blueprint for
FREE SPEECH

EXPANDING ANONYMOUS TIPPING TECHNOLOGY IN EUROPE

Authors: Naomi Colvin, Veronika Nad, Chris Culnane, Bruno Galizzi, Dr. Suelette Dreyfus

Design: Ilva Letoja

Co-funded by the
Internal Security Fund
of the European Union

This report has been made possible in part by grants by the European Union's Internal Security Fund - Police, and by the Open Society Initiative for Europe within the Open Society Foundations. Its content represents the views of the authors only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Table of Contents

Chapters

Appendices

1. Executive Summary

The Expanding Anonymous Tipping (EAT) Project was set up with the aim of extending the user base for secure online dropboxes, particularly among private enterprises and public institutions, within 11 southern and eastern European Member States. Nine partner organisations were involved in the Project, which ran from January 2018 to January 2021.

On-the-ground work in those 11 EU Member States produced valuable insights into the factors that lead to organisations adopting secure online dropboxes as a route for public submissions or as part of their own internal compliance mechanisms. A second key element of the project was to expand the knowledge base around dropboxes and how they are used in practice. This final report explains the background to the project and what was achieved over the course of those two years.

In light of our findings, we propose a toolkit for the consistent and privacy-preserving reporting of key metrics, in order to evaluate dropbox outcomes. We anticipate that this will be useful both for future researchers and for organisations who are considering adopting a secure online dropbox solution as part of their requirements under EU Directive 2019/1937 on the protection of persons who report breaches of Union law ("the EU Whistleblower Directive").

The project's nine partner organisation are NGOs with activities in anti-corruption, policy research and advocacy, transparency and right to know, media development, secure technology development, journalism and human rights fields. Through their in-country communities, they sought out organisations from the private and public sectors willing to participate in installing secure digital dropboxes for making disclosures. This required developing a process of how to integrate boxes into different types of institutions, which had varying governance and institutional cultures.

EU countries involved in the project included Hungary (Atlatszo, journalism), Romania (Centru Pentru Journalism), Spain (FIBGAR, human rights), Italy and Malta (The Good Lobby, advocacy), Bulgaria and Croatia (Media Development Center), Czechia (Oživení, right to know) and Greece (Transparency International, anti-corruption). In addition to these key EAT territories, research partner Blueprint for Free Speech has also worked on dropbox adoption and outreach in Cyprus, and Italy's Hermes Foundation provided the disclosure technical platform GlobaLeaks.

This is the first time a project such as this has been tried at scale with secure digital dropboxes anywhere in the world. The bold nature of the project tested boundaries, uncovered surprising hurdles and made discoveries by applying innovative encryption and anonymising technologies in order to make societies more secure. The lessons learned are set out in our recommendations.

The roll out of national whistleblower protection laws across 27 countries over a two year period, to be completed by the end of 2021, is also a bold world-first. It will ultimately transform the integrity systems underpinning the everyday functioning of these societies. We hope the insights from this report will inform and support that transition.

1. Executive Summary

Findings:

The value of dropboxes

Secure online dropboxes produce more whistleblower reports overall. Promotion, a track record of responsiveness to reporting persons and demonstrated commitment on behalf of the dropbox operator all help increase confidence in the system. (Chapter 2)

Dropbox adoption is expanding beyond early adopters in media and media-adjacent organisations. There are important lessons to be learned from the experience of pioneers in public and private institutions in order to ensure wider dissemination. (Chapter 2)

Public authorities who have implemented secure online dropbox systems have found them to be of significant value. (Chapter 4)

The ability to have ongoing communication with a whistleblower is a particularly valued property of secure online dropbox systems. (Chapter 3)

Legal obligations

Legal obligations make a difference to adoption at the point when they become national law. This is particularly the case in countries where whistleblower frameworks do not already exist. (Chapter 2)

National transposition of the EU Whistleblower Directive should support the introduction of anonymous disclosure methods. (Chapter 4)

Governance

Governance issues are a key concern for organisations who are considering implementing secure online dropbox solutions. (Chapter 2)

Lack of clarity about the relation of whistleblowing procedures to other regulatory areas, for instance data protection, inhibits the take up of secure online dropboxes. (Chapter 4)

Authorities should consider providing a how-to guide to assist organisations with implementing internal channels. (Chapter 4)

Freedom of Information procedures may be an example to follow. The forthcoming ISO 37002 may also provide guidance. (Chapter 4)

1. Executive Summary

Usability and security

Dropboxes on their own are not a guarantee of anonymity. Getting the administrative set-up right is important to ensure confidentiality. (Chapter 3)

Dropbox operators should be prepared for users to default to the least secure way of using their channel, even if they intend to stay anonymous. (Chapter 5)

Where an assurance of anonymity is likely to be a major driver of reports, operators should consider giving explicit warnings to users or enforcing use of the Tor Browser in order to access a reporting channel. (Chapter 5)

A suite of technologies may be needed, beyond the secure dropbox. Examples include two-way live chat providing true anonymity and onion services, such as Tor. (Chapter 5)

Safe reporting standards

Dropbox metrics should be reported using differential privacy in order to protect the identity of reporting persons. (Chapter 5)

Particular care should be taken when the absolute number of submissions is small. Reporting trends is preferred over absolute figures. (Chapter 3)

Support for further research

New functionality added to the GlobaLeaks platform should facilitate quantitative research. (Chapter 5)

We have proposed a toolkit for reporting dropbox metrics based on differential privacy. (Chapter 5)

Facilitating access to a secure anonymous messenger from within a dropbox interface would likely improve the quality of submitted reports. (Chapter 5)

Further work is needed to determine best practices and evaluate what educational approaches work best in guiding users toward using Tor. (Chapter 5)

1. Executive Summary

Recommendations:

- Resources should be put toward awareness-building among the the citizenry of EU member states about:
    - whistleblowing,
    - the options of technologically-based anonymity and confidentiality, including digital dropboxes
- Such resources improve security by combating corruption but also improve public awareness of cyber security more generally.They are dual use.

- Develop voluntary standards and accompanying quality assurance labelling that helps consumers make well-informed choices for disclosure options.
    - Consumers in this case may be organisations choosing a service to comply with the new Directive as well as whistleblowers themselves
    - **Open-sourcing** of template technology should be a component of this in order to instill confidence and trust

- Create re-useable blueprints for organisations to adopt in terms of human governance structures behind the technology of the boxes themselves, in order to manage and respond to disclosures
    - Lack of governance structures is a **major gap**, and a **barrier to uptake**.
    - It is also pressing, as new national laws will roll out in 2021
    - The **business and public sectors are not prepared** or indeed, in many cases, even **aware**. Our project partners encountered this **repeatedly across 11 countries**.
    - This is relevant not only to digital dropboxes, but also regarding even the most basic requirements that will be introduced by the Directive.

- Build a central repository of de-identified metadata from such boxes around Europe, to enable accurate study and measurement of impact.
    - This will likely require visible support from the European Commission to be successful. Agencies need ‘permission’ and incentives to share the data.
    - The design should be informed by technical expertise in re-identification of data to protect whistleblowers.
    - The annual output statistics should be open-sourced for the benefit of regulatory, law enforcement, compliance, and research bodies as well as public accountability civil society groups

- Support ongoing development of, and marketing to, the community of free-to-use, **open-source** software that supports the implementation of the EU Directive.
    - This includes dropbox software onion routing services, integrated secure chat and other such programs
    - Collecting these all in one place as a resource for the business and public sector communities across all the member states may be helpful and cost-effective, especially for smaller businesses which will have new compliance costs and a steep learning curve

2. Introduction

Corruption is a tax on society's economic activity. If we are to make a serious attempt at combating corruption, then anonymous tipping is one of the best tools at our disposal, a means both of detecting corrupt practices and of preventing it happening in the first place. (Johanssen & Carey 2015) Whistleblowers often play a critical role in uncovering fraud, mismanagement and waste by revealing information that would otherwise go unnoticed and unreported.

Studies confirm again and again that internal disclosures are an effective means of detecting fraud and are often more effective for this purpose than external auditors. In their 2016 Global Fraud Study, the Association of Certified Fraud Examiners identified tips as the single most effective detection method, while also determining the annual impact of fraud in the cases they examined to be over EUR6 billion. Managers too cite whistleblowing as the “most effective” means of detecting fraud. (Association of Certified Fraud Examiners 2016, Bausa 2016)

Making a disclosure can be a risky enterprise for the whistleblower. Real-world examples of whistleblowers facing retaliation, dismissal or legal sanction for speaking out are all too common, even when whistleblowers use designated reporting channels and procedures. It is not surprising that research studies show that whistleblowers, and particularly those who perceive themselves to be at risk of negative consequences, are more likely to come forward if they can do so without disclosing their identity. (Kenny 2019, Johanssen & Carey 2015, Agers & Kaplan 2005)

The combination of these two elements - facilitating protected disclosures as well as protecting the whistleblowers who come forward - is therefore critical to anti-corruption efforts. As the G20 recognised in their 2019 High Level Principles for the Effective Protection of Whistleblowers, "the risk of corruption is heightened in environments where reporting is not facilitated and protected." (G20 2019)

The EU Whistleblower Directive, which was passed part-way through the EAT Project timeline, provided an essential background to our activities. The way emerging legal obligations interact with organisations’ willingness to adopt dropbox mechanisms is a key theme of this report.

The Directive acknowledges the importance of whistleblowing disclosures to the fight against corruption and fraud, though the scope of the legislation is broader than that, taking in as it does all violations of Union law. While the Directive does not directly mandate the provision of anonymous reporting channels, this is explicitly indicated as an option Member States may wish to legislate for. Blueprint for Free Speech has produced an online tool for evaluating draft national legislation as it appears. (EU Directive 2019; Blueprint for Free Speech 2020)

The evolving practice of anonymous tipping

Technology has made anonymous reporting more accessible than it was in the past. The advent of the secure online dropbox allows whistleblowers to make a disclosure online, which may include the submission of source documents, with reasonable confidence that their identity will not be revealed by the means of transmission. There are of course factors separate from the way information is transmitted that might betray a whistleblower's identity. Some of these are summarised at Appendix G.

2. Introduction

Secure online dropbox systems typically make use of the Tor network in order to obfuscate the digital origin of any material submitted. Some systems are configured to be accessible solely over the Tor network, necessitating the whistleblower to download the Tor Browser Bundle in order to access the dropbox[1]. There is a trade-off here between accessibility and security. Once a submission is received, it is encrypted and passed on to designated recipients.

Secure online dropbox systems typically also enable those making disclosures to continue a discussion with the person on the receiving end of a submission, usually by supplying a password that allows a report to be revisited at a later date. This is a powerful combination of features that is difficult to replicate as securely with other, older forms of anonymous submission, such as by post or telephone.

The secure online dropbox as a technology is less than 15 years old. They were initially developed to enable whistleblowers to disclose sensitive information to media organisations and the public directly[2]. In this they were hugely successful: it is not a coincidence that the public visibility of whistleblowing - and support for the protection of whistleblowers - has increased dramatically since the first appearance of major news stories facilitated by dropbox technology.

In this respect, too, secure online dropboxes have already made a significant contribution to the fight against corruption. Many of the major public interest disclosures of the past 15 years have transformed public understanding of complex issues like money laundering and tax avoidance. In several cases, public authorities have been able to use the information from news stories to launch investigations and take enforcement action. There have, for example, been a series of important journalistic investigations from the International Consortium for Investigative Journalism (ICIJ) and the Organised Crime and Corruption Reporting Project (OCCRP).

Today two established open source systems are available - GlobaLeaks, maintained by EAT partner Hermes (Italy) and SecureDrop (USA), which is maintained by the US-based Freedom of the Press Foundation. Together they are used by a large number of established media organisations and are increasingly being adopted as reporting channels within organisations as well as by public bodies. Commercial integrity systems operated or sold by a number of different entities are also available. One example is the Business Keeper (BKMS) Compliance System, which is developed by a German vendor.

Between them, GlobaLeaks and SecureDrop account for the overwhelming majority of journalistic dropbox instances as well as many others. Keeping track of how many dropboxes are live, and who runs them, can be challenging, as there is ultimately no restriction on who can use and install open source software and closed source applications may not make their client lists public. (Di Salvo 2020: 99) For a list of existing GlobaLeaks and SecureDrop instances, based on current information from Hermes and the Freedom of the Press Foundation see Appendix A.

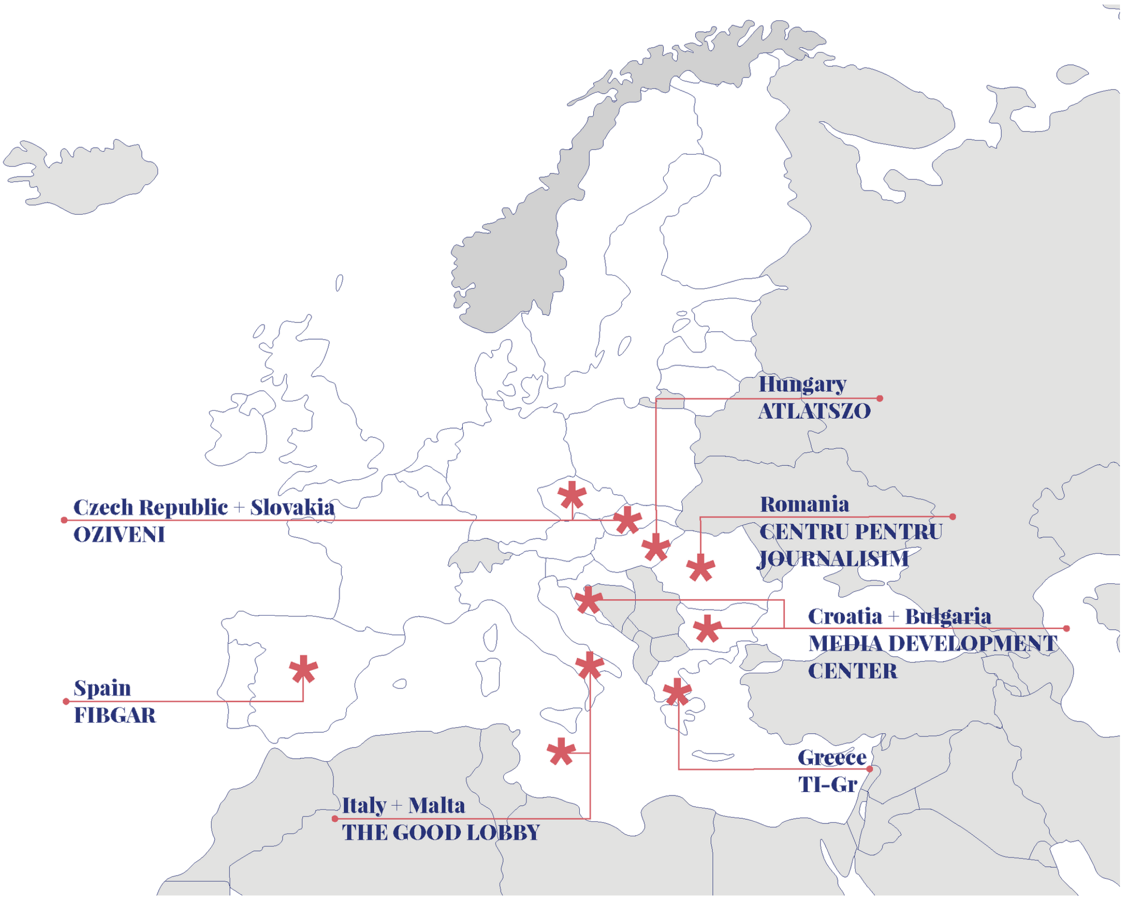
[1] Where this report refers to a dropbox submission "using Tor", this more secure configuration in which the user is obliged to access the dropbox over the Tor network is what is meant.

[2] The WikiLeaks dropbox, generally regarded as the world's first, was launched in 2007.

2. Introduction

Expanding Anonymous Tipping

The EAT project was set up to facilitate the adoption and use of secure dropbox technologies within the 11 EU Member States with the lowest scores on the Transparency International's Corruption Perceptions Index. Many of these countries also lack coherent whistleblower protection frameworks and will be introducing these for the first time with the transposition of the EU Whistleblower Directive into national legislation. The EAT Project countries are Bulgaria, Croatia, Cyprus, Czechia, Greece, Hungary, Italy, Malta, Romania, Slovakia and Spain.



One key goal of EAT has been active dissemination of secure dropbox technologies by partner organisations on the ground, who have the benefit of local knowledge in their respective countries. Along with Hermes, the EAT Partners include Atlatszo, based in Hungary; Romania's Centru Pentru Journalism; Fibgar in Spain; the Good Lobby, based in Italy and also responsible for the project in Malta; Bulgaria's Media Development Center, which has also been approaching beneficiaries in Croatia; Oživení, responsible for Czechia and the Slovak Republic and Transparency International Greece. In addition to these key EAT territories, research partner Blueprint for Free Speech has also worked on dropbox adoption in Cyprus.

2. Introduction

Throughout the life of the project, local partner organisations contacted public and private institutions (hereafter "beneficiaries") encouraging adoption of secure dropbox technology based on GlobaLeaks, supplied and maintained by partner organisation Hermes. EAT partners could also approach media organisations and journalistic organisations in the countries they were working in. EAT dropboxes are hosted on a dedicated disclosers.eu platform, with provision available for extended support beyond the scope of project funding.

While the advent of Covid-19 and the resulting lockdown interrupted the onboarding process for several partner organisations, the EAT project has resulted in the installation of new dropbox instances by public institutions and private companies in Bulgaria, Cyprus, the Czech Republic, Greece, Italy, Romania and Spain. Others are likely to follow once the EU Directive requirements have been transposed into national law. A full list of dropboxes installed as part of the EAT Project, which are active as of 26 January 2021, is given in Appendix C.

