



► Deliverable D3.2

Annual Development Review and TalkFree platform prototype

Author ► Project partner ► Date

Dissemination level	Public
Contractual date of delivery	Month 12 December 2016
Actual date of delivery	Month 14 February 2016
Work package	WP3 TalkFree Design and Development
Deliverable number	D3.2 Annual Development Review and TalkFree platform prototype
Type	Report
Approval status	Approved
Version	1.0
Number of pages	42
File name	D3_2-20170217_1_Cambridge.docx

Abstract

This report describes how the design of The Whistle has been developed in the first year of the project, and the plans for development going forward.

The information in this document reflects only the author's views and the European Community is not liable for any use that may be made of the information contained therein. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.



Co-funded by the European Union

History

Version	Date	Reason	Revised by
0.1	26/01/17	Structure	Richard Mills
0.5	01/02/17	First draft of most sections	Richard Mills
0.7	03/02/17	Added comments and materials	Isabel Guenette Thornton
0.9	09/02/17	Added comments and materials	Matthew Mahmoudi
1.0	15/02/17	Responded to comments, added new sections	Richard Mills

Author list

Organization	Name	Contact information
Cambridge University	Richard Mills	rm747@cam.ac.uk
Cambridge University	Matthew Mahmoudi	matt.3pehr@gmail.com
Cambridge University	Isabel Guenette Thornton	isabel.guenette.thornton@gmail.com

Executive Summary

This document describes the development of The Whistle’s design (originally provisionally referred to as ‘TalkFree’) in the first year of the project, and explains how the design of the platform has emerged from the user requirements gathering phase of the project.

A detailed plan for developing The Whistle is described along with the rationale for this approach. This plan calls for in-depth collaboration on design with the NGO partners that will run the first reporting campaigns, to ensure that The Whistle is positioned to serve these campaigns well and to maximise the efficiency with which we use our engineering resources. This deliverable also describes the set of features and approaches which The Whistle will ultimately support, along with illustrative design mock-ups and proof of concept prototypes.

It is our intention to submit an updated version of this deliverable ahead of the project’s interim review – deliverables for WP3 were scheduled in the expectation that reviews would be annual, we anticipate making significant progress in WP3 before M18 and will communicate this in an updated report ahead of the review.

Table of Contents

HISTORY.....	1
AUTHOR LIST.....	1
EXECUTIVE SUMMARY.....	1
TABLE OF CONTENTS.....	2
1 INTRODUCTION.....	3
1.1 REVISED APPROACH TO TALKFREE.....	3
2 DESIGN AND DEVELOPMENT OF THE WHISTLE IN YEAR 1.....	5
2.1 LESSONS FROM RESEARCH INFORMING DESIGN (WP2) AND RESEARCH ON COLLECTIVE AWARENESS PLATFORMS (WP7).....	6
2.2 AIMS OF THE WHISTLE.....	8
2.3 HIGH-LEVEL DESIGN.....	9
2.4 CIVILIAN WITNESS REPORTING INTERFACE.....	10
2.4.1 SMS/MMS MESSAGES.....	11
2.4.2 SMARTPHONE MESSAGING CLIENTS.....	11
2.4.3 WEB FORMS.....	12
2.4.4 INSTALLABLE SMARTPHONE APP.....	12
2.4.5 MESH NETWORKS.....	13
2.5 CIVILIAN WITNESS REPORTING INTERFACE – PROTOTYPES.....	14
2.5.1 MESSAGING APPROACH.....	14
2.5.2 WEB FORM APPROACH.....	19
2.6 FACILITATING VERIFICATION.....	20
2.6.1 VERIFICATION-AIDING SERVICES.....	20
2.6.2 YOUTUBE MULTITool PROTOTYPE.....	22
2.7 NGO DASHBOARD.....	22
2.8 DATA HANDLING AND EXTERNAL PUBLICATION.....	28
2.8.1 REPORT STORAGE.....	28
2.8.2 EXTERNAL PUBLICATION.....	28
2.8.3 DISTRIBUTED LEDGER AND BLOCKCHAIN.....	30
3 WP3 SMART TARGETS.....	31
4 APPENDIX.....	32
4.1 - WEB FORM CIVILIAN WITNESS FRONT-END MOCK-UPS.....	32
4.2 - YOUTUBE MULTITool.....	38

1 Introduction

In the early stages of the project, we identified a number of additional user requirements for the ‘TalkFree’ concept with respect to its initial description in the project’s Description of Work, mainly relating to security and transparency concerns. These necessitated a shift in emphasis away from open community analysis of incoming reports and towards closer partnership with the NGOs who would run reporting campaigns, with all incoming reports being processed by this NGO and only highly abstracted information about the reports being made publicly accessible. Section 1.1 details this initial revision to the initial concept of TalkFree (henceforth “The Whistle”), as communicated to the EC alongside the project’s response to the ethical evaluation. The concept has since been further developed, design work and development of components is underway, and the remainder of this document will describe our current plans for developing The Whistle.

