available information about the backend security measures (Leeds Beckett University 2018).

In general, custom-built platforms are likely to only be suitable for large organisations with bountiful resources, or organisations with very specific and niche requirements. While they offer boundless customisation options, they are less likely to be built using tried and tested security protocols, and in the long run are unlikely to prove sustainable.

Suitability for Anti-Corruption Agencies

The reporting of corruption by witnesses, victims and even perpetrators themselves is an important means of promoting transparency, accountability and participation. As such, it is an important means of promoting trust, be this between directors and shareholders in the private sector, or between citizens and government in the public sector (Chansarkar 2020).

As well as being a means of preventing, arresting and remedying wrongdoing, an effective whistleblowing mechanism can be a key part of an anti-corruption agency's arsenal as a way to gather information about the extent and forms of corruption, as well as trends and patterns. Whistleblowing channels can thus complement other accountability mechanisms like social audits, public expenditure and tracking surveys, e-government tools, and service delivery questionnaires (Kossow and Dykes 2018). Yet while these other forms of "crowd-sourced" data about corruption focus chiefly on petty corruption, whistleblowing mechanisms can be better suited to uncovering cases of more serious bureaucratic or political corruption. By producing targeted and detailed information about significant corruption cases, whistleblowing channels can serve as the vital first step in a successful prosecution, and thereby improve vertical accountability between citizens and the state (Chansarkar 2020).

This is recognised in the recent G20 High-Level Principles for the Effective Protection of Whistleblowers, which encourage countries to adopt “diverse, highly visible and easily accessible reporting channels…and extend protection to all eligible persons reporting through those channels” (G20 2019). The Principles also state that G20 should consider ways to enable whistleblowers to “make a report without revealing their own identity while being able to communicate with the recipient of the report” (G20 2019).

The technical demands of setting up a secure and anonymous whistleblowing mechanism can seem daunting. Yet public sector organisations such as anti-corruption agencies do not need to develop their own system from scratch. As illustrated above, there are a number of both open-source and proprietary providers of digital whistleblowing platforms that can be deployed by public agencies.

Organisations looking to adopt web-based whistleblowing systems should be mindful of the broader whistleblowing context, such as the legal protections for whistleblowers, the severity of physical and digital threats, as well as organisational capacity vis a vis the anticipated volume of reports and the relative sophistication of technical infrastructure needed. Chosen solutions should therefore be tailored to local contexts and organisational needs to ensure that whistleblowers are provided with the most useable means to report wrongdoing that simultaneously provides the greatest level of security feasible in order to protect their identity.

This Helpdesk answer has laid out the core principles and practical considerations for online reporting systems, as well as the chief digital threats they face and how various providers’ solutions respond to these threats. Overall, the paper has identified that of the three main types of providers, the open source solutions tend to offer the greatest security for whistleblowers themselves. GlobaLeaks in particular offers itself as a viable solution for public sector organisations like Anti-Corruption Agencies, not least given that it does not charge fees. The increasing adoption of GlobaLeaks by municipal governments and public agencies can therefore be expected to continue (The Tor Project 2018).

The propriety software on the market places greater emphasis on usability and integrated case management functionalities, which offers advantages to organisations looking to improve internal integrity and compliance. This focus on the recipients of whistleblower disclosures is perhaps unsurprising, given that the corporate solutions are marketed at organisations rather than whistleblowers. The fee structure of many of the private sector providers of whistleblowing solutions may complicate their adoption by public sector bodies, as they tend to charge a fixed amount by user or number of employees. It is unclear how they would charge an organisation like an anti-corruption agency, which provides a channel for potentially millions of citizens to file whistleblowing reports.

Limited consideration was given in this Helpdesk answer to custom-built bespoke whistleblowing platforms developed by individual organisations. In general, these are only likely to be suitable for organisations with large resources to dedicate to the system or very niche organisational requirements. It is expected that bespoke platforms are typically less secure and less sustainable than their open source or proprietary counterparts.

References

Association of Certified Fraud Examiners. 2018. *Report to the nations: 2018 global study on occupational fraud and abuse*.

Bacher, P. And Popp, V. 2019. "New standards for whistleblower protection in the upcoming EU directive – practical implications for companies", *International Bar Association.*

Berret, C. 2016. "Guide to SecureDrop", *TOW Centre for Digital Journalism.*

Brown, A. J. 2008. *Whistleblowing in the Australian Public Sector. Enhancing the Theory and Practice of Internal Witness Management in Public Sector Organizations*. Australian National University Press

Canary Whistleblowing. 2020. "Security."

Chansarkar, M. 2020. "Governance and Technologies – Role in Corruption Control", *International Conference on E-Business, E-Management, E-Education and E-Governance.*

Convercent. 2017. *Convercent Ethics Cloud: Security and Business Continuity Overview*.

EQS. 2019a. *Which reporting channels are suitable for your organisation?*

EQS. 2019b. "EU Whistleblower Protection: How to meet the new requirements", *EQS Blog*.

Ethicontrol. 2020a. "Service Privacy Policy."

Ethicontrol. 2020b. "Pricing."

Ethicontrol. 2020c. "FAQ."

Ethics Global. 2020a. "Reporting Channels."

Ethics Global. 2020b. "Ethics Global History."

ExpoLink. 2020. "Protecting Whistleblowing Data."

ExposeIT. 2019. "Whistleblowing Data Protection."

ExposeIT. 2020. "ExposeIT Homepage."

G2. 2020. "Best whistleblowing software."

G20. 2019. "High-Level Principles for the Effective Protection of Whistleblowers".

Gilsinan, K. 2018. "The Radical Evolution of WikiLeaks", *The Atlantic.*

GitHub. 2020a. "GlobaLeaks: Penetration Tests."