Secure online dropboxes and the regulatory environment

Given the passage of the EU Whistleblower Directive in April 2019, part way through the project timeline, compliance with upcoming legal requirements formed part of the offer to potential beneficiaries. Under the terms of the Directive, all entities employing 50 people or more are required to set up reporting channels, as are organisations empowered to receive external reports ("responsible organisations").

Dropbox systems present one way of implementing these channels and have other potential benefits that can help meet other Directive requirements. By keeping track of when submissions are made and acknowledged, as well as how investigations are opened and concluded, dropbox systems can help organisations meet the record keeping and case management requirements of the Directive.

The Directive also has stringent requirements for confidentiality - the anonymity properties of dropbox systems can be useful here, in combination with strong organisational policies about information processing. Confidentiality is key even where submissions may be made anonymously. This is particularly critical in terms of internal channels. In small or medium sized organisations, it may be possible to know who a disclosure has come from to a high degree of confidence even if it is not signed - in such cases, the credibility of whistleblowing processes will depend on a degree of confidentiality being observed by the dropbox operator.

It follows that secure online dropbox systems are not a total solution in themselves. The effectiveness of channels based on dropboxes also depends on the efficiency and integrity of systems on the receiving end and, particularly for external reporting channels, the wider institutional setup.

The experience of EAT partner organisations highlighted the need for clarity in legal requirements. In many instances, organisations were hesitant about adopting technology ahead of national transposition of the Directive - this is particularly the case in countries where transposition will result in the first introduction of whistleblower protection regulations.

Organisations also had concerns, not so much about the installation of the dropbox but about the internal governance and rules that would be necessary to support it. Concerns were expressed about the interaction of whistleblower mechanisms with other regulatory areas, particularly data protection.

2. Introduction

Some organisations expressed a desire that national transposition should bring with it official guidance to clarify exactly what they needed to do to be in compliance. The forthcoming ISO 37002 recommendations on whistleblowing systems have the potential to serve a similar purpose. (Pop 2021)

Regulatory uncertainty hinders adoption

Country E is an EAT Project country where there is currently no existing stand-alone whistleblower protection legislation. A number of municipal authorities engaged with approaches from their local EAT partner organisation and were aware that legal requirements to institute reporting channels were on the horizon.

Despite this interest, the municipalities were reluctant to move forward before the Directive requirements had been transposed into national law. Concerns were expressed about installing a channel with 'informal' status. A completed national transposition was viewed as a kind of authorisation to do something they were unsure about.

Internal governance was also a key concern. One municipality drew an analogy with freedom of information procedures, where they knew exactly what needed to be put into place and how it related to the rest of the organisation. At present, the situation for whistleblower channels was less clear and they did not want to put resources into developing a system that might be superseded by national legislation in the near future.

This anxiety on the part of potentially beneficiary organisations informed our approach for other aspects of the project, which involved some changes from our original plan. Initially the partners in the project had approached expanding secure dropboxes with a view that large organisations could be invited to provide proper secure channels, but if they refused to do so, a GlobaLeaks instance might be set up pointed at, for example, their compliance department's email address for raising concerns. This kind of pressure point might work well for an advocacy group taking an anti-corruption action.

However, as the partners began to engage with possible beneficiary organisations, the situation became much clearer. The business and public agency communities had so little understanding of whistleblowing, let alone secure dropboxes, that there was an enormous amount of education work to be done. Partners found that these communities often could not even agree on a single word, translated into the local language, to describe the activity of whistleblowing. EAT partners spent more time trying to actually explain what a dropbox might do and what whistleblowing was as an integrity system than they were able to spend trying to negotiate agreements to bring beneficiaries on board to the project at no costs to themselves.

2. Introduction

Some potential beneficiaries had no idea legislation would be coming via national transposition, and some refused to believe it would actually ever be passed. This was echoed by meetings with senior civil servants and even parliamentarians who were also in the dark about passage of the Directive and the timeline for its implementation. The response varied by country.

In the dark

Sometimes it was clear that national policymakers were totally uninformed about whistleblower protection and upcoming legal requirements. They were simply not ready for a discussion about reporting channels.

In one country, an EAT partner had several telephone meetings with the federal civil servant in charge of staff training on anti-corruption and integrity issues. This person had no knowledge of the coming changes, the Directive, whistleblowing or digital dropboxes.

The EAT partner realised that in order to win any department or agency as a beneficiary, we would have to first co-run extensive training sessions with the staff, and this would require a great deal of administrative approval and overhead. It would also likely have needed letters of support from the Commission in order to make it happen.

Exploring Anonymous Tipping

The EAT Project timeframe covered a period where the technology behind dropboxes was maturing and where legal requirements are coming into force. Nevertheless, we have found that adoption cannot be taken for granted. A number of factors should be taken into account.

This report examines a number of these issues in turn.

One key element of the EAT Project has been to expand the knowledge base around secure online dropboxes. Chapter 3 looks at the state of academic knowledge prior to the start of the EAT Project and how that informed our initial research agenda. Many of these insights have been borne out: practical issues around adoption predicted by previous research have been indeed reflected in the experience of EAT partners.

2. Introduction

The research around secure online dropboxes to date has largely relied on qualitative measures, based on interviews, rather than quantitative ones, using metadata derived from the dropbox instances themselves. Nevertheless, the adoption of secure dropbox technology by national and regional agencies, and in particular some pioneering work in Spain, has raised the bar for reporting the dropbox outcomes, which has become necessary both for internal monitoring and external accountability. Accordingly, Chapter 3 raises the need for consistent reporting standards that protect privacy while allowing meaningful comparisons to be made between dropbox instances.

Expanding Anonymous Tipping requires understanding the technology and how it has been used to date. It also requires understanding what arguments most appeal in practice to the public and private organisations who might be persuaded to adopt the dropboxes. Chapter 4 looks at the experience EAT partners had in approaching potential beneficiary organisations in the public and private sector, in particular their attitude to anonymous disclosure. This tends to be a key technical property for those promoting secure online dropboxes but is not necessarily the strongest argument for those they are trying to target.

In order to put our research issues in context we interviewed a varied group of dropbox operators. These included organisations from the anti-fraud, regulatory, media and other areas. We interviewed GlobaLeaks and SecureDrop operators, a group broader than those directly involved in the EAT Project itself, in order to analyse the topic across different types of technology used for the same purpose. Information on interviewees is supplied in Appendix D.

Finally, throughout the project, we have been preparing the ground for better quantitative studies of secure online dropboxes. From the beginning, the intention was that the new dropbox instances that came out of the EAT Project would be capable of producing meaningful comparative data to fill the research gap. Chapter 5 explains how our research questions have resulted in Hermes making changes to ensure that metadata[3] will in future be available within the GlobaLeaks platform, something that will assist dropbox operators and greatly facilitate further research.

In addition to increasing the availability of metadata, there are clearly privacy concerns associated with data submitted via secure online dropboxes that need to be addressed. As useful as standard metrics are likely to be in increasing understanding of the effectiveness of dropboxes in the future, care needs to be taken in reporting them. In Chapter 5 we propose an innovative toolkit based on differential privacy that will allow meaningful comparisons to be made without the risk of identifying individual submissions and exposing dropbox users.

[3] Metadata is information about the submissions made using a particular platform, as opposed to the content of the submissions themselves.

3. Understanding Anonymous Tipping

The existing state of knowledge and the EAT research agenda

Not only has the advent of the secure online dropbox changed the way whistleblowing happens, it has made a fundamental change to the visibility and public perception of whistleblowers. As a result, secure online dropboxes can be said to have contributed to the increased public pressure for whistleblower protections in law. The application of this technology itself is scarcely 15 years old. (Vandekerckhove 2016)

This chapter outlines key developments in the evolution of secure online dropboxes, before going on to look at the central research questions that informed the EAT Project, which were informed by previous work in this area.

Within the relatively short lifetime of secure dropbox technology, it is possible to identify three distinct 'waves' of adoption. While commercial integrity systems had been offered to market since at least 2001, the first generation of dropboxes we have identified were directly inspired by the example of online media organisation WikiLeaks, which pioneered the secure online dropbox in 2007 and came to widespread public attention in 2010 and 2011 as a result of that dropbox system's anonymity properties. Other organisations soon attempted to copy this first mover's innovation. In the absence of externally-developed dropbox systems being available for organisations to adopt, first generation media dropboxes were sometimes hastily put together and their anonymity and security properties did not always survive scrutiny by technologists.

By 2013, the two main open source dropbox systems used today, GlobaLeaks and SecureDrop were available for external organisations to adopt. While the primary users of dropboxes in this second wave were still primarily media organisations and media-adjacent civil society groups, there was a degree of innovation in the collaboration models and workflow adopted by dropbox operators. Organisations found that the dropbox was a flexible technology that could be adapted to meet their particular needs.

The third and final wave of adoption considered here concerns the spread of secure online dropboxes beyond media applications into private companies and public institutions, in particular local government and anti-corruption authorities. This move has partly been prompted by legal changes mandating the introduction of internal channels, as in Italy, but also by public sector innovation supported by civil society, as seen in the Anti Corruption Authorities of Catalunya (Oficina Antifrau de Catalunya or OAC) and Valencia (Agencia Valenciana Antifraude or AVAF).

The expansion of tipping technology beyond journalism and civil society presents new and different issues: internal governance, regulatory compliance and external reporting are areas that have been brought into sharp focus by EAT partners' experience promoting dropboxes on the ground. This is particularly so where private sector bodies have contracted out such channels to external companies. The arms-length nature of such disclosure channels has benefits, such as perceptions of independence and therefore trustworthiness. However technical protections and management of the incoming information are not standardised nor is there any industry 'seal of approval' that those making disclosures and those buying the services can rely upon for quality assurance.

The advent of published metrics by public institutions means that we can start to answer questions about how dropboxes are being used and how effective they are in quantitative as well as qualitative terms. Today we are very much at the start of this process. This chapter outlines the state of existing knowledge on some of these key questions, which have in turn informed the EAT Project research agenda. How the EAT Project intends to make answering these questions easier in the future is dealt with in Chapter 5.

Public support for better whistleblower protections

Recent research shows significant public support for whistleblower protections in EAT project countries.

A national survey undertaken by Blueprint For Free Speech in Spain in collaboration with IPSOS in October 2020 shows that 71% of Spaniards think whistleblowers should be supported instead of punished, even if they disclose information from inside organisations. This support is borne out across age cohorts and social groups.

Another recent survey conducted by EAT project partner Oživení in the Czech Republic showed that 56% of those surveyed had a positive reaction to whistleblowers, but the majority (71%) were not familiar with the concept before it was explained to them. Familiarity with the term whistleblower was strongest among graduates and younger people. (Oživení 2020)

This indicates that awareness among the citizenry still need attention through public knowledge-building. The passage of the EU Directive as actively changing the public perception of whistleblowing, rather just than following it.

First generation dropboxes

Secure online dropboxes were initially developed for the purposes of bringing sensitive disclosures to public attention, leveraging cryptographic methods to provide some assurance that submissions could be made without revealing the sender's identity. In the wake of WikiLeaks' highly visible publications of 2010 and 2011, the potential of this technology was seized on immediately by a number of media and civil society organisations, though this first wave of dropboxes was not always implemented very effectively. (Chen 2011, Sifry 2011, Greenberg 2012)

Al Jazeera and The Wall Street Journal both set up their own dropboxes in 2011, which imitated the WikLeaks idea without replicating its security properties. Both projects were quickly criticised by technologists who saw their security shortcomings. Both were ultimately rather short-lived[4]. Nevertheless, this first wave of dropbox projects did serve as a prompt for others to develop the kind of "off the shelf" technology solution that was clearly needed.

[4] Today both publications run SecureDrop instances

3. Understanding Anonymous Tipping

A very few dropboxes of this era do survive, including German newspaper Die Zeit's Briefkasten system, which was launched in July 2012. This project - "a reasonably secure web application for submitting content anonymously" - is still used by Die Zeit and appears to be actively maintained. The code is open source and auditable.

Slightly more common are journalistic or civil society projects initiated during this era which have moved beyond home-grown or sui generis dropbox systems to adopt systems developed by third parties. Kenya's Ethics and Anti-Corruption Commission dropbox originally dates from 2013 and since 2015 has been based on the BKMS submission system. BalkanLeaks is an example of a "first wave" platform from 2010 that has evolved to reflect best practices in dropbox design. BalkanLeaks adopted SecureDrop in 2013, soon after the system became publicly available. The platform is still online today, operated by the Bulgarian journalistic collective Bivol. (Arnold 2020, Di Salvo 2020: 104)

The early history of secure online dropboxes is part of a broader movement of collaborative research and innovative human rights and journalistic work made newly possible by technology, much of which enabled greater participation in these areas than had been possible previously. Commentators have noted the emerging role of online networks in journalism and human rights work. In some cases, such as India's ipaidabribe.com or Alexei Navalny's Rospil project, projects have become synonymous with broader social and political movements. (Arnold 2020).

GlobaLeaks use cases

3. Understanding Anonymous Tipping

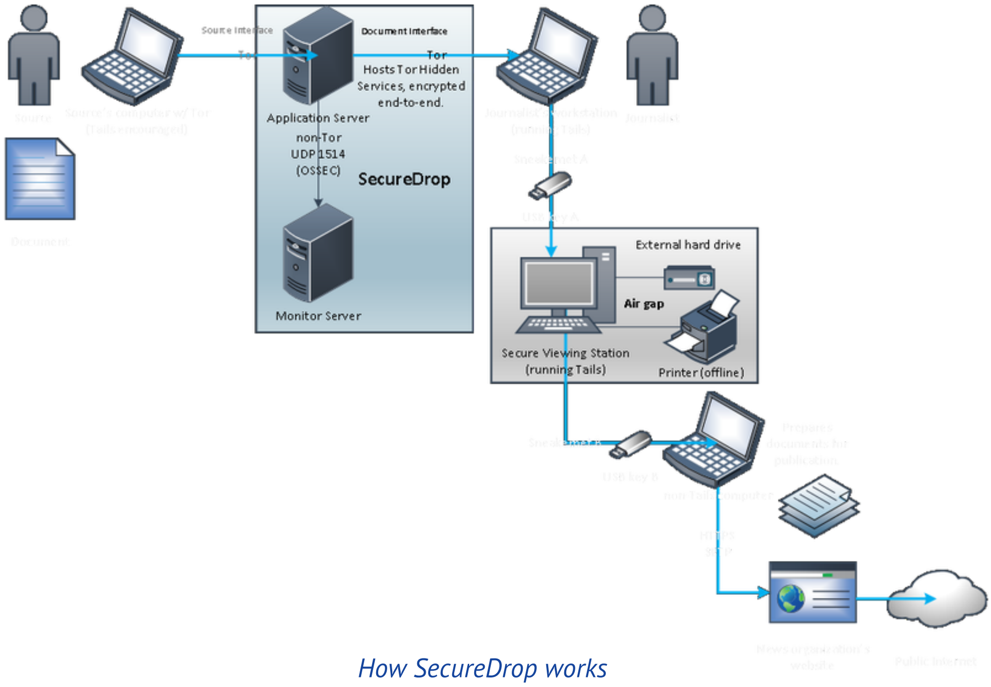
What makes a secure online dropbox secure?

Technical security was an important area of discussion during the ‘first generation’ of dropbox adoption and remains so today. Unfortunately, the security properties of dropboxes is also an issue that is dealt with inconsistently in the research literature.

One study of online whistleblowing systems have defined a whistleblower reporting system as one that “allows users to submit whistleblowing reports anonymously via the internet.” In this sense, anonymity tends to mean more than simply the ability to make a disclosure without a name attached to it. It is inextricably linked to other secure communications technologies that offer a degree of resistance to surveillance. (Lowry, Moody & Galetta 2014: 155, Di Salvo 2020)

In some areas, there is still a wide diversity in the kinds of digital whistleblowing solutions organisations make available. This was the finding of a survey of sports federation and anti-doping agency platforms conducted in 2017, an area that had seen a period of rapid growth as a result of a series of public scandals. The authors of that survey found that the “level of sophistication” in whistleblower channels varied so dramatically - ranging from externally-hosted dropboxes on one hand to supplied email addresses on the other - that it was “difficult to determine what good practice in this context looks like.” (Leeds Beckett University 2018)

There is in fact a greater degree of consensus over what constitutes a “good” secure online dropbox system than this suggests (Bausa 2016, Zafia et al 2017, Palumbo 2017) Today there are two main open source - and therefore auditable - dropbox solutions with slightly different security properties. While both GlobaLeaks and SecureDrop systems utilise Tor, the latter is only accessible to users via the Tor Browser bundle, as opposed to a regular internet browser, while GlobaLeaks allows dropbox operators to set up alternative configurations. The variation in design choices owes much to the anticipated use cases (the “risk model”) adopted by the different projects.



How SecureDrop works

3. Understanding Anonymous Tipping

SecureDrop is designed to cater to high risk applications - the paradigm example being a transnational crime disclosure being made to a major newsroom - while GlobaLeaks is intended to be used in a wider set of situations. Whether potential whistleblowers are obliged to use Tor to access the dropbox as opposed to a normal internet browser, or whether they are able to do so is just one of several differences between the two systems.

Which system to adopt is a decision that will therefore require a needs analysis on the part of the organisation concerned. An account of one such assessment in an Indonesian academic setting described how GlobaLeaks was ultimately preferred over SecureDrop on grounds of “simpler” and less costly arrangements for setup and maintenance. (Zafia et al 2017)

This is echoed by the experience of our own team in training media in cybersecurity to protect their sources. As an example, a major daily newspaper we worked with chose to provide two disclosure avenues, a high-security SecureDrop option and an easier to use lower security option. This was successful, with the majority of the disclosures coming in via the lower security option as it was easier to use. However, the high security option was still there for sources who were worried for their personal safety.