1.1 Revised approach to TalkFree

We have adopted the name “The Whistle” for the reporting platform provisionally titled “TalkFree” at the beginning of the project. We have also elaborated more around the scope of how The Whistle platform will work, and the additional goals will be described in terms of how they modify the initial description of TalkFree.

The Whistle connects reporters and their reports directly to the organisation that is running the report-gathering campaign – optionally passing the report with accompanying attachments and meta-data through a number of APIs whose output can aid in checking whether a report represents credible evidence. The Whistle will not be a platform where any aspects of incoming reports are published directly, and no crowdsourcing will occur on this platform, as a new layer is being introduced to strengthen transparency and security aspects. .

The project’s approach to verification of civilian reports has been re-conceptualized. Initially this was described as an open community activity, but two major ethical issues with this were identified.

Firstly, many reporting campaigns will relate to sensitive issues where the civilian reporter may be at risk if they were identified. An initial planning to mitigate this was to only publish aspects of the reports which could not be used to identify individuals. In the initial stages of our ethics self-assessment this was determined to be problematic because 1) in response to an open question a reporter might unwittingly provide information that could be used to identify them and 2) verification will often be facilitated by access to the sensitive information that cannot be openly published.

Secondly, the verification of reports for (at least some) campaigns will not be an appropriate task for volunteer community members. The evidence submitted alongside reports for a campaign may include graphic or disturbing images/video/audio/description – this raises the possibility of secondary trauma suffered by the people who are conducting verification work. Where there is a risk of secondary trauma, it is not appropriate to conduct verification or analysis in the open with volunteer contributors.

Verifying reports is also a difficult (and high-stakes) task that benefits from expert knowledge and experience. Accepting a false report as genuine, or rejecting a genuine report as false, can have damaging effects on how the project is perceived, or on the reporter, respectively. Some NGOs already have members of staff

dedicated to the verification of civilian reports, and in some cases immediately publishing any details of a report would be counterproductive. For example, where there is a possibility of pursuing justice through the courts an incoming report is just the first step in a lengthy process of corroboration and evidence-gathering - making any aspect of such a report publicly accessible could serve as a warning to perpetrators and offer an opportunity to cover their tracks, or raise concerns about the chain of custody for evidence provided as part of the report.

Our approach to the verification of reports has shifted broadly from crowdsourcing this where possible to making verification the responsibility of the NGO running a campaign. To this end, The Whistle will provide a dashboard that facilitates their verification of reports, integrating a number of tools that are already used by practitioners who conduct this kind of verification in order to streamline and support existing workflows, ultimately reducing the burden of the verification bottleneck for many NGOs.

These modifications allow The Whistle's "front-end" to emphasise informing potential civilian reporters' about what they are consenting to when they submit a report – and steps they should take to protect themselves or their identity. The TalkFree platform as initially described would collect reports, but also open aspects of these reports up to community analysis. Having these two distinct activities (one related to receiving sensitive information from potentially vulnerable sources, the other an open public analysis of that information) occurring on the same platform would have been problematic because it would require the platform to present two very different faces to these two distinct user groups. Each of The Whistle's reporting campaigns will have its own Front-end with information specific to that campaign.

The only people who will have access to The Whistle's back-end are nominated representatives of the organisations that are running campaigns. When an organisation sets up a reporting campaign on The Whistle, only their representatives will be able to access submitted reports. Their options for interacting with these reports are to:

- 1) Pass aspects of the reports through external APIs (e.g. tineye) and add the output from those APIs as new data to the report. Methods of protecting or disguising material passed to external APIs are being evaluated.
- 2) Export the reports according to the NGOs own data protection best practices
- 3) Add a verification decision or other information and notes to the report

Reporting campaigns will have bespoke configurations, each asking for specific types of information from reporters, in line with the subject of the campaign and what the organisation running the campaign wants to use the reports for. The creation of each new reporting campaign will need to be considered from an ethical perspective, and be reviewed by the Ethical Advisory Board (see D2.1) before the campaign is launched. The configuration of each test reporting campaign will be bespoke to some extent. In working with NGO partners to create these bespoke configurations we will learn about the types of flexibility required for the product design to scale more easily in the long-term. Ultimately it should be possible to configure The Whistle for a specific reporting campaign through the platform itself.