GitHub. 2020b. "GlobaLeaks: Security Audit 5: Team Subgraph."

GitHub. 2020c. "GlobaLeaks."

GlobaLeaks. 2020. "Encryption."

GlobaLeaks. 2020. "Homepage."

GlobaLeaks. 2020. "Who uses it?"

GlobaLeaks. 2020a. "Case Management."

GlobaLeaks. 2020c. "Features."

Got Ethics/ 2020. "Security."

Homann, M. 2018. "Do I need a digital whistleblowing system?", *EQS Blog*.

HTW Chur. 2018. *Whistleblowing Report 2018*.

Hussein, M. and Yamanaka, T. 2017. "Whistleblowing at work: Can ICT encourage whistleblowing?".

IntegraCall. 2020a. “Homepage.”

IntegraCall. 2020b. “Security Overview.”

IntegraCall. 2020c. “Products and Services.”

International Standards Organisation. 2020. “ISO 37001: Anti-Bribery Management Systems.”

Kossow, N. and Dykes, V. 2018. *Embracing Digitalisation: How to use ICT to strengthen Anti-Corruption*, GIZ.

Leeds Beckett University. 2018. *Global Whistleblowing Landscape for Reporting Doping in Sport*.

O’Leary, R. and Pike, S. 2018. *IDC Innovators: Whistleblower Ethics and Reporting Management*.

Official Journal of the European Union. 2019. *Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law*.

Open Technology Fund. 2019. “Taking anonymous online: Whistleblowing Global.”

Pfitzmann, A. and Hansen, M. 2010. *A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management*.

Pilkington, E. 2013. “Adrian Lamo on Bradley Manning: ’I knew my actions might cost him his life’.”

Pupic, T. 2019. “Bringing Ethics Back to Business: Alethia”, *Entrepreneur*.

Recurity Labs. 2019. “Continuous Web Application Audit Confirmation of Business Keeper AG’s BKMS Sysyem.”

Roberts, A. 2012. ‘WikiLeaks: the illusion of transparency’, *International Review of Adminstrative Sciences,* vol. 78(1): 116-133.

Rossi, L., McGuinn, J. and Fernandes, M. 2017. *Estimating the economic benefits of whistleblower protection in public procurement*.

Schwartz, T. 2020. *A Public Service: Whistleblowing, Disclosure and Anonymity*, OR Books.

SecureDrop. 2020. “Configuring Localization for the Source Interface and the Journalist Interface.”

SecureDrop. 2020a. “About SecureDrop.”

Sillaman, B. and Bernadi, A. 2018. “Italy steps up whistleblowing regulation”, *The FCPA Blog*.

Sofwerx. 2018. *SecureDrop Security Analysis: Final Report*.

Sportsleaks. 2020. “Homepage.”

Süsse, S. 2014. ‘Whistleblowing - Hinweisgebersysteme als Bestandteil eines effektiven Compliance-Managements’, *Compliance Officer,* pp 195-217.

The Tor Project. 2018. “Italian Anti-Corruption Authority (ANAC) Adopts Onion Services.”

Transifex. 2020. “GlobaLeaks.”

Transparency International Italia. 2020. “Whistleblowing PA.”

Transparency International. 2016. *Complaint Mechanisms: Reference Guide for Good Practices*. Berlin: Transparency International.

Transparency International. 2018. *A best practice guide for whistleblowing legislation*. Berlin: Transparency International.

Transparency International. 2019. *Five Principles for Engaging Citizens in Anti-Corruption Mechanisms*. Berlin: Transparency International.

Uddholm, J. 2016. *Anonymous Javascript Cryptography and Cover Traffic in Whistleblowing Applications*, The Royal Institute of Technology, School of Computer Science and Communication.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. 2019. "Datenschutz-Gütesiegel der Firma Business Keeper AG."

UNODC. 2015. *Resource Guide on Good Practices in the Protection of Reporting Persons*.

UNODC. 2020. "Whistleblowing systems and protections."

Whispli. 2020 "Our Trust Center."

WhistleB. 2020a. "WhistleB Trust Centre."

WhistleB. 2020b. "Whistleblowing software."

WhistleblowerSecurity. 2020a. "Global Ethics Hotline."

WhistleblowerSecurity. 2020b. "FAQ."

WhistleblowerSecurity. 2020c. "Data Privacy and Security."

Wired. 2012. "Oops! did vice just give away john mcafees location with photo metadata?"

World Anti-Doping Agency. 2020. "Speak Up!"

Yawnbox. 2016. "GlobaLeaks and SecureDrop: which is right for you?".

DISCLAIMER

All views in this text are the author(s)' and may differ from the U4 partner agencies' policies.

PARTNER AGENCIES

DFAT (Australia), GIZ/BMZ (Germany), Global Affairs Canada, Ministry for Foreign Affairs of Finland, Danida (Denmark), Sida (Sweden), SDC (Switzerland), Norad (Norway), UK Aid/DFID.

ABOUT U4

The U4 anti-corruption helpdesk is a free research service exclusively for staff from U4 partner agencies. This service is a collaboration between U4 and Transparency International (TI) in Berlin, Germany. Researchers at TI run the helpdesk.

The U4 Anti-Corruption Resource Centre shares research and evidence to help international development actors get sustainable results. The centre is part of Chr. Michelsen Institute (CMI) in Bergen, Norway – a research institute on global development and human rights.

www.U4.no
U4@cmi.no

KEYWORDS

whistleblowing – ICTs

OPEN ACCESS

We apply a Creative Commons licence to our publications: CC BY-NC-ND 4.0.