When it isn’t safe to use the high security option

Risk models can be complex and the security profile of SecureDrop means - somewhat counterintuitively - there are environments where it is not safe to use it.

In countries where internet use is monitored, use of the Tor network can mark an individual out as suspicious. In these circumstances, the Freedom of the Press Foundation recommends against the use of SecureDrop and recommends that potential operators, in this case predominantly media organisations, use alternative methods.

3. Understanding Anonymous Tipping

Evolving uses of dropboxes - from civil society and the media to public and private institutions

Beyond these accounts of the first wave of interest in secure online dropbox systems at the start of the decade, some of the most detailed work on the evolving use of dropboxes is the recent study by academic Philip Di Salvo, which examines a group of 21 dropboxes over the course of 2015. By this point, both GlobaLeaks (first prototype of which was made available in 2011) and SecureDrop (publicly released in 2013) were both available to organisations interested in adopting them.

Supporting adoption at around this time was the renewal of interest in privacy enhancing technologies after Edward Snowden's revelations about pervasive online surveillance (Di Salvo 2020: 105). As numerous studies have attested, this major news story increased awareness of the impact of surveillance on investigative journalism generally. Newsrooms have been obliged to integrate privacy enhancing technologies into their day to day practice and, in turn, significant increased effort that has gone into developing accessible tools designed for non-expert users. Signal, the encrypted instant messaging protocol and application, is one of the most successful examples of this. (Blueprint for Free Speech 2018, Wiener 2020)

Di Salvo's study, the first attempt to survey a number of dropbox operators and find points of comparison between them, is essentially aimed at understanding heterogeneity in a relatively young field, where different organisations were trying to understand how to make best use of new technology. Di Salvo limits his study to organisations "with a clear journalistic trait," which at that point accounted for the primary users of the technology. (Di Salvo 2020: 92)

Organisations “with a clear journalistic trait” is a more expansive group than organisations staffed or run by journalists and includes NGOs or activist groups who feed information to journalists or publish news stories based on information passed to them. It includes several EAT partner organisations. However, Di Salvo’s criteria clearly excludes many of the organisations who are targeted EAT beneficiaries and several of those we have interviewed.

The platforms surveyed by Di Salvo included 13 GlobaLeaks dropboxes and 7 based on the SecureDrop platform, with one sui generis system operated by the German newspaper Die Zeit. Not all of those platforms are still active today. Indeed, four of the dropboxes studied by Di Salvo became inactive over the course of the study period (Jan-December 2015). The list of dropboxes surveyed in Di Salvo's study is provided in Appendix B.

The research was based on semi-structured interviews of 30-45 minutes, supplemented by email as well as online and in person conversations. In general, traditional media organisations, constrained by the need to protect their sources, were more reluctant to engage with research, compared to NGOs and advocacy groups. This is reinforced by some policy decisions by dropbox developers themselves - FPF generally discourage users of SecureDrop from discussing submissions, which includes identifying the role of the platform in news stories.

Di Salvo’s interview group included traditional media organisations, journalists’ groups like working cooperatives or unions, NGOs and activists. He noted that, in all the organisations he surveyed, access to reports submitted through the secure online dropbox system was restricted to a relatively small number of people. His key finding was that operators of secure online dropboxes were innovative in the way they situated these channels in their own organisational context and that a number of different working models[5] were possible. (Di Salvo 2020: 128)

In fact, Di Salvo found four main “editorial approaches and strategies” among the platforms he surveyed.

The first he called publishing platforms. These are not traditional journalistic organisations but they publish source documents or their own stories based on documents submitted to them. An example would be EAT partner Atlaszo's MagyarLeaks project.

The second category identified by Di Salvo are the collaborative platforms, which do not release leaks on their own but form a bridge between whistleblowers and journalists. Examples cited in this category include the conservation focused dropbox Wildleaks.

A third category are multi-stakeholder platforms. These draw on specific functionality available through the GlobalLeaks platform that allows those submitting reports to decide which of a selection of recipients should receive the disclosure. These are primarily a technical service and can enable reports to be routed to journalists or researchers working for entirely different organisations. This kind of collaborative endeavour between media organisations is distinctive. Examples of multi-stakeholder platforms still in operation today include Sourcesûre, Publeaks.nl and MexicoLeaks.

Finally, Di Salvo identified a number of media platforms, operated by traditional media organisations for their own in-house purposes. This is the most familiar working model for secure online dropboxes and the majority of SecureDrop installations, which has been tailored for major newsrooms, fit into this category.

Looking beyond the temporal scope of his study, Di Salvo notes that after 2015, working models kept evolving and some individual journalists also launched their own personal dropboxes. These include Jean-Marc Manach in France, Barton Gellman in the US and Stefania Maurizi in italy.

While Di Salvo identified a great deal of innovation in the world of dropbox operators, particularly in terms of collaboration between journalists from different organisations, there is a basic similarity between the organisations he surveyed. In certain important respects, this sets them apart from the private and public institutions targeted as potential beneficiaries in the EAT Project.

News organisations and others who might deal with confidential sources on a similar basis have a particular workflow which is often predefined by existing policies. While the digital age presents challenges for journalists working with sources the general principles that govern such relationships are fairly well developed. One of the lessons of the third wave of dropbox adoption - of which the EAT project is a part - is that regulatory environments and internal policies are key to mainstream adoption. (Blueprint for Free Speech 2018)

[5] In this, Di Salvo draws from Micah Sifry's earlier study of WikiLeaks which described the organisation experimenting with different ways of working; from operating as a kind of source for journalists, to a content producer to a facilitator of journalistic partnerships between other media organisations. (Sifry 2011)

3. Understanding Anonymous Tipping

A third wave of dropbox adoption - from civil society to institutions

At the same time as Di Salvo was surveying secure online dropbox operators, the expansion of secure online dropboxes into public institutions was gathering pace. The momentum for instituting a City of Barcelona dropbox dates from around 2015, when active civil society agitation met with a new, responsive municipal government. The launch of the Barcelona dropbox in partnership with civil society organisation Xnet in January 2017 in turn paved the way for the Antifraud Agencies of Catalonia and Valencia to follow suit in December 2017 and May 2018 respectively. (Change of Direction 2017, Xnet 2017, Beltran 2018)

The spread of secure online dropbox systems into public institutions coincided with the introduction of legal obligations in the financial sector. EU Directive 2015/849 on the prevention of money laundering introduced requirements for a “specific, independent and anonymous” channel for internal reporting. This was the prompt for Germany’s Federal Financial Supervisory Authority (BaFin) establishing their own secure online dropbox. Italy's Law No. 179/2017 has similarly encouraged many public authorities to adopt dropbox systems.

There also were some precedents for Spanish authorities soliciting public reports, though not by means of a secure online dropbox. National agencies including the National Markets and Competition Commission, the Ministry of Labour and Social Security and the Tax Authority had previously solicited reports from the public in some form. (Benitez Palma 2018)

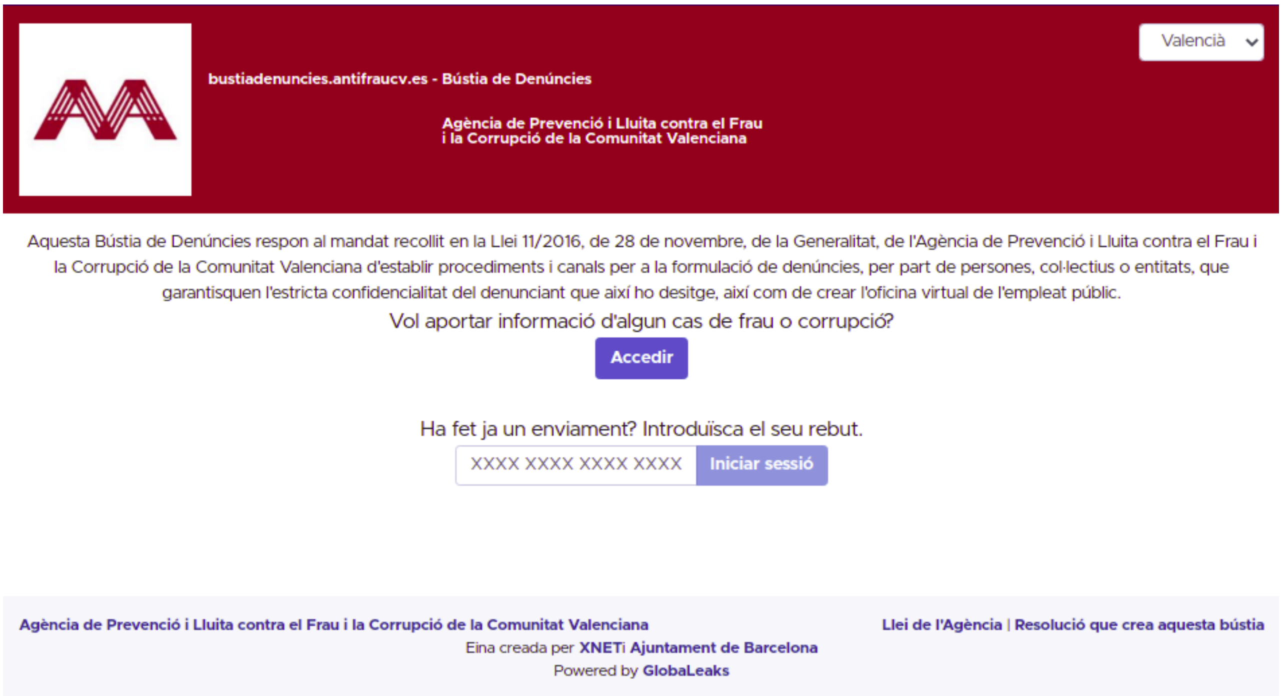
But there was much that was new about what happened in Barcelona. The Director of Analytics at the City of Barcelona has written an account of the development of the City’s secure online dropboxes, which places significant emphasis on the institution-building that had to precede the launch itself. (Sanchez 2019)

Barcelona’s dropbox was envisioned as a route for ordinary members of the public to contact the council with information that corresponds to a broad anti-corruption remit, soliciting reports on issues might impact good governance. An Office for Transparency and Good Governance was set up at the end of 2015. The dropbox, based on GlobaLeaks, went live roughly a year later on 2 January 2017.

In the meantime, a number of committees were set up. Representatives from civil society were invited to participate in an Advisory Council on Transparency, which was set up in 2016. A number of regulations had to be formulated ahead of the launch of the dropbox in order to ensure compliance with data protection standards and other legislation. In 2018, an Ethics Committee with a supervisory role was established in order to settle issues arising from the operation of the dropbox.

The Barcelona experience illustrates how setting up external reporting channels within existing organisations can be more complex than for journalist or activist operated secure dropboxes. Where investigations have the potential to require change in the organisation hosting the dropbox, defining lines of responsibility, complaints and other internal governance procedures are critical. Doing this institutional work from scratch, as happened in Barcelona, required significant organisational investment. In the event, Barcelona’s experience informed adoption by the two regional anti-corruption agencies.

3. Understanding Anonymous Tipping



bustiadenuncies.antifraucv.es - Bústia de Denúncies

Agència de Prevenció i Lluita contra el Frau
i la Corrupció de la Comunitat Valenciana

Aquesta Bústia de Denúncies respon al mandat recollit en la Llei 11/2016, de 28 de novembre, de la Generalitat, de l'Agència de Prevenció i Lluita contra el Frau i la Corrupció de la Comunitat Valenciana d'establir procediments i canals per a la formulació de denúncies, per part de persones, col·lectius o entitats, que garantisquen l'estricta confidencialitat del denunciant que així ho desitge, així com de crear l'oficina virtual de l'empleat públic.

Vol aportar informació d'algun cas de frau o corrupció?

Ha fet ja un enviament? Introduïsca el seu rebut.

Agència de Prevenció i Lluita contra el Frau i la Corrupció de la Comunitat Valenciana

Llei de l'Agència | Resolució que crea aquesta bústia

Eina creada per XNETi Ajuntament de Barcelona

Powered by GlobaLeaks

Landing page for the Valencia Antifraud Agency GlobaLeaks dropbox

The advent of analytics

Another important consequence of the "third wave" of secure online dropbox adoption is that a limited number of quantitative measures about the workings of those dropboxes have begun to be published. This creates the possibility of a different quality of insight to what has been available previously: older research on dropboxes has largely had to rely on interview data.

This data provision is in its early days and the information available is not comprehensive, but it provides some interesting insights nonetheless, which we sought to investigate further in the EAT Project. To date partial figures have been published by the City of Barcelona for the years 2016 and 2017 and for the Valencia Antifraud Agency for the years 2017-19. (Sanchez 2019, Agencia Valenciana Antifraude 2020)

Given the nature of secure online dropboxes, any publication of quantitative data should limit the possibility of "reidentifying" submissions that have been made anonymously. This is a particularly acute concern in instances where the overall number of submissions is relatively small. In this respect, the reporting conventions adopted in these early data releases may be suboptimal. How to remedy this issue is discussed in detail in Chapter 5.

One absolutely fundamental issue is whether whistleblowers actually use secure online dropboxes and whether they produce actionable reports. A related question is whether, as a form of anonymous reporting, secure online dropboxes produce more actionable - or useful - reports than other reporting methods.

Previous research does suggest some connection between whistleblowers' propensity to make reports and their ability to do so without disclosing their identity. An Australian study of 231 publicly listed companies, based on responses submitted to KPMG's biannual fraud survey in 2004, 2006, 2008 and 2010 found that firms operating anonymous disclosure channels reported receiving more fraud reports. (Johanssen & Carey 2015)

A related source of information are the Annual Reports of Italy's National Anticorruption Agency. Under the terms of Anticorruption law no 190/2012, public institutions are required to submit information about their whistleblowing procedures on an annual basis.

Academics who have looked at this data have found a strong correlation between the number of reports received and organisations who have installed a secure online dropbox ("a dedicated information system with internal cryptographic measures and security systems"), though these organisations accounted for a small proportion of the total. The association was less clear for weaker types of whistleblowing channel. (Previtali & Cerchiello 2017: 11, Palumbo & Manna 2019: 14)

Of note, however, is that the absolute number of whistleblowing reports received by these organisations is rather small. Given that these are internal whistleblowing channels for individual institutions rather than external channels operated by national or regional agencies, that is not entirely surprising. It does, however, reinforce the need for care to be taken in reporting dropbox outcomes so as to not re-identify submissions.

One study looking at reports made by 69 Italian publicly owned universities to the National Anti Corruption Authority for the years 2015 and 2016 found that only a quarter of those institutions (69 out of a total of 365) had received at least one report over the two year period. Where institutions had received at least one report, the average reports received over the entire two year period was between 2 and 3. Clearly, with figures this small, reporting does carry with it a risk of identifying individual reports. (Previtali & Cerchiello 2017)

The figures from the Spanish dropboxes are of a different magnitude, as might be expected. The Barcelona figures suggest a significant increase in reports after the launch of the secure online dropbox on 2 January 2017. Barcelona's Director of Analytics states that 63 reports were received in 2016, which increased to 499 in 2017. Of this 2017 figure, 479 reports were routed through the secure online dropbox and 204 of these were submitted anonymously. (Sanchez 2019)

Likewise, the Valencia Anticorruption Agency's 2019 Annual Report gives figures for reports received across all communications channels (including email and post) for periods both before and after the Agency's secure online dropbox was launched in May 2018.

In Valencia, the proportion of reports coming from the secure online dropbox also appears to have grown year on year. Submissions made via the dropbox accounted for 54% of all reports received in 2018, despite the dropbox only being launched in May of that year. Dropbox reports then accounted for 76% of all submissions in 2019. Interestingly, anonymous reports accounted for 50% of all reports received in both years. (Agencia Valenciana Antifraude 2020)

Antifraud Agency of Valencia - 2019 annual report

Net reports received across all reporting channels.

2017 - 35
2018 - 181
2019 - 168

3. Understanding Anonymous Tipping

The Valencia data includes further details about reports received - not all of which came via the dropbox - including their subject. The most frequent subject of reports were public procurement and human resource issues. From the limited data available, the agency appears to have received a steadily increasing number of reports (8% in 2018 to 16% in 2019) about issues that fall outside of its formal remit. This suggests that there is a demand for disclosure channels to be available in other areas.

The Valencia Agency also supplies some information for investigations opened and their status. Much of this relates to internal categories - "in research", "in analysis", "pending", "interrupted" - so may be difficult to compare with other organisations even if comparable data were available.

From the limited information available from Barcelona and Valencia, we can say that there seems to be a strong correlation between the presence of a secure online dropbox and an increase in reports. It is worth noting that both of these dropboxes were launched with national - and in the case of the Barcelona municipality international - media attention.

The impact of legal frameworks on whistleblower reports

The Italian data also provides some indication of how effective legal requirements are for getting institutions to install internal channels. A whistleblowing system was one of the requirements of Anti Corruption Law no 190/2012, but passing legislation on its own has not been sufficient to ensure adoption. This was identified as an issue by the National Anti Corruption Agency itself in 2015.

One study conducted after the passage of anti corruption law no 190/2012 looked at a group of 365 Italian public administrations, made up of 86 hospitals, 137 health agencies, 39 universities and 103 major municipalities. Of the group of 365, only 240 organisations reported adopting whistleblowing channels, despite being obliged to do so. Only 43 organisations had implemented a secure dropbox system, as opposed to a phone number or email address, even though those who did so received more reports overall. (Previtali & Cerchiello 2017)

Do promotion and feedback make a difference?

The provision of anonymous reporting channels can be an important signal about an organisation's ethical culture. Some analysts have seen this as their most important function, with the adoption of whistleblowing channels being motivated by a desire to improve the external perception of the organisation, perhaps in response to public scandal, with the effectiveness of that channel being very much a secondary concern. (Pitroff 2013: 409, Leeds Beckett University 2017, Verschuuren 2019)

This is not necessarily always the case - at least one study has found that publicly listed firms with independent boards, indicating generally high standards of corporate governance, were more likely to institute anonymous reporting channels than others. It may also be the case that potential whistleblowers are sensitive to this distinction. Several studies have found that wider confidence in the system in place in an organisation - including who has the responsibility of dealing with a report and what the potential outcome might be - is an important determinant of people wanting to come forward. (Johanssen & Carey 2015, Pitroff 2013)

3. Understanding Anonymous Tipping

Interpreting an absence of submissions

An EAT partner described a secure online dropbox operated by a public municipality that had not yet received any submissions. They emphasised that the lack of submissions should not be taken as a sign that all was well in the organisation.

The dropbox had been installed in the wake of a series of scandals and was operated by a single named person, who was senior in the organisation. The partner organisation indicated that, not only would this represent a bottle-neck for any reports that were submitted, there was reason to doubt that the review of reports would be truly independent.

The municipality had not run any awareness campaign to support their dropbox and it was unclear how prominent it would be on their new website. The partner organisation concluded that, in this instance, potential whistleblowers would be unlikely to have confidence in the new dropbox.

The presence of a secure online dropbox, then, may not in itself be sufficient to ensure that the facility is used, particularly in an environment where people feel at risk of retaliation. A number of studies have looked at what factors generate confidence in whistleblower systems. Healthcare, where reporting information is of critical importance, has been a particular focus for some of these studies.

Looking at data provided to Italy’s National Anti Corruption Agency, there seems to be a link between specific training on whistleblowing issues - as opposed to general ethics training - and the frequency of reports received in healthcare institutions. (Previtali & Cerchiello 2017)

Furthermore, a pilot study from a British hospital employing 700-800 junior doctors found that endorsement by senior staff, the involvement of peers and consistent feedback increased doctors’ propensity to use an online complaints system.

A web-based system for reporting relatively minor complaints (‘gripes’) was trialled for junior doctors to report concerns like staffing levels that, while important, could not be routed through existing systems for reporting major incidents. The system instituted did not meet the requirements for an anonymous submission system: in practice any individual submission could be trivially attached to an individual doctor whether or not they included their name along with their report. However, other means were used to promote confidence in the system.

These included internal promotion - for instance posters in staff areas - but also face to face recommendations in staff meetings. Trust in the system was furthered by a junior doctor being one of three members of staff tasked with responding to reports. (Carr et al 2016)

Other researchers have noted that feedback, including the monthly reporting of reports received has proven valuable in encouraging people to come forward. As time goes on, a track record of responsiveness can become a key component of trust in the system. (Bausa 2016; Lowry, Moody, Galetta 2014)

4. Experiences of EAT partners and other dropbox operators

Expanding Anonymous Tipping requires understanding what arguments most appeal in practice to the public and private sectors who might be persuaded to adopt secure online dropboxes. This chapter looks at the experience EAT partners had in approaching potential beneficiary organisations in the public and private sector, a process that has produced concrete results and many rich insights.

In order to put the research issues outlined in the previous chapter into context we interviewed a varied group of dropbox operators and those involved in promoting the use of dropboxes to others. For this set of interviews, we approached a group that was broader than those directly involved in the EAT Project, including major media organisations, organisations running SecureDrop instances and two organisations based outside the European Union.

What follows is based on a group of semi-structured qualitative interviews conducted between August and December 2020. The group includes public authorities as well as non-governmental organizations.

Not all of the organizations interviewed operate secure online dropboxes themselves. Some - like the US based Freedom of the Press Foundation, which maintains the open source SecureDrop system - focus their activities on the further dissemination of anonymous reporting schemes in public and private institutions.

Among those interviewees that do operate their own secure online dropboxes, there is a large degree of diversity in how those reporting channels are applied and used. Organisations interviewed differ in their overall mission and objectives, in the resources available to them and in their perception of the security needs of those who make reports to them. Regional socio-cultural and political conditions also have their part to play in how secure online dropboxes are used.

Secure online dropboxes and anonymous disclosures

For many of the organisations interviewed, the provision of secure online dropboxes was synonymous with facilitating means of anonymous disclosure. This was generally seen as an important way both to encourage whistleblowers to come forward and then also to protect them from potential reprisal - a view that, as we have seen, has some support in the research literature.

Nevertheless, in discussions with potential beneficiary organisations, the availability of anonymous reporting was not necessarily received positively. For the EAT partner organisations and others involved in promoting the use of secure online dropboxes as internal channels within organisations, a recurring theme was that anonymity as such can still prove a challenging message.

Interviewees cited several reasons for public and private institutions’ hesitation to introduce anonymous reporting channels. Some reported a generally suspicious view of anonymous reporting on the part of potential beneficiary organisations and that anonymity as such is a “scary” concept. Public institutions in particular expressed concerns about the prospect of an uncontrollable and unverifiable influx of personally motivated reports, which would be challenging to deal with. Historical and cultural factors certainly play a role here.

4. Experiences of EAT partners and other dropbox operators

The Czech NGO Oživení, engaged in combating corruption and relying on whistleblower disclosures to do so, observed that:

> "People in Czech Republic, and I think that's the same for all the former Eastern bloc [countries], are somehow suspicious of anonymity. And secondly, I don't think people are aware enough of their digital security, or that there are ways to stay anonymous online, so we wanted to offer a new channel."

Similarly, the Romanian media freedom organization CPIJ said:

> "The main barrier in obtaining collaboration agreements with potential beneficiaries in Romania remains the general perception of whistleblowers in our country, which is one of snitchers or informers, not of active citizens making a revelation to protect the public interest."

A second problem that was frequently cited by EAT Partner organisations is the very fact of prevailing corruption in the countries concerned. Some officials might have self-interested reasons for resisting the introduction of anonymous reporting schemes in public institutions and may fear establishing avenues that could lead to themselves being implicated in whistleblower disclosures.

A third recurring theme among EAT partner organisations was that, notwithstanding the EU Directive, the lack of a national legal framework around whistleblower protection in several countries inhibited organisations from adopting secure online dropbox systems. Many cited the need to wait until there was certainty. In addition, public authorities in EU countries surveyed for this research repeatedly cited the ongoing transposition of the EU Whistleblowing Directive as one of the reasons for hesitation in this area.

One complicating factor is that the Directive itself leaves a great deal of discretion to Member States on the topic of anonymous disclosure channels and it is possible that national-level regulations in this area will differ. While an anonymous whistleblower whose identity becomes revealed in the course of an investigation is entitled to the same level of legal protection than other whistleblowers under the Directive, the legislation stops short of introducing an obligation to provide for anonymous channels.

It is therefore up to each Member State to determine how much support to give to anonymous disclosure channels, to determine whether they should be encouraged or indeed made mandatory. It is perhaps not surprising that public authorities are taking this into consideration.

Secure online dropboxes in action

As discussed elsewhere in this report, secure online dropbox systems are available from a number of providers. Dropbox operators interviewed for this chapter were users of three well-established systems: GlobaLeaks, SecureDrop and BKMS. These products differ in several respects but what they have in common is the possibility to communicate back and forth with an anonymous person via an encrypted channel.

4. Experiences of EAT partners and other dropbox operators

Beyond the differences in systems adopted, civil society organisations reported using their secure online dropbox systems in different ways, recalling the diversity observed by Philip Di Salvo and other researchers.

Some organizations including Xnet in Spain and Oživení in Czech Republic have established anonymous whistleblowing channels in order to receive insider tips that allow them to fulfil their organizational mission. They advertise a number of public contact points in addition to their dropbox.

For civil society organizations in this position, the secure online dropbox is usually not their most frequently used means of contact. On average, the civil society organizations interviewed that provided a secure online dropbox alongside other contact points such as phone, e-mail or unencrypted online forms report receiving roughly 10-15% of their communications through the encrypted channel. Organisations in this position typically report concerns about missing messages they would otherwise receive as a reason for remaining accessible through email, social media and other less-secure ways of making first contact.

EAT dropbox brings rapid results

One public authority launched a secure online dropbox as a result of the EAT Project and report having received three actionable reports in the first month of their dropbox being online.

In contrast, Transparency International Italy channels all public inquiries through their GlobaLeaks instance, making the possibility of anonymous communication explicit for anyone who would like to get in touch with them.

For public authorities, which usually provide secure online dropboxes to facilitate anonymous whistleblower reports on specific issues such as corruption or money laundering, the use of these channels is relatively high. Institutions such as the German financial regulator BaFin or the Spanish Anticorruption Agency AVAF reported an estimated 85% of their whistleblower disclosures reaching them via the encrypted channel.

Similarly, the reported quality of information coming through the secure online dropbox channel seems to differ. Civil society organizations report struggling to deal adequately with a considerable influx of reports that may be groundless or mistaken.

In contrast, public authorities with a defined scope report that the vast majority of incoming messages are considered useful and contribute to the organization‘s mission in a meaningful wayxii. The German financial regulator BaFin, which has been running a BKMS instance since 2017, states that the benefits of anonymous reporting schemes far outweigh any disadvantages:

4. Experiences of EAT partners and other dropbox operators

> "I think it is important that this option exists, because it enables whistleblowers to submit their information to us without exposing themselves to unnecessary danger. We highly value the possibility of anonymous reporting. In addition, I believe that we would not receive the majority of the reports we are getting now if we did not have the opportunity to do so anonymously. [...] Of course, motivations of whistleblowers differ. I would consider abuse as a minor problem though. You have to make sure that you filter out factual information [...] and things are not always crystal clear. The bottom line is that such disadvantages can be neglected compared to the advantages of an anonymous whistleblower system."

Making anonymity work

Three major themes emerged from our interviews: first, explicit support for anonymous disclosure in national legal frameworks makes a considerable difference to the willingness to adopt these methods.

As previously mentioned, several of the organizations advocating for the adoption of such channels have faced challenges stemming from the ongoing transposition of the EU Whistleblowing Directive. Some of them understand the problem of operating anonymous dropboxes within a missing or incomplete legal framework first hand, as discussed with the Italian branch of Transparency International with regards to data protection:

> "The law on whistleblowing in Italy dated from December 2017 required the Anticorruption Authority to release some guidelines on how to manage information, and then show that these guidelines should also touch on the storage of data. But this guideline has not been issued yet. So we really don't know how to behave, it's just an interpretation based on the general GDPR principles. But there is no transposition of GDPR principles in whistleblowing law in Italy, or on how external third parties like NGOs should treat the information they receive."

The desire for explicit guidance on how to implement whistleblowing procedures is a recurring theme in our interviews. Our interviewee at the German financial regulator BaFin suggested that a well defined legal framework also constitutes a kind of insurance for officers handling anonymous reports, as potential conflicts with other regulations have already been taken into due consideration, clearly defining responsibilities and duties:

> "The establishment of an independent whistleblower unit is based on a legal requirement which specifies the setting up of dedicated channels which have to be appropriately protected. And from my point of view, this whistleblower unit, the organizational separation of some employees as well as its independence, is a really effective and valued measure."

4. Experiences of EAT partners and other dropbox operators

Crucially, those public institutions which had implemented secure online dropboxes typically found them to be extremely valuable. Interestingly, when asked to estimate the proportion of reports received through these channels that were actionable or useful, they reported receiving more workable results from their secure online dropboxes than some of the civil society organisations did.

Setting the question of resources aside, there are a number of reasons why anonymous reporting schemes seem, in many cases, to yield more effective results when operated by public authorities than by civil society organizations. When asked to to give an estimate of percentage of cases in which whistleblowers‘ first report is addressed to the respective organization, we have found that public authorities maintaining dedicated channels almost exclusively receive initial reports – as opposed to civil society organizations, who are far more often approached by whistleblowers who have already suffered detriment and whose issues may therefore be more difficult to resolve.

In addition where anonymous channels are provided by an official state institution, that may contribute to their increased acceptance by the general public. As discussed, a negative perception of anonymous reporting is still common in some countries and sectors. The experience of Anticorruption Agencies in Spain shows that the wider implementation of secure online dropboxes is likely to contribute to a more favourable interpretation of anonymous reporting and prompt more whistleblowers to come forward in the future.

> "What we have noticed is that the percentage of reports has been increasing since the letterbox was implemented, both in total numbers and in percentages. [...] The intuition is that it will go from less to more. I anticipate more publicity, of being able to make known more knowledge of irregular facts I have thought of professional platforms, that is to say, systems where a public or private employee can have relatively fast access with corporate platforms, that apart from the possibility of a suggestion box can have an anonymous complaints box and I visualize an increase of anonymous complaints, a consolidation of the anonymous complaints box.“

This does not mean that receiving whistleblower disclosures in other contexts becomes less valuable: the work of organizations like the US-based Freedom of the Press Foundation, which has taken on the mission of further developing and disseminating the anonymous reporting technology SecureDrop, underlines the importance of whistleblower disclosures for the work of journalists. Moreover, the pioneering efforts of civil society organizations have paved the way for public institutions that now benefit from their experience:

> "One of the things that helped us a lot, to demonstrate that it really works, was that we showed them [the municipality] what a tip looks like, what kind of conversations we used to have with the tipper; so they saw that it really works, that we work with that and that it is quite easy to use. So I think that broke the hesitance from their side."

The adoption of anonymous reporting schemes in the formalized framework of public authorities is in its early days, but already it is clear that its importance should not be underestimated. The experience expressed by institutions that use secure online dropboxes is largely positive.

4. Experiences of EAT partners and other dropbox operators

Accessibility

Finally, there were a number of concerns expressed about the usability and accessibility of secure online dropboxes. In particular, our interviews support the indication in the quantitative data that whistleblowers might prioritise accessibility over security in practice, even if they want to maintain their anonymity.

In many cases, using secure anonymous reporting channels requires extra effort on both sides: as described previously SecureDrop requires whistleblowers to use Tor and necessitates additional installation and upkeep demands on the part of the dropbox operator. GlobaLeaks recommends that whistleblowers make any disclosures over Tor, but dropbox operators have the option of not requiring this.

There is no question that these technical hurdles impact the use of anonymous channels: the majority of NGOs surveyed stated that they only receive a minority of reports through respective anonymized channels. Organizations such as Atlatzso in Hungary and Pištaljka in Serbia note that they receive most of their reports through an unencrypted online form provided on their website, and consider Tor as a “hurdle“ for reporting persons.

Whether technical setups remain a hurdle also depends on a whistleblower‘s perception of the risk they face if discovered. Czech Anti-corruption NGO Oživení, which supports whistleblowers by both giving legal support and receiving disclosures, notes that reports on actual corruption cases are far more likely to be submitted through the anonymous channel than through other means of communication the organization provides. That is, whistleblowers who perceive themselves to be at risk take action accordingly.

Similarities can be observed on the side of organizations advocating for and providing secure channels. The US based organization Freedom of the Press Foundation, which maintains the journalism-focused SecureDrop system, does not see it is the optimal solution for everyone:

> "When we talk to news organizations, we discuss their threats with them, discuss what kinds of stories they expect and want to report on, whether they want to be the organization that can receive tips on and run the next Ed Snowden revelation. And if they are, they probably need something like SecureDrop. If they are more interested in corporate crime, and they want to report on minor violations of the law in your areas, say you are a local paper, something like a Signal tip line might be a better fit.”

At the same time, organizations that have decided to introduce more complex technological solutions to protect their sources and work seem to benefit from the investment. Paul Lewis, Head of the Investigative Team at the British newspaper the Guardian, describes SecureDrop as “an integral part of the way we work now, on a daily, sometimes hourly basis” and says that, despite the fact that “that sort of user interface can take a bit longer” to get acquainted with, “the trade-off is worthwhile”.

None of this negates the need for further developing anonymous communication channels to make them more user-friendly and effective to use. Certainly, the trend in anonymous messengers has been to aim at adoption by as mainstream an audience as possible. (Wiener 2020)

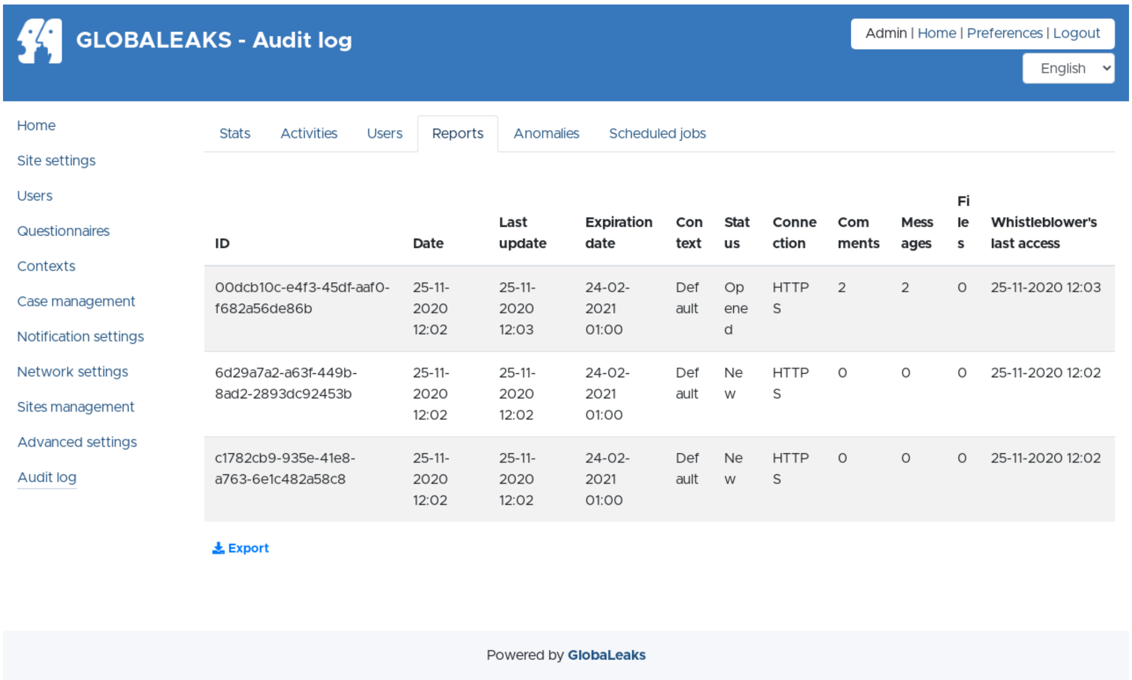
4. Experiences of EAT partners and other dropbox operators

Not all dropbox solutions include read receipts or other features that would allow those handling incoming reports to know whether a whistleblower has received their reply and intend to further communicate, functionality that assists organisations in meeting the case management aspects of the EU Directive and have proven effective in use. Clearly structured, flexible questionnaires offer whistleblowers guidance when making reports, and facilitate the work of those at the receiving end. These and other improvements to the setup of anonymous channels can, and will, make them more effective tools.

5. Assessing the Efficacy of Dropboxes with Quantitative Data

One of the challenges in assessing the efficacy of secure online dropboxes is access to metadata about their usage. By their very nature the data associated with a dropbox is closely guarded, including the metadata – information about submissions - as well as their content. Whilst this presents a particular challenge for analytics, the fact that such data is closely protected and difficult to acquire should be viewed as reassuring, and a positive from an anonymity and more general privacy perspective.

The EAT Project has resulted in new functionality being added to the GlobaLeaks platform, in the interests of facilitating future research work. This new functionality will also improve the ability of organisations to audit their own dropboxes, by allowing dropbox operators to download selected metadata using the "Reports" option in the Audit Log menu. While this functionality was originally intended to allow analysis of dropboxes set up as part of the EAT Project, it is now available to all running the latest version of GlobaLeaks.



ID	Date	Last update	Expiration date	Context	Status	Connection	Comments	Messages	Files	Whistleblower's last access
00dcb10c-e4f3-45df-aaf0-f682a56de86b	25-11-2020 12:02	25-11-2020 12:03	24-02-2021 01:00	Default	Opened	HTTPS	2	2	0	25-11-2020 12:03
6d29a7a2-a63f-449b-8ad2-2893dc92453b	25-11-2020 12:02	25-11-2020 12:02	24-02-2021 01:00	Default	New	HTTPS	0	0	0	25-11-2020 12:02
c1782cb9-935e-41e8-a763-6e1c482a58c8	25-11-2020 12:02	25-11-2020 12:02	24-02-2021 01:00	Default	New	HTTPS	0	0	0	25-11-2020 12:02

The categories of metadata collected as part of the EAT Project are supplied in Appendices E and F. These include information supplied as part of the questionnaire, which was included across EAT Project dropboxes, as well as some general metadata - visible in the image above and highlighted in blue in Appendix E - which is now available to all GlobaLeaks users who have upgraded to the latest version of the software (version 4 or later). Our beneficiary agreements included providing access to this data for research purposes within the timeline of the project.

The data we have received from EAT Project dropboxes, consequent to those beneficiary agreements, is limited, in part because several of these secure online dropboxes were launched relatively late in the project timeline[6]. Nonetheless, analysis of this data suggests some interesting insights about the way dropboxes are being used, which will be referred to in our discussion of Tor use.

[6] The EAT dropbox data reached us pre-cleaned. Some submissions made on the day of dropbox activation with no data - strongly suggestive of test submissions - were excluded from the set.

5. Assessing the Efficacy of Dropboxes with Quantitative Data

Given the difficulty we have had in obtaining significant metadata within the project timeline, our experience in accessing metadata from dropbox operators with whom there has been no prior agreement has been similarly challenging, which has prevented a large-scale comparative study. However, utilising existing relationships we have been able to access limited metadata, which has still provided useful insights on the usage of secure online dropboxes. In recognition of the challenges associated with accessing and sharing metadata we will also propose a framework and outline specification that could be developed to facilitate wider sharing of metadata in a privacy and anonymity secure manner.

Evaluating data from REF:DATA_PROV_1

Using the new functionality added to the GlobaLeaks platform, DATA_PROV_1 – an organisation based in an EAT Project country though not a direct beneficiary of the Project - kindly provided us with access to a metadata set covering a period of 4 years usage of their secure online dropbox.

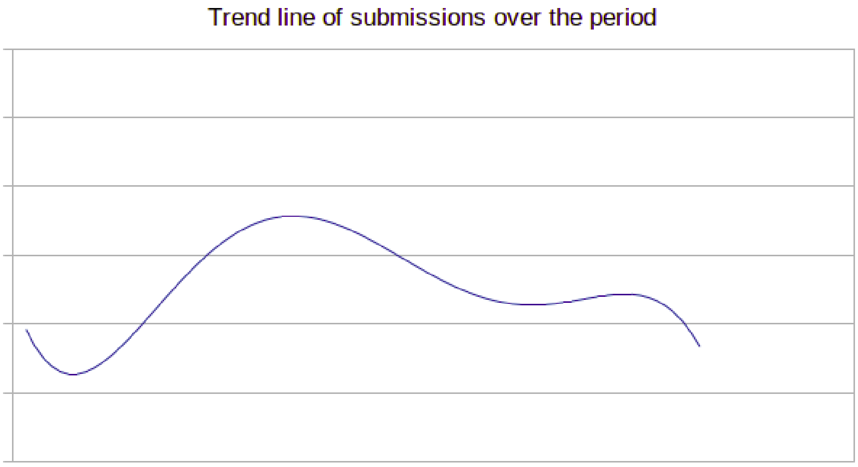
That data showed a limited number of fields for each entry, for example, whether an entry was sent via Tor or not, and how many files or messages had been sent as part of a submission. Whilst this dataset is a single organisation in a single jurisdiction, it still provides some useful insights, albeit not necessarily at a statistically significant level. We will detail that analysis below.

Throughout this analysis the privacy of the data is paramount, as such, we will only quote high-level aggregate statistics, and only in a manner that we consider limits any additional data inferences. For example, we will not provide exact counts, only trends or relative proportions and correlations.

Prior to analysis we excluded data from the earliest year which contained a low number of submissions and therefore was not sufficiently well protected to be released even as aggregate high-level statistics. We also excluded a small number of submissions that looked like incomplete or test submissions, occurring within one hour of each other on the same day.

Trend in submissions

There was an initial upwards trend in the number of submissions being made, peaking in the second year of analysis. Since that point there has been a steady decline in submissions. Figure 1 shows a polynomial trend line of 5 degrees. This was selected as it best matched the underlying data without revealing precise values. We have adjusted the graph's axis to shift the values for further protection, as such, the figure should only be used for interpreting a trend and not for extracting values.



5. Assessing the Efficacy of Dropboxes with Quantitative Data

Whilst the trend has been downwards since the second year, we cannot be certain that this reflects dropbox submissions as a whole. As better whistleblower protections are provided, and more organisations start to provide internal and/or external dropboxes, the total number of submissions may be spread over a greater number of dropboxes. This is a further argument for wider reporting of metadata, to allow a broad picture of whistleblowing in a particular sector or jurisdiction to be established.

Whistleblower Interaction

An additional metric we have measured is the time between the last login from the whistleblower and the original creation date of their submission. Whilst we cannot know intermediate logins, we can use this value as a proxy for engagement, under the assumption that a whistleblower who has a long period between creation and last login is likely to have maintained engagement with the secure online dropbox and the submission they have made. Looking at absolute values for this analysis is of limited use, as submissions from year 1 have the potential to have much higher values than submissions from year 4. As such, we analysed whether there was a positive correlation between the number of files submitted, the number of messages, or the usage of Tor, and the number of days between first and most recent login. Those results are shown in Table 1.

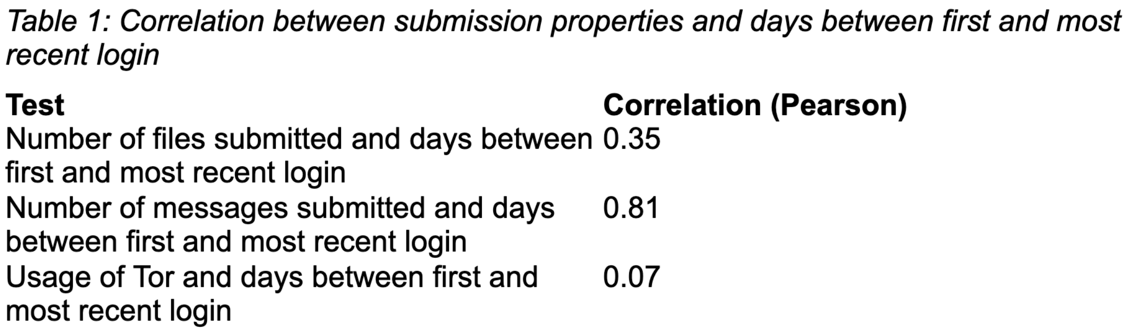


Table 1: Correlation between submission properties and days between first and most recent login

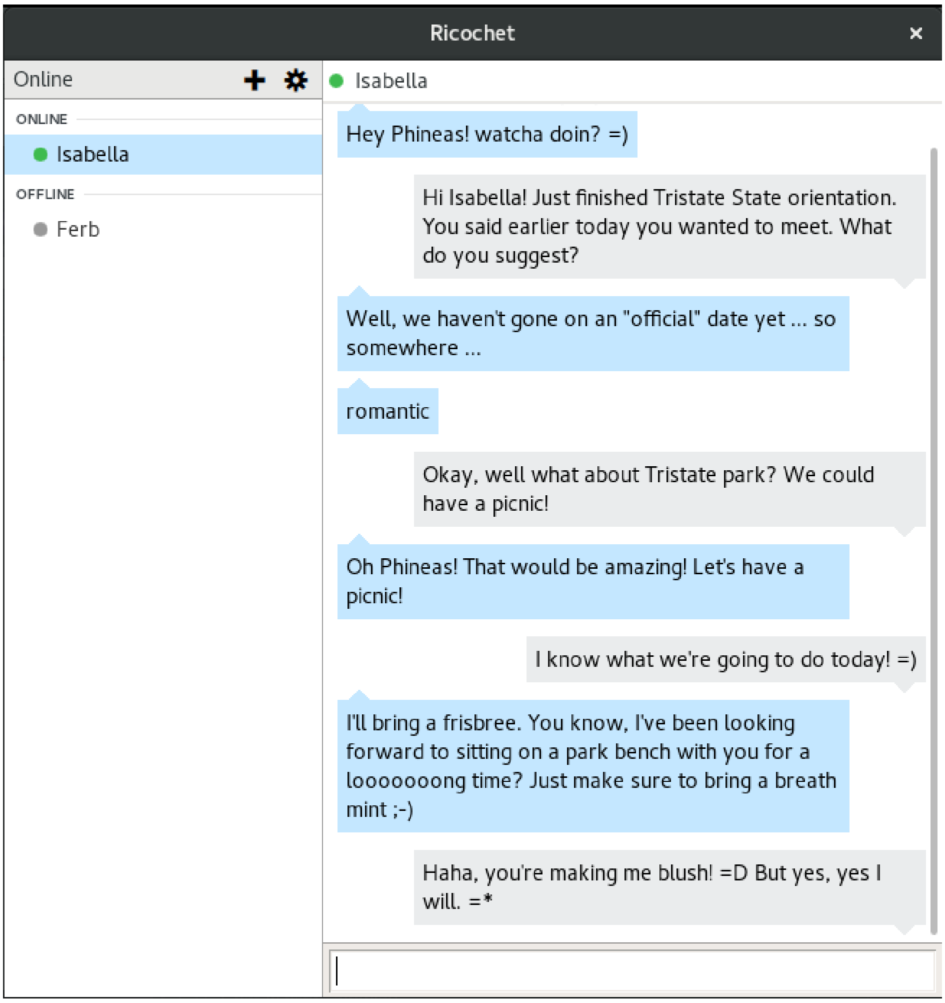
Test	Correlation (Pearson)
Number of files submitted and days between first and most recent login	0.35
Number of messages submitted and days between first and most recent login	0.81
Usage of Tor and days between first and most recent login	0.07

As Table 1 shows, there is no correlation between Tor usage and our proxy for engagement. This is consistent with generally low Tor usage, which we shall discuss further below. The number of files submitted shows a low correlation, indicating that a larger number of files submitted does not always result in greater engagement, which stands to reason, since the files could be delivered in one upload. There is fairly strong correlation between the number of messages and the period of engagement. This is also somewhat to be expected, since multiple messages are probably not going to be delivered on the same day, and as such, one would expect the greater the number of messages the longer the period they are spread out over.

However, the result does indicate the messaging is a core requirement of a dropbox and we can therefore assume that the provision of an easy to use, reliable, and secure messaging platform within the dropbox is essential to maintain engagement. This observation is supported by published remarks from the City of Barcelona's Director of Analytics, who has said that the ability for ongoing conversation between a dropbox operator and the individual who has submitted a report is one of the most important properties of a dropbox system. (Sanchez 2019)

We also evaluated whether there was a correlation between the number of messages and the number of files submitted, to determine whether there tended to be greater interaction with a larger submission. We calculated a correlation of 0.49, which is low to moderate and does not indicate a strong relationship.

5. Assessing the Efficacy of Dropboxes with Quantitative Data



Hey Phineas! watcha doin? =)

Hi Isabella! Just finished Tristate State orientation. You said earlier today you wanted to meet. What do you suggest?

Well, we haven't gone on an "official" date yet ... so somewhere ...

romantic

Okay, well what about Tristate park? We could have a picnic!

Oh Phineas! That would be amazing! Let's have a picnic!

I know what we're going to do today! =)

I'll bring a frisbree. You know, I've been looking forward to sitting on a park bench with you for a looooooong time? Just make sure to bring a breath mint ;-)

Haha, you're making me blush! =D But yes, yes I will. =*

Blueprint supports the ongoing development of Ricochet Refresh[7], a free, open-source desktop based, text messaging software application. The program is believed to be the only free desktop chat software using Tor that provides real anonymity and privacy. By comparison, widely used programs such as Signal require a personal phone number. Ricochet Refresh enables dropbox operators to have a live chat conversation with someone making a submission, while also safeguarding the identity as well as communication privacy of that person.

EAT project dropbox installations provided easy to use access to Ricochet Refresh, an improvement made to the standard GlobaLeaks system as part of the project. As Ricochet relies on the Tor network to provide anonymity as well as confidentiality, we were not able to easily gather statistical data on its use without compromising disclosers' activities.

The use of Ricochet Refresh in this project provides a useful example of how a shared software tool, developed for all, can make it easy and inexpensive for an organisation to transition to the new rules as the Directive is rolled out.

[7] https://www.ricochetrefresh.net/

5. Assessing the Efficacy of Dropboxes with Quantitative Data

Usage of Tor

A surprising result of our analysis was the relatively uncommon usage of Tor for submissions. There were no meaningful correlations between Tor and the number of messages (0.15), the number of files (-0.04) or the time between first and most recent login (0.07). Additionally, as a percentage of submissions, Tor was always in the minority and halved between year 1 and the following years.

Table 2: Percentage of submissions made over Tor

Year	Percentage of submissions using Tor
1	29%
2	13%
3	16%
4	15%

This result raises some concerns. Not only has the percentage of submissions using Tor trended downwards, but it also dropped significantly in year 2, which was the year with the most submissions. This indicates that whistleblowers are not utilising the most anonymous and secure method for submissions, and that the vast majority of submissions come over channels that could be susceptible to greater monitoring.

This presents a particular challenge for dropbox maintainers: how can Tor be made more accessible and usable, so that it becomes the default option for the whistleblower. It is possible that the submissions are coming from machines on which the whistleblower does not have permission to install software. However, that in itself is of concern, since that suggests that whistleblowers are making submissions over a work network, which would not be considered a safe location to make such a submission.

Alternatively, the result could be due to a lack of user education or nervousness about using Tor correctly. Previous researchers have found that non-technical users find it difficult to assess online risks in a whistleblowing context (Lam and Harcourt 2019; Lowry, Moody and Galetta 2014). In many regards this would be the more desirable outcome, since providing better education is a more tractable task than overcoming a technical limitation.

Wanting anonymity and using Tor don't always go together

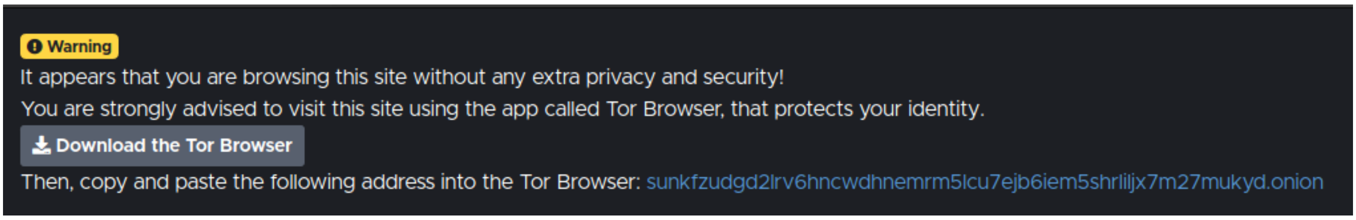
Analysis of metadata from EAT Project dropboxes bears out these preliminary findings about the use of Tor. Usage of Tor was largely consistent at 20%. However, worryingly, over 30% of anonymous submissions were not made over Tor.

This suggests that greater guidance or education is needed in order to make sure that whistleblowers who want to stay anonymous choose the technical option that is most appropriate to their needs.

Whilst the number of submissions per dropbox is too small to draw conclusions, there does also appear to be variance in how dropboxes in different countries perform with regard to Tor usage. Further analysis of those dropboxes performing better, with a larger sample, would assist in being able to determine if this result is significant, and if so, what are the best practices that other dropbox operators can learn from.

5. Assessing the Efficacy of Dropboxes with Quantitative Data

Without access to a wider set of dropboxes we cannot tell whether this trend is across all dropboxes or just this one. This prevents us from being able to compare different educational approaches. For example, GlobaLeaks shows a banner specifically recommending the usage of Tor and a link to download the Tor browser, as shown in Figure 2.



Warning

It appears that you are browsing this site without any extra privacy and security!

You are strongly advised to visit this site using the app called Tor Browser, that protects your identity.

Then, copy and paste the following address into the Tor Browser: sunkfzudgd2lrv6hncwdhnemrm5lcu7ejb6iem5shrliljx7m27mukyd.onion

With access to metadata from across different dropboxes and providers it would be possible to determine best practices and evaluate what educational approaches work best in guiding users towards using Tor.

Future of dropbox statistics

Clearly there are still lessons to be learned with deploying and managing dropboxes. Without widespread statistics on usage and efficacy it will be difficult for best practices to be established, tested and shared. We have faced significant challenges in acquiring any metadata about dropbox usage. As already discussed, on the one hand it is comforting to know that the administrators are taking a safety first approach. On the other hand, it indicates we need to look at better, more secure, ways of sharing statistics to provide assurance to dropbox administrators that they can safely share such statistics.

Are aggregate statistics safe?

The simple answer is no, due to what has been termed the “Fundamental Law of Information Recovery” which is formulated as "overly accurate answers to too many questions will destroy privacy in a spectacular way." (Dwork and Roth 2014) Such attacks are more commonly referred to as Reconstruction Attacks, which cover any methods for reconstructing private data from publicly available aggregate data.

There may be a narrow set of occasions when sharing such data is safe, for example, where the same data is available elsewhere or is considered common knowledge or a matter of the public record. For example, the number of births or deaths in a given year in a given country. However, there are many occasions, particularly when such data is released longitudinally, i.e. once a month, quarter, or year, where it might not be safe. In such circumstances changes in the underlying population of records can potentially be recovered from changes in the aggregate statistic. A simple hypothetical example would be if a company declared the number of members of its board that had heart disease each quarter – something investors may want to know to judge resilience or stress in the board. Firstly, extreme values reveal a lot, for example, if everyone in the board has heart disease then an adversary learns the status of each individual. Inversely, if no one has heart disease the same attribute is learnt for the entire group.

A more nuanced example is when the statistics change over a period of time. For example, if the number declared in Quarter 1 was 4 and the number declared in Quarter 2 was 3, and one member of the board had stepped down, then the attribute for that individual can be inferred by differencing the Quarter 1 and Quarter 2 results. The above is a very simple example, much more complicated reconstruction attacks can be performed.

Differential Privacy

If aggregate statistics aren't safe, what can we do? The answer is rather than releasing the raw aggregate statistics we can release protected statistics using a technique known Differential Privacy. Differential Privacy provides a mathematically rigorous method for bounding the privacy cost of a release. Whilst the underlying mathematics can seem complicated, it is relatively straightforward conceptually. Cynthia Dwork, one of the co-creators of Differential Privacy, describes the English language definition of Differential Privacy as follows:

> "The outcome of any analysis is essentially equally likely[8] independent of whether any individual joins, or refrains from joining, the dataset[9]."

In essence the above statement means that if you had two different datasets, one that contained the individual's data and one that did not, the probability of any release statistic occurring is almost the same across both datasets. As such, when seeing a particular released statistic it will not be possible, within a probabilistic bound, to determine if a particular individual's data was included in the calculation of it, even if the adversary knows all the data in both datasets. The "almost the same" is bounded by a value called epsilon, or more commonly referred to as the privacy budget. This value is kept small, typically 1.

The above may seem purely theoretical and too complicated for real-world use. However, the US Census Bureau has committed to releasing its 2020 census products using Differential Privacy, which it describes as the "...gold standard in data privacy protection." (US Census Bureau) This is important for a number of reasons. Firstly it will increase awareness and acceptance of Differential Privacy. Second, it will cause anyone who wishes to utilise US Census statistics to understand how Differential Privacy works, creating a widespread upskilling in the data analysis sector.

Furthermore, there are also automated tools for calculating Differentially Private releases of simple datasets, for example, the R package DiffPriv[10], which provide a set of tools for performing differential privacy with minimal background knowledge.

[8] The property is probabilistic in nature, so whilst we describe it in absolutes there is an underlying probability distribution, hence the use of the phrase "essentially equal"

[9] A video of a seminar by Cynthia Dwork on the definition of Differential Privacy is available from: https://www.youtube.com/watch?v=lg-VhHlztqo

[10] https://www.bipr.net/diffpriv/

5. Assessing the Efficacy of Dropboxes with Quantitative Data

Dropboxes and Differential Privacy

The type of metadata required to evaluate the efficacy of dropboxes is ideally suited to protection by Differential Privacy. The data is basically just counting queries, i.e. counting the number of submissions made using Tor, or the average number of files submitted over Tor, or the average number of files submitted not over Tor. The protected statistics that would be generated would include random noise, but that is fine for the analysis required, since we are not interested in exact values, rather the trends and determining if changes made have a positive or negative impact.

As such we propose that a standard set of statistics is agreed upon to be created and shared with researchers and oversight bodies. Those statistics should be protected using Differential Privacy at the point of extraction, i.e. within the dropbox platform, using an agreed set of Differential Privacy parameters. Table 3 shows an initial proposed set of statistics. This is intended to be a starting point for building a collaborative list and agreeing on standard differential privacy statistics. The release statistics are paired, one for submissions made via Tor and one for submissions made without Tor to allow for comparisons and trends to be evaluated across the different submission channels. The pairs can be summed to get the overall numbers irrespective or channel, if desired.

These statistics are phrased as a query, as opposed to a single field, to make them compatible with Differential Privacy. As such, they represent the results of running a query, for example, counting the number of submissions in a given period, or calculating an average. The reporting period is left for administrators and may need to vary between dropboxes depending on overall usage. We would recommend using divisible periods, so different providers can release on different schedules but still be comparable. A base period of 1 week or 1 month would provide good flexibility. If one dropbox releases on a monthly schedule and another releases quarterly the monthly statistics can be summed to cover the equivalent period.

5. Assessing the Efficacy of Dropboxes with Quantitative Data

Table 3: Proposed Statistics

Proposed Statistic Name	Purpose
Number_of_submissions_via_Tor	Capture the total number of submissions via Tor in a given period. Combined with Number_of_submissions_not_via_Tor gives the total number of submissions
Number_of_submissions_not_via_Tor	Capture the total number of submissions not via Tor in a given period. The combination of these two allow evaluation of Tor usage, as well as determining the efficacy of changes to support or encourage Tor usage over time
Average_files_per_submission_via_Tor	Calculates the average number of files that are attached to a submission that is made via Tor.
Average_files_per_submission_not_via_Tor	Calculates the average number of files that are attached to a submission that is not made via Tor. Combined with Average_files_per_submission_via_Tor will provide insights on the nature of submissions via different channels, as well overall performance by summing together and seeing trends in submissions overall
Average_messages_per_submission_via_Tor	Calculates the average number of messages that are attached to a submission that is made via Tor.
Average_messages_per_submission_not_via_Tor	Calculates the average number of files that are attached to a submission that is not made via Tor. This will act as one of the proxies for engagement, and also help to evaluate whether different channels provide different engagement results. It may also be possible to deploy different messaging services on the different channels, for example, Ricochet when submitting via Tor, and determine what impact that has on engagement.
Average_engagement_period_via_Tor	Calculates the average number of days since first and most recent login for all submissions that had a login in this period, and were sent via Tor.
Average_engagement_period_not_via_Tor	Calculates the average number of days since first and most recent login for all submissions that had a login in this period, and were not sent via Tor. Combined with Average_engagement_period_via_Tor provides an alternative proxy for engagement to allow analysis of overall whistle-blower engagement and efficacy of drives for greater engagement.

6. Conclusion

The EAT project captures a moment where secure online dropboxes are on the threshold of mainstream adoption. In this respect, it has been ahead of its time - but not too far.

Our experience promoting anonymous tipping technology to public institutions and private companies across the European Union shows that there is a need for national regulation to be in place before business but also many institutions in the state sector feel able to come on board.

Notwithstanding this, we have found that early adopters of secure online dropbox technology are invariably very happy with the results, and this is particularly the case for public sector organisations.

The start of quantitative data being available means we are on the threshold of a much better understanding of how dropboxes work in practice and which factors encourage their adoption by organisations and their use by whistleblowers. There are, however, still significant barriers in acquiring the data.

Through this project, we have begun to make the purely technical side of this easier. Today, anyone running the current version of GlobaLeaks (version 4 and onwards) can download a set of metadata from the internal Audit menu. This will be useful for internal audit purposes and external researchers alike. This feature was inspired by EAT.

Nevertheless, many dropbox operators are likely to be cautious about sharing this data - which is entirely understandable given the importance of protecting those who have submitted information anonymously. Dropbox operators also may be concerned about the Data Protection position, not having explicit authority to share metadata with others. It would be helpful to have clarification in law or regulation on this matter.

Policy makers can assist with this in two respects. It would be valuable to establish requirements for sharing this kind of data, so that comparisons can be made. This does, however, need to be accompanied by the establishment of conventions for reporting this data in a safe way that limits the possibility that whistleblowers can be reidentified from published statistics. Differential Privacy techniques have an important role to play here and we have suggested how this could work in practice.

7. References

Agencia Valenciana Antifrau. (2020) Memoria 2019, online at: https://www.antifraucv.es/wp-content/uploads/2020/03/MEMORIA_2019_VAL.pdf. Accessed 26 January 2021.

Arnold, J.R. (2020) Whistleblowers, Leakers and Their Networks. Rowman & Littlefield.

Bausa, C., 2016. Tres controles efectivos a implantar para detectar y disuadir el fraude: el canal de denuncias, el análisis de datos y la autoevaluación del control interno. Revista de Contabilidad y Dirección, 23, pp.113-133.

Beltran, A. (2018) Las denuncias de la corrupción no solo son confidenciales, ya pueden ser anónimas. El Diario. Online at: https://www.eldiario.es/comunitat-valenciana/antifraude-buzon-denuncias-agencia-valenciana_1_2108701.html, accessed 26 January 2021.

Blueprint for Free Speech (2020) Whistleblower Protection Compliance Tool. Online at: https://tool.blueprintforfreespeech.net/, accessed 26 January 2021.

Blueprint for Free Speech (2018) The Perugia Principles for Journalism: Working with Whistleblowers in the Digital Age, online at: https://www.blueprintforfreespeech.net/s/Blueprint_Perugia_Principles-3m6h.pdf, accessed 26 January 2021.

Carr, S., Mukherjee, T., Montgomery, A., Durbridge, M. and Tarrant, C., 2016. Developing the 'gripes' tool for junior doctors to report concerns: a pilot study. Pilot and feasibility studies, 2(1), pp.1-8.

A Change of Direction (2017). Xnet and Barcelona Municipality launch Whistleblower Platform, online at: https://www.changeofdirection.eu/campaign-central/xnet-and-barcelona-municipality-launch-whistleblower-platform, accessed 26 January 2021.

Chen, N., 2011. Wikileaks and its Spinoffs: new models of journalism or the new media gatekeepers?. Journal of Digital Research & Publishing, 1, pp.157-167.

Di Salvo, P. (2020) Digital Whistleblowing Platforms in Journalism. Palgrave Macmillan.

Dwork, C. and Roth, A., 2014. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3-4), pp.211-407.

G20 (2019). High-level Principles for the Effective Protection of Whistleblowers, online at: https://www.bmjv.de/SharedDocs/Downloads/EN/G20/G20_2019_High-Level-Principles_Whistleblowers.pdf. Accessed 26 January 2021.

Gökçe, A.T., 2013. Teachers' value orientations as determinants of preference for external and anonymous whistleblowing. International Journal of Humanities and Social Science, 3(4), pp.163-173.

Gonzalez, G. (2020) La Generalitat alienta la delación de la corrupción de forma anónima, El Mundo. Online at: https://www.elmundo.es/cataluna/2020/12/15/5fd8a4eb21efa0f47d8b4638.html, accessed 26 January 2021.

7. References

Greenberg, A., 2012. This Machine Kills Secrets: How WikiLeakers, Hacktivists, and Cypherpunks Are Freeing the World's Information.

Johansson, E. and Carey, P. (2016) Detecting Fraud: The Role of the Anonymous Reporting Channel. Journal of Business Ethics. Journal of business ethics, 139(2), pp.391-409

Kenny, K. (2019) Whistleblowing: Toward a New Theory. Belknap Press.

Lam, H. and Harcourt, M., 2019. Whistle-blowing in the digital era: motives, issues and recommendations. New Technology, Work and Employment, 34(2), pp.174-190.

Leeds Beckett University. (2018) Global Whistleblowing Landscape for Reporting Doping in Sport, online at: https://www.wada-ama.org/sites/default/files/resources/files/leeds_beckett_wada_report_on_whistleblowing_platforms_july_2018.pdf, accessed 26 January 2021.

Lowry, P.B., Moody, G.D., Galletta, D.F. and Vance, A., 2013. The drivers in the use of online whistle-blowing reporting systems. Journal of Management Information Systems, 30(1), pp.153-190.

Oživení. (2020) Whistleblowing - Quantitative research (interview survey CAVI), online at: https://www.oziveni.cz/wp-content/uploads/2021/01/v4-Whistleblowing_EN.pdf, accessed 26 January 2021.

Palma, E.B., 2018. El control externo y el whistleblowing (canales de denuncia). Revista española de control externo, 20(59), p.32.

Palumbo, R. and Manna, R., 2019. Uncovering the relationship between whistleblowing and organizational identity. International Journal of Public Sector Management.

Pittroff, E. (2014). Whistle-blowing systems and legitimacy theory: A study of the motivation to implement whistle-blowing systems in German organizations. Journal of Business Ethics, 124(3), pp.399-412.

Pop, M. (2021) ISO standard 37002 on whistleblowing systems, online at: https://cji.ro/en/iso-standard-37002-on-whistleblowing-systems/, accessed 26 January 2021.

Previtali, P. and Cerchiello, P., 2018. The determinants of whistleblowing in public administrations: an analysis conducted in Italian health organizations, universities, and municipalities. Public Management Review, 20(11), pp.1683-1701.

Sánchez, R.M.S., 2019. El Buzón Ético y de Buen Gobierno del Ayuntamiento de Barcelona. Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal, (6), pp.59-72.

Sifry, M.L., 2011. WikiLeaks and the Age of Transparency. OR Books.

7. References

US Census Bureau (2020). Disclosure avoidance and the 2020 Census. Online at: https://www.census.gov/about/policies/privacy/statistical_safeguards/disclosure-avoidance-2020-census.html, accessed 26 January 2021.

Vandekerckhove, W., 2016. Freedom of expression as the “broken promise” of whistleblower protection. La Revue des droits de l’homme. Revue du Centre de recherches et d’études sur les droits fondamentaux, (10).

Verschuuren, P., 2020. Whistleblowing determinants and the effectiveness of reporting channels in the international sports sector. Sport Management Review, 23(1), pp.142-154.

Wiener, A. (2020) Taking Back our Privacy, The New Yorker. Online at: https://www.newyorker.com/magazine/2020/10/26/taking-back-our-privacy, accessed 26 January 2021.

Xnet (2017) Clonación del buzón anónimo de Xnet: nuevo buzón de denuncias anónimas de l’Oficina Antifrau de Catalunya, online at: https://xnet-x.net/clonacion-buzon-xnet-antifrau-catalunya/, accessed 26 January 2021.

Appendix A - Secure online dropbox instances

The following list of active dropboxes was produced for the EAT Project, based in part on information from Hermes and the Freedom of the Press Foundation. The many Italian GlobaLeaks dropboxes set up as part of the WhistleblowingPA project have not been included here (https://www.whistleblowing.it/adesioni/). Most dropboxes provided by commercial entities will also not be included on this list. All links were active as of 31 January 2021.

Name	Sector	Country	URL	Provider
2600	Media	USA	https://www.2600.com/securedrop/	SecureDrop
ABC	Media	Australia	https://www.abc.net.au/news/securedrop/	SecureDrop
AfriLeaks	Civil Society	International	https://secure.afrileaks.org/#/	GlobaLeaks
Aftonbladet	Media	Sweden	https://securedrop.org/directory/aftonbladet/	SecureDrop
The Age	Media	Australia	https://www.theage.com.au/confidential-news-tips/securedrop	SecureDrop
Agencia Valenciana Antifraude	Public Sector	Spain	https://bustiadenuncies.antifraucv.es/#/	GlobaLeaks
Agenzia regionale per la tecnologia e l'innovazione (ARTI)	Public Sector	Italy	https://whistleblowing.arti.puglia.it/#/	GlobaLeaks
Al Jazeera	Media	Katar	https://www.aljazeera.com/tips/	SecureDrop
Espen Andersen	Media	Norway	https://espenandersen.no/contact	SecureDrop
Angelini	Private Sector	Italy	https://segnalazioni.angelini.it/	GlobaLeaks
Autorità Nazionale Anticorruzione (ANAC)	Public Sector	Italy	https://servizi.anticorruzione.it/segnalazioni/#!/#%2F	GlobaLeaks

Appendix A - Secure online dropbox instances

Name	Sector	Country	URL	Provider
Atlatzso	Media	Hungary	https://atlatszo.hu/magyarleaks/	GlobaLeaks
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)	Public Sector	Germany	https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=2BaF6&c=-1&language=ger	BKMS
BalkanLeaks	Media	Bulgaria	http://3qf4wewa5bojmcgr.onion	SecureDrop
Berliner Zeitung	Media	Germany	https://www.berliner-zeitung.de/missstandshinweis.226	SecureDrop
Bundesdruckerei	Public Sector	Germany	https://report.whistleb.com/de/bundesdruckerei	WhistleB
Business Insider	Media	USA	https://www.businessinsider.com/how-to-tip-business-insider-securely-guide-signal-securedrop-2017-6	SecureDrop
Bústia Ètica Barcelona	Public Sector	Spain	https://bustiaetica.barcelona.cat/#/?lang=ca	GlobaLeaks
Buzzfeed	Media	USA	https://securedrop.org/directory/buzzfeed/	SecureDrop
CBC News	Media	Canada	https://www.cbc.ca/securedrop/	SecureDrop
Center for Investigative Reporting	Media	USA	http://leak.revealnews.org/	SecureDrop

Appendix A - Secure online dropbox instances

Name	Sector	Country	URL	Provider
Center for Public Integrity	Media	USA	https://apps.publicintegrity.org/tips/	SecureDrop
ChileLeaks	Civil Society	Chile	https://chileleaks.org/denuncia.html	GlobaLeaks
Dagens Naeringsliv	Media	Norway	https://www.dn.no/staticprojects/2016/12/securedrop/	SecureDrop
Daily Beast	Media	USA	https://www.thedailybeast.com/tips	SecureDrop
Dallas Morning News	Media	USA	https://interactives.dallasnews.com/secure-drop/	SecureDrop
Dr Oetker	Private Sector	Germany	https://coho.oetker-group.com/#/	GlobaLeaks
Edison	Private Sector	Italy	https://segnalazioni.edison.it/#/	GlobaLeaks
Ethics and Anticorruption Commission	Public Sector	Kenia	https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=111KACC33&language=eng	BKMS
Falck Renewables	Private Sector	Italy	https://segnalazioni.falckrenewables.eu/	GlobaLeaks
Ferrocarrils de la Generalitat de Catalunya (FGC)	Public Sector	Spain	https://canalcompliment.fgc.cat	GlobaLeaks
FT	Media	United Kingdom	https://ft.com/news-tips/	SecureDrop
Funding Fish	Civil Society	United Kingdom	https://fishyleaks.eu/en/	GlobaLeaks

Appendix A - Secure online dropbox instances

Name	Sector	Country	URL	Provider
Barton Gellman	Media	USA	https://tcfmailvault.info/	SecureDrop
Generalitat of Catalunya	Public Sector	Spain	http://governobert.gencat.cat/ca/bustia-etica/	GlobaLeaks
Global Reporting Centre	Public Sector	Canada	https://globalreportingcentre.org/tips/	SecureDrop
Global Witness	Civil Society	United Kingdom	https://www.globalwitness.org/en/securedrop/	SecureDrop
The Guardian	Media	United Kingdom	https://www.theguardian.com/securedrop	SecureDrop
Claudio Guarnieri	Civil Society	International	https://nex.sx/contacts/	SecureDrop
Harvard IQSS	Public Sector	USA	https://www.hmdc.harvard.edu/securedrop.html	SecureDrop
Heise Investigativ	Media	Germany	https://www.heise.de/investigativ/briefkasten/	SecureDrop
Houston Chronicle	Media	USA	https://projects.houstonchronicle.com/newstips/	SecureDrop
ICIJ	Media	International	https://www.icij.org/leak/	SecureDrop
IndonesiaLeaks	Civil Society	Indonesia	https://www.indonesialeaks.id/	GlobaLeaks
The Intercept	Media	USA	https://theintercept.com/source/#securedrop	SecureDrop

Appendix A - Secure online dropbox instances

Name	Sector	Country	URL	Provider
IrpiLeaks	Media	Italy	https://irpimedia.irpi.eu/diventa-una-fonte/irpileaks/	GlobaLeaks
Le Journal de Montreal	Media	Canada	https://www.journaldemontreal.com/dossiers-secrets	SecureDrop
Jean-Marc Manach	Media	France	https://jean-marc.manach.net/securedrop.html	SecureDrop
Kommunal Report	Media	Norway	https://securedrop.kommunal-rapport.no/	SecureDrop
Leaks.ng	Media	Nigeria	https://www.leaks.ng/	GlobaLeaks
Lleida City Hall	Public Sector	Spain	https://www.paeria.cat/bustiaetica/ca/index.asp_	GlobaLeaks
La Marzocco	Private Sector	Italy	https://segnalazioni.lamarzocco.com	GlobaLeaks
Lucy Parsons Labs	Civil Society	USA	https://invisible.institute/contact	SecureDrop
Stefania Maurizi	Media	Italy	https://stefaniamaurizi.it/en-contactme.html	SecureDrop
The Markup	Media	USA	https://themarkup.org/tips	SecureDrop
McClatchy DC	Media	USA	https://www.mcclatchydc.com/customer-service/contact-us/#navlink=mi_footer	SecureDrop

Appendix A - Secure online dropbox instances

Name	Sector	Country	URL	Provider
Meduza	Media	Russia	https://meduza.io/cards/u-menya-est-vazhnaya-informatsiya-dlya-meduzy-no-ya-boyus-ee-peredavat-kak-sdelat-eto-po-nastoyaschemu-anonimno	SecureDrop
Government of Mexico	Public Sector	Mexico	https://alertadores.funcionpublica.gob.mx/	GlobaLeaks
MexicoLeaks	Media	Mexico	https://mexicoleaks.mx/enviar.html	GlobaLeaks
NBC	Media	USA	https://www.nbcnews.com/securedrop	SecureDrop
New York Times	Media	USA	https://www.nytimes.com/tips#securedrop	SecureDrop
NOYB	Civil Society	Austria	https://noyb.eu/en/securedrop	SecureDrop
NRK	Media	Norway	https://www.nrk.no/varsle/#part1	SecureDrop
OCCRP	Media	International	https://www.occrp.org/en/aboutus/securedrop/	SecureDrop
Oficina Antifrau de Catalunya	Public Sector	Spain	https://denunciesanonimes.antifrau.cat/#/?lang=esp	GlobaLeaks
Oživení	Civil Society	Czechia	https://secure.oziveni.cz/#/	GlobaLeaks
PeruLeaks	Civil Society	Peru	http://leaks.pe/#	GlobaLeaks

Appendix A - Secure online dropbox instances

Name	Sector	Country	URL	Provider
Pištaljka	Civil Society	Serbia	https://pistaljka.rs/	GlobaLeaks
Politico	Media	USA	https://www.politico.com/news-tips/	SecureDrop
Kevin Poulsen	Media	USA	https://freedom.press/people/kevin-poulsen/	SecureDrop
ProPublica	Media	USA	https://www.propublica.org/tips/	SecureDrop
Publeaks.nl	Media	The Netherlands	https://secure.publeaks.nl/#/	GlobaLeaks
Public Intelligence	Civil Society	USA	https://publicintelligence.net/contribute/	SecureDrop
Radio Canada	Media	Canada	https://sourceanonyme.radio-canada.ca/	SecureDrop
Reflets.info	Media	France	https://reflets.info/secure-contact	SecureDrop
Reuters	Media	USA	https://www.reuters.com/investigates/special-report/tips/	SecureDrop
RINA	Private Sector	Italy	https://whistleblowing.rina.org/	GlobaLeaks
Rise.md	Media	Moldova	https://www.rise.md/leaks/	SecureDrop
Rue89	Civil Society	France	http://alerte.rue89locaux.com	GlobaLeaks
RUV Kveikur	Media	Iceland	https://www.ruv.is/kveikur/opnum-securedrop/	SecureDrop

Appendix A - Secure online dropbox instances

Name	Sector	Country	URL	Provider
SAES Group	Private Sector	Italy	https://segnalazioni.saesgetters.com	GlobaLeaks
Schwartz Media	Media	Australia	https://www.themonthly.com.au/tips	SecureDrop
Siemens	Private Sector	Germany	https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=19siem14&c=-1&language=ger	BKMS
Slate	Media	USA	https://slate.com/tips	SecureDrop
Gruppo Sole 24 Ore	Media	Italy	https://segnalazioni.gruppo24ore.com/#/	GlobaLeaks
Sourcesûre	Media	France	https://ensecurite.sourcesure.eu/#/	Globaleaks
Subterraneo	Civil Society	Nicaragua	https://subterraneoni.org/	GlobaLeaks
Süddeutsche Zeitung	Media	Germany	https://www.sueddeutsche.de/projekte/kontakt/	SecureDrop
Stuff.co.nz	Media	New Zealand	https://www.stuff.co.nz/securedrop/index.html	SecureDrop
Svenska Dagbladet	Media	Sweden	https://www.svd.se/securedrop/	SecureDrop
Technopolice	Civil Society	France	https://technopolice.fr/leak/	SecureDrop

Appendix A - Secure online dropbox instances

Name	Sector	Country	URL	Provider
The Telegraph	Media	United Kingdom	https://www.telegraph.co.uk/news/investigations/contact-us/	SecureDrop
Terrassa City Hall	Public Sector	Spain	https://bustiaetica.terrassa.cat/	GlobaLeaks
Toronto Crime Stoppers	Civil Society	Canada	https://www.222tips.com/SecureDrop	SecureDrop
Transparency International Ireland	Civil Society	Ireland	https://lostineurope.eu/	GlobaLeaks
Transparency International Italia	Civil Society	Italy	https://alac.transparency.it	GlobaLeaks
Transparency International Kosovo	Civil Society	Kosovo	https://raporto.kdi-kosova.org/#/	GlobaLeaks
Transparency International Portugal	Civil Society	Portugal	https://provedoria.transparencia.pt/	GlobaLeaks
Transparency International Tunisia	Civil Society	Tunisia	https://billkamcha.tn/	GlobaLeaks
USA Today	Media	USA	https://newstips.usatoday.com/securedrop.html	SecureDrop
The Verge	Media	USA	https://www.theverge.com/a/tip-us-secure-contact-email	SecureDrop
VG	Media	Norway	https://www.vg.no/securedrop/	SecureDrop
Wall Street Journal	Media	USA	https://www.wsj.com/tips	SecureDrop

Appendix A - Secure online dropbox instances

Name	Sector	Country	URL	Provider
Washington Post	Media	USA	https://www.washingtonpost.com/securedrop/	SecureDrop
WildLeaks	Civil Society	USA	https://wildleaks.org/how-wildleaks-works/	SecureDrop
Wired	Media	USA	https://www.wired.com/securedrop/	SecureDrop
Die Zeit	Media	Germany	https://meine.zeit.de/briefkasten	Briefkasten
Zvizgac	Media	Slovenia	https://zvizgac.si/	SecureDrop

Appendix B - Dropbox instances surveyed by DiSalvo (2020)

Secure online dropbox operators surveyed by Philip Di Salvo. Not all of these projects are still online.

Source: Di Salvo 2020: 110

Publishing	**Collaborative**	**Multistakeholder**	**Media**
BalkanLeaks	BayLeaks	AfriLeaks	Die Zeit Briefkasten
Ecuador Transparente	ExpoLeaks	MafiaLeaks	News Leaks
InfodioLeaks	IrpiLeaks	MexicoLeaks	NRKBeta
MagyarLeaks	Filtrala	PubLeaks	ProPublica
Pistaljka	WildLeaks	Source Sure	The Globe and Mail
POGO			The Sun

Appendix C - EAT Project dropboxes

This list reflects dropboxes that were active during the project. Other dropboxes are likely to come online after the formal end of the project.

Country	Organization	Description	Dropbox URL
Italy	Ferrovie Calabria	Private company	https://ferroviecalabria.disclosers.eu/#/
Italy	Ciao people	Private company	https://backstairfanpage.disclosers.eu/#/
Bulgaria	Anti Corruption Fund	NGO	http://acf.disclosers.eu/#/
Bulgaria	Ministerio de Defensa	Public agency	http://armymedia.disclosers.eu/#/
Bulgaria	Ayuntamiento de Tryavna	Public agency	http://tryavna.disclosers.eu/#/
Bulgaria	OffNews Media Group	Private company	http://offnews.disclosers.eu/#/
Romania	Fair Mediasind	Journalists' Union	http://fairmediasind.disclosers.eu/#/
Greece	Autoridad única e independiente para la contratación pública (EAADHSY)	Public agency	http://whistle2eaadhsy.disclosers.eu/#/
Greece	Sol Consulting	Private company	http://whistle2solconsulting.disclosers.eu/#/
Greece	Crowe Greece	Private company	http://whistle2sol.disclosers.eu/#/
Czechia	Brno Stred	Public Agency	https://brnostred.disclosers.eu/#/
Spain	Federación de Sindicatos de Periodistas (FeSP)	Journalists' Union	http://aslertasfesp.disclosers.eu
Spain	FIBGAR	NGO	http://alertacovid19.disclosers.eu/#/
Cyprus	Legal Legion Cyprus	NGO	https://3lcy.disclosers.eu/

Appendix D - List of interviewees

Interviews included representatives of the following:

EAT Partners

Atlatszo (Hungary)
CIJ (Romania)
The Good Lobby (Italy)
MDC (Bulgaria)
Oživení (Czechia)

Media organisations

OCCRP (multi-country)

Non governmental organisations

Freedom of the Press Foundation (USA)
Pištaljka (Serbia)
Transparency International Italy

Public institutions

BaFin (Germany)
Catalunya Antifraude (Spain)

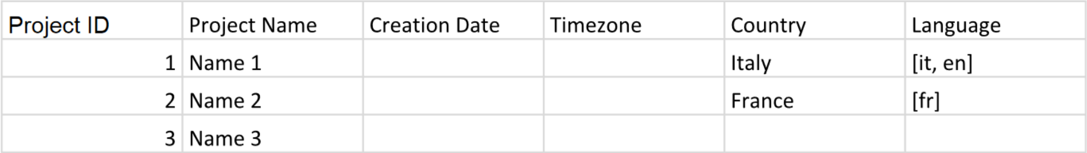
We also drew on The Guardian's contribution to the following online seminar:

https://www.youtube.com/watch?v=1mI3uQnXPdM

Some interviewees preferred not to be cited directly, therefore are not included in this list.

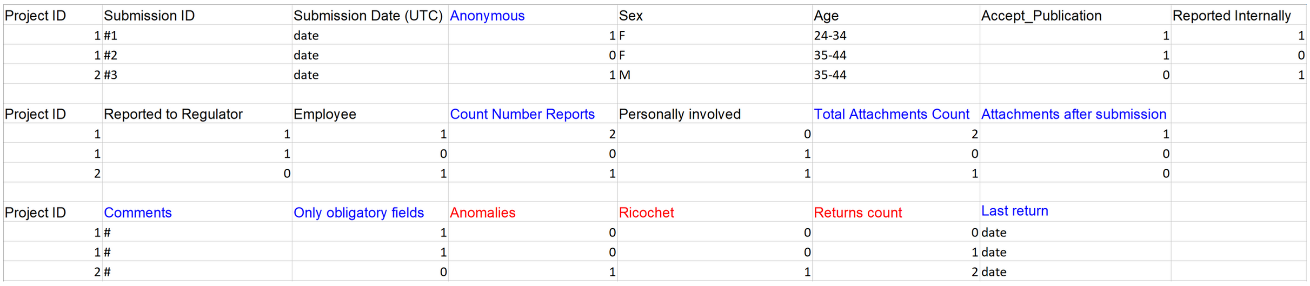
Appendix E - Metadata table

Instances



Project ID	Project Name	Creation Date	Timezone	Country	Language
1	Name 1			Italy	[it, en]
2	Name 2			France	[fr]
3	Name 3				

Submissions



Project ID	Submission ID	Submission Date (UTC)	Anonymous	Sex	Age	Accept_Publication	Reported Internally
1	#1	date	1	F	24-34	1	1
1	#2	date	0	F	35-44	1	0
2	#3	date	1	M	35-44	0	1

Project ID	Reported to Regulator	Employee	Count Number Reports	Personally involved	Total Attachments Count	Attachments after submission	
1	1	1	2	0	2	1	
1	1	0	0	1	0	0	
2	0	1	1	1	1	0	

Project ID	Comments	Only obligatory fields	Anomalies	Ricochet	Returns count	Last return	
1	#	1	0	0	0	date	
1	#	1	0	0	1	date	
2	#	0	1	1	2	date	

Appendix F - Research questions

EAT – how we collect data for research purposes

Setting up 250 anonymous drop boxes across 10 EU countries is a major undertaking. A key part of the EAT project is to use this experience to understand how these platforms work in practice and what are the factors that make them more effective.

The EAT platform will remain operational for Your organisation at least until January 31th, 2021. Hermes Center for Human Rights (the maintainer of the platform) will share during the project certain specific metadata [1] with the researching organisation Blueprint for Free Speech, who will conduct a statistical analysis on aggregated metadata and write a final report. The type of data which will be shared is listed below.

The project is deliberately adopting a conservative approach to metadata sharing. The metadata shared with Blueprint for Free Speech are the minimum necessary metadata to conduct a useful analysis.

There is **no report content shared with EAT partners**, and all metadata is in an anonymised format: the consortium, in particular Hermes and Blueprint for Free Speech are not able to link a questionnaire response to any specific disclosure.

What questions are we trying to answer?

We have developed a series of research questions that tackle the following main issues:

- Can we replicate findings from other whistleblowing research?
- Does the success of anonymous whistleblowing channels depend on their visibility? What kind of promotion works best?
- How are whistleblowing channels used in practice? Are they being used safely?
- Has the EAT Project fulfilled its aims?

For the full list of research questions, please see Appendix 1.

What data are we collecting?

There are three main categories of data we are collecting:

- Whether a report is marked ‘open’ or ‘closed’ at the receiving organisation end.
- Some limited categories of metadata (“information about information”, listed below).

[1] Metadata describes other data. It provides information about a certain item's content. For example, an image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data.

Appendix F - Research questions

List of metadata collected:

Due to the nature of the project, we are limiting collection to a few set categories. These will include the following:

- For each instance (each individual dropbox), we will record an ID, Project Name, time zone, country and language.
- For each submission, we record:
    - A unique ID
- When the reporting person logged in to the site
- What time a submission was made
- How many documents were submitted, if any
- Whether the reporting person used Tor
- Whether the reporting person clicked on a link to the Ricochet Refresh site
    - How many times the reporting person returned to the website after making a submission
    - The last date the reporting person logged in to the site
    - Whether an anomalous event (an attack on the dropbox) has been recorded.

Note:
For any doubt or question about the full questionnaire in place, please see Appendix 2.

Appendix F - Research questions, 1

Research questions

Will whistleblowers use anonymous channels if they are provided?

Does the provision of anonymous reporting channels result in actionable reports?

Do whistleblowers prefer to use external channels? Is mandatory internal reporting necessary?

Are whistleblowers happy for their reports to be shared with third parties?

What characteristics do whistleblowers share?

How important are intermediaries (lawyers, NGOs, unions etc)?

How important are legal frameworks?

How large is the risk of abuse and of submissions being not serious?

Does media coverage affect the use of channels?

Does the attitude of the receiving entity make a difference?

What kind of response can whistleblowers expect?

Do whistleblowers want anonymity?

Are digital whistleblowing channels accessible? Are they being used safely?

How do whistleblowers use electronic channels? Is two-way communication important?

Do digital whistleblowing channels come under attack?

Does the submission model adopted make a difference?

Appendix F - Research questions, 2

Draft EAT Questionnaire with program notes (V3)

* indicates an obligatory field

SECTION 1 – PRELIMINARY INFORMATION

PROG NOTE:
ADD AT TOP OF SCREEN THE FOLLOWING MESSAGE AND A HORIZONTAL SLIDER THAT SHOWS PERCENTAGE OF QUESTIONS ANSWERED

“There are 28 questions that follow. These will help the intended recipient of your disclosure to understand what it is about.

We also ask for some statistical data, which does not identify you. We do this to help the team supporting this dropbox to understand how to improve it in future.

You only have to answer the boxes with a * next to the question to move forward in the submission. The other questions are optional. You can exit the process at any time.”

PROG NOTE:
ADD NEXT, WITH A LINK TO TOR BROWSER DOWNLOAD SITE

If you want to be anonymous, you must use the software program Tor to make a submission to this site. You can download the Tor Browser here <Add hyperlink>. It works like Safari, Chrome or other web browsers, except that it hides where you are coming from. If you download the browser, and then return to this site using that Tor Browser, your internet address will be hidden from anyone at this site.

This dropbox’s Terms and Conditions

Please confirm by ticking this box* <Insert Box> that you understand that if you do not use Tor, it results in the inability to protect your anonymity.
To further improve your security, follow the instructions below:

- In case you want to remain anonymous, do not send any personal data (such as your name or the type of relationship you have with the person you are making a disclosure about, or any information that could be used to track you down).
- Please do not send any data from a PC provided by your employer. A connection in a local network could jeopardize your anonymity.

By ticking this second box, you confirm that you accept these terms and conditions.* <Insert Box>

Appendix F - Research questions, 2

SECTION 2 – TELL US ABOUT THE WRONGDOING

Q1. What kind of organisation is your report about? *

PROG NOTE:
- SINGLE RESPONSE

1. A private company
2. A public body
3. Other
4. Don’t know / prefer not to say

P2. Have you tried to report this before? *

PROG NOTE:
- SINGLE RESPONSE
- RANDOMISE 1-2

1. Yes
2. No GOTO 5
3. Don’t know / Prefer not to say GOTO 5

Q3. Who have you tried to report this to? Select all that apply. You can also “prefer not to say”.*

PROG NOTE:
- MULTIPLE RESPONSES ALLOWED
- RANDOMISE 1-9

1.Superior
2.Colleague
3.Compliance officer
4.An advice line run or contracted by my employer
5.An industry regulator or ombudsman
6.A union, professional group or industry body
7.Police or other law enforcement
8.A journalist or other media
9.A lawyer
10.Other - please specify (OPEN TEXT FIELD)
99.Prefer not to say

Appendix F - Research questions, 2

Q4. What was the outcome of your report? *

PROG NOTE:
- SINGLE RESPONSE
- RANDOMISE 1-4

1.No response
2.Adequate response
3.Inadequate response
4.My report is being investigated
99.Don't know / prefer not to say

Q5. Is there a reason why haven't you reported this before?

PROG NOTE:
- OPEN TEXT FIELD

Q6. What is your relationship to the organisation you are reporting on? *

PROG NOTE:
- SINGLE RESPONSE
- RANDOMISE 1-6

1.Employee
2.Former employee
3.Supplier
4.Sub-contractor or consultant
5.Volunteer
6.Customer
7.Other – please specify (OPEN TEXT FIELD)
99.Don't know / Prefer not to say

Q7. What is your level of involvement in the subject matter of your report? *

PROG NOTE:
- SINGLE RESPONSE
- RANDOMISE 1-4

1.I'm involved personally
2.I have first-hand knowledge
3.I've heard about it
4.I have been harmed
99.Other/Prefer not to say

Appendix F - Research questions, 2

SECTION 2 – YOUR REPORT

[2.1 BASIC REPORTING FIELDS]

Q8. Please give a brief summary of your report (in a maximum 200 characters). *

PROG NOTE:
- OPEN TEXT FIELD
- 50-200 characters

Q9. Please describe your report in more detail.*

PROG NOTE:
- OPEN TEXT FIELD

Q10. Attach documents to support your report.

PROG NOTE:
- ADD FILE BUTTON

[2.2 ADDITIONAL INFORMATION]

Q11. When did the wrongdoing happen?

PROG NOTE:
- OPEN TEXT FIELD

Q12. Is the wrongdoing ongoing or likely to happen again?

PROG NOTE:
- SINGLE RESPONSE

1.Yes
2.No

Q13. Who benefited from the wrongdoing?

PROG NOTE:
- OPEN TEXT FIELD

Appendix F - Research questions, 2

Q14. Does the wrongdoing put anyone at risk, or has anyone been harmed?

PROG NOTE:
- SINGLE RESPONSE

1.Yes
2.No

Q15. Do you feel that you are at risk, or have been harmed?

PROG NOTE:
- SINGLE RESPONSE

1.Yes
2.No

Q16. Which of the following best describes what your report is about? You can select more than one option. *

PROG NOTE:
- MULTIPLE RESPONSE
- RANDOMISE 1-9

1.Fraud or theft
2.Unfair recruitment practices GOTO 18
3.Conflict of interest or other improper decision making GOTO 18
4.Misuse of information, including unauthorised access or release GOTO 18
5.Bribery or corruption
6.Waste or mismanagement of resources
7.Lack of accountability, or covering up wrongdoing GOTO 18
8.Danger to public health, safety or the environment GOTO 18
9.Workplace conditions, bullying or harassment GOTO 18
10.Other – please specify (OPEN TEXT FIELD)
11.Don’t know / prefer not to say

Q17. What do you think has been the economic cost of the wrongdoing?

PROG NOTE:
- OPEN TEXT FIELD

Q18. Can you provide us with any useful information to verify the authenticity of your report? If you don’t hold the information yourself, can you tell us where the data exists and could be accessed?

PROG NOTE:
- OPEN TEXT FIELD

Appendix F - Research questions, 2

Q19. Who are the people involved in the incident?

PROG NOTE:
- OPEN TEXT FIELD

Q20. Which companies or entities are involved?

PROG NOTE:
- OPEN TEXT FIELD

SECTION 3 – ABOUT YOU

This section is completely optional. You can choose to answer some, all or none of the following questions.

Q21. Do you want to tell us who you are?

PROG NOTE:
- SINGLE OPTION

1. No - GOTO 24
2. Yes

Please do not answer any questions that you are at all unsure or uncomfortable about. You do not need to answer any of these questions to submit your report.

Q22. What is your name?

PROG NOTE:
- OPEN TEXT FIELD

Q23. How old are you?

PROG NOTE:
- SINGLE RESPONSE

1. Under de 16
2. 16-24
3. 24-34
4. 35-44
5. 45-54
6. 55-64
7. 65-75
8. 75+

Appendix F - Research questions, 2

Q24. What is your gender?

PROG NOTE:
- SINGLE RESPONSE
- RANDOMISE 1-2

1. Male
2. Female
3. Other
4. Prefer not to say

Q24. Location

PROG NOTE:
- OPEN TEXT FIELD

Q25. Job title

PROG NOTE:
- OPEN TEXT FIELD

Q26. Do you want to provide any contact details?

1. No - GOTO 28
2. Yes

Please do not answer any questions that you are at all unsure or uncomfortable about. You do not need to answer these questions to submit your report.

Q27. Please supply contact details here if you would like to.

PROG NOTE:
- OPEN TEXT FIELD

Q28. Is there anything else you would like to tell us?

PROG NOTE:
- OPEN TEXT FIELD

Section 3. Do you want to have an online chat with us?
If you would like us to be able to contact you for clarification or feedback, but you want to have a technological guarantee of anonymity, download free software called Ricochet IM here <link to Ricochet IM>. Install it, get a Ricochet ID, and type the ID here <Space for a ricochet ID here>.

Appendix F - Research questions, 2

P
The Ricochet ID of the recipient of this dropbox is <ID HERE>
The Ricochet ID of the tech team who runs this box is <ID HERE>

When we next log on, we will try to contact you online, but you must have Ricochet open to do so. Don’t use it from work.

New section : Do you require urgent assistance ?

Appendix G - Summary list of common ways a discloser may be identified online if not using a secure anonymous dropbox

The anonymity provided by a secure digital dropbox plays a crucial role in protecting a whistle-blower. The challenge is both a technical and user one, in that even if the technology is available, it depends on the user understanding and being able to use it. In this section we will briefly describe some of the risks when using a dropbox without adequate anonymity protection.

The threats against a whistle-blower can be thought of as operating at different levels:

- Local – the machine, device, or environment the whistle-blower uses to make their submissions
- Network – the communications infrastructure, both internal and external that is used to send the submission
- Remote – the receiving dropbox and associated metadata

Local

Local threats are difficult to counter as they depend on the whistle-blower taking appropriate action to protect themselves. This can be particularly challenging if a whistle-blower is attempting to make a submission from within a corporate or organisation network, and hence do not have full control over the equipment or environment.

- Device monitoring – corporate and organisation devices are often monitored for both software installs, websites, and potentially even resource access. This can counter even anonymous dropboxes since it effectively monitors the source. Countering is primarily down to good user education, in particular, if they don't own/control the device they are using they are at risk of monitoring.
- Environment monitoring – even if the whistle-blower controls the device they may be subject to environmental monitoring, i.e. the times they are in the building, where in the building they are. Again, countering this requires good user education.

Network

Network monitoring is commonplace both within organisations and more broadly by communication providers. Standard security approaches taken for services such as online banking and shopping are not sufficient to protect against monitoring and profiling of a whistle-blower.

- TLS Interception – the public have become accustomed to trusting TLS as a way of protecting their online activities from observation. However, in practice, TLS is often intercepted within corporate and government networks. TLS interception is a core component of cyber security monitoring in corporate networks, and is a largely automated process. It can be transparent to the average user making it extremely difficult to detect. Usage of techniques like Certificate Pinning and anonymous routing like Tor can help detect or, in the case of the latter, counter such threats. Again, if the user does not control the device they could be at risk.

Appendix G - Summary list of common ways a discloser may be identified online if not using a secure anonymous dropbox

- DNS Monitoring – Even when TLS is not being intercepted, the Domain Name Service (DNS) lookups, which map a web address to an IP address can be either monitored or redirected. This reveals which sites an individual is visiting. It does not reveal the contents or the pages visited, but would be sufficient to detect who had accessed a particular dropbox service. Usage of secure DNS is becoming more popular, but if the DNS server is internal, or hosted by an untrusted third-party, such monitoring can still take place. This is a particular concern with Internet Service Providers, which frequently use their own DNS servers and can therefore determine all the sites their customers visited, and therefore potentially identify someone accessing a dropbox.

- Traffic Analysis – even if the DNS is protected and the traffic is encrypted, there remains a risk of traffic analysis, this is particularly true for ISPs and corporate networks. Whilst they may not be able to see the content, they may be able to determine the size of a request being sent to the server. If they are aware of the document that may have been uploaded there is a chance they will be able to determine from where the upload originated by searching for a submission request of suitable size. This is dependent on the nature of the submission and how dissimilar it is to normal traffic. Large uploads present a potentially greater danger as they may be relatively unusual on the network.

Remote

Remote vulnerabilities occur on or near the destination server. They are difficult for the user to be aware of, since they do not have sight of, or information about the remote infrastructure.

- Load balancing/TLS Proxying – if a dropbox is hosted in third-party cloud infrastructure, or utilises load balancers, Web Application Firewalls, or Content Delivery Networks there is a chance that the TLS connection will be being intercepted by the provider of that service. This is necessary to provide the load balancing, or firewall/protection of the final destination server. However, such interception will be invisible to the user, but would require the user to trust the third-party to protect their anonymity. Usage of anonymous routing technology like Tor can help counter such threats.

- Meta-data collection – requests to a web server typically create a large amount of metadata, from information about the device making the request, through to the IP address of the device. It is important that such logs are protected and ideally destroyed within a short window to protect such data from unauthorised access by administrators, theft during an hack of the server, or access by law enforcement. Users can use Tor to better protect themselves.

Appendix H - Further resources

EAT partners

Fundación Internacional Baltasar Garzón (FIBGAR)

Coordinator of the Project, Spain. FIBGAR is based on the pillars of solidarity, respect, the promotion of Human Rights, village development cooperation, mediation and the fight against impunity.

With these bases FIBGAR encourages action programs from the areas of education, justice, society, politics and culture to defend and apply Human Rights in defense of victims and their rights to truth, justice and repair and to prosecute corruption and organized crime in all its forms.

The basic tools to promote the activities that constitute the essence of the Foundation, will be research, training and cooperation with other foundations, organizations and academic, social, political and legal entities coupled with direct action in coordination with relevant actors.

web: https://www.fibgar.org/

Hermes Center

Our mission is to promote and develop in the society the awareness of and the attention to transparency and accountability, be they related to the society-at-large or not. Our goal is to increase the citizens' involvement in the management of matters of public interest and to boost the active participation of workers and employees to the correct management of corporations and companies they work for.

web: https://www.hermescenter.org/

Blueprint for Free Speech

Blueprint for Free Speech is non-profit charity that works internationally to promote the right to freedom of expression without undue interference or intrusion. Our research and advocacy strive to defend Article 19 of the Universal Declaration of Human Rights, which asserts the right to freedom of opinion and expression for all people.

web: https://blueprintforfreespeech.net/en/1577-2/

Appendix H - Further resources

Atlatszo.hu Kozhasznu Nonprofit Korlatolt Felelossegu Tarsasag – Hungary

Atlatszo.hu is a watchdog NGO and online newspaper for investigative journalism to promote transparency, accountability, and freedom of information in Hungary.

Established in 2011, atlatszo.hu – “atlatszo” means transparent in Hungarian – produces investigative reports, accepts information from whistleblowers, files freedom of information requests, and commences freedom of information lawsuits in cases where its requests are refused.

web: https://english.atlatszo.hu/about-us-fundraising/

Fundația Centrul Pentru Jurnalism Independent (CPJI) – Romania

The Center for Independent Journalism is a non-profit organization, with 25 years of experience, which acts as a watchdog of professional and quality journalism, by protecting journalism standards and developing a balanced, honest and responsible media environment.

CIJ is an active promoter of responsible, ethical and professional journalism in Romania and advocates for an informed public, as a prerequisite for any democratic society.

web: www.cji.ro

Transparency International Greece (TI-GR) – Greece

TI Greece was founded in 1996 by a group of high-profile professionals including former politicians, businessmen, scientists, journalists, lawyers, public officers and private employees which decided to make a stance against corruption.

TI-Greece calls for transparent and ethical principles to be implemented for good governance and to fight corruption that undermines Greece’s political and financial system. TI-G’s vision is to combat indifference and ignorance towards issues of transparency.

To fulfill its vision TI-G is currently involved to anti-corruption projects such as the Integrity Pact, Integrity Watch and the Expanding Anonymous Tipping Technology Deployment, Operation, and Trustworthiness to Combat Corruption in Eastern and Southern Europe by promoting the adoption of Whistleblowing online platforms to certain public and private entities.

web: http://www.transparency.gr/ti-kanoume/whistleblowing/e-a-t/

Appendix H - Further resources

Fondatsiya Tsentar Za Razvitie Na Mediite (MDC) – Croatia and Bulgaria

Media Development Center, Sofia (MDC) is a non-profit, non-partisan organization founded in 1998. It was established to promote independent media in Bulgaria, and to foster capacity-building of the media by encouraging good practice in journalism, stimulating the professional ethics, institutionalizing the dialogue among the state administration, the media and the NGO sector and to boost the networking and cross-border cooperation in the region of Southeast Europe.

web: http://www.mediacenterbg.org/about-us/

Oživení – Czech Republic

We endeavour to increase the transparency of decision-making processes and financial management at public institutions in the Czech Republic, as well as the personal liability of public officials, and thereby to boost the active participation of citizens. Our main areas of interest include the right to information, public procurement and management of public property. Last but not least, we are involved in spreading anti-corruption know-how and educating and networking anti-corruption and civic activists.

web: https://www.oziveni.cz/

The Good Lobby Italia – Delegación en Italia

The Good Lobby Italia is the Italian chapter of Brussels-based organisation The Good Lobby active in Europe since 2015. We work in order to make society more democratic, more participative, and fair. Every citizen can make a difference for its community. We aim at influencing major policy decisions, hold our political representatives accountable and share with them new solutions facing society.

web: https://www.thegoodlobby.it/