The reporting context for a campaign will determine the level of security precautions required. For example, a "Living Wage" campaign conducted in the United Kingdom that asks civilians to report their wage levels and

working conditions would be considered relatively low risk - reporters would not necessarily be encouraged to use Tor, and there would be less restriction of the questions which could be asked of reporters. In contrast, a campaign about human rights violations in Syria would be considered to expose reporters to a higher level of risk, so reporters would be instructed to protect their identity, the campaign might have to make use of Tor or other technologies mandatory for reporters, and NGO representatives might be restricted to accessing reports on a secure server, limiting export functionality . Each prospective reporting campaign will be considered in depth from an ethics/security perspective internally within the project team, and then also by the Ethics Advisory Board.

In initial stages, we will work with the organisation that is running the campaign to determine what the public output of that campaign (if any) should be. Aspects of reports that are relevant to assessing companies' ESG performance will be passed to WikiRate through API calls after the reports have been verified by representatives of the non-profit(s) running the campaign. The information that is passed to WikiRate is likely to be aggregated, or will in any case be stripped of PII (personally identifying information). This would be the first point at which any aspect of the original report will be viewable by the public, and the full detail of the reports will be held under restricted access on protected servers.

The Whistle will be designed and developed with a focus on the reporting of human rights violations by civilian witnesses. –The initial approach by which TalkFree could be described as “reporting campaigns about businesses, incorporating human rights violations”, can now be better described in The Whistle as “reporting campaigns about human rights violations, incorporating businesses”. There are a number of reasons that benefit the project by adopting this updated description:

1. Human rights reporting and fact-finding is a more established and active area than reporting on business practices. There are more NGOs working on this broader problem, giving the project more scope to find suitable partners, and increasing the potential impact of an effective tool.
2. Human rights offers more challenging test-cases, a tool which works in this domain could likely also be applied to many campaigns about business practices where reporters are external to the business and risks are relatively low.
3. The greatest potential for civilian reporting on business practices lies with workers, and this sets a minimum level of risk which reporters would be exposed to. A reporter who was identified as submitting reports about their employer to The Whistle would risk losing their livelihood. Power exerted over employees by employers makes discovery more likely. While it may be possible to mitigate these risks, high-risk reporting scenarios will be avoided in the first reporting campaigns.

2 Design and Development of The Whistle in year 1

In the first year of the project, an overall design for The Whistle has been produced which specifies how it is intended to function agnostic of use case. However, development thus far has been limited to prototypes of individual components to test their viability. The overall design of The Whistle is ambitious in scale, and so decisions about which aspects to prioritise and details of design are heavily dependent on the nature of the first reporting campaigns the platform will serve. Section 2.1 explains why we have adopted an approach of developing in collaboration with reporting campaign partners, and subsequent sections present the design of the full platform and describe prototypes which have been produced.

2.1 Lessons from research informing design (WP2) and research on collective awareness platforms (WP7)

Research conducted as part of WP2 and WP7 has had a profound influence on our approach to developing The Whistle.

Deliverable 7.1 includes a broad overview of existing platforms that serve some of the same needs that The Whistle is intended to serve, and therefore which could be considered as competitors. Since the submission of D7.1 this research has continued with a deeper scrutiny of the four platforms most similar to The Whistle (to be reported in D7.3). To summarise, there are (or have been) a large number of projects which have attempted to gather better information from civilian witnesses and/or enable collaborative work on the verification of such information. Many of these projects have already ended without achieving their aims, and of those which remain there are no signs that they will achieve the specific goals of The Whistle. It is vital that the project learn from these existing efforts and avoid reproducing approaches which have already been tested without success, unless reasons for failure can be identified and mitigated.

Research to inform the design of The Whistle (WP2) has involved assessing a large number of NGOs who have the potential to be partners for reporting campaigns, identifying the most relevant organisations and interviewing representatives from those organisations. The outcomes of this interview study will be reported in full in Deliverable 2.2, but this research is already shaping our understanding of the user requirements for The Whistle, and so a summary is merited here. The two major findings from this study are that 1) report collection and verification practices vary significantly between organisations, and 2) these practices rarely involve the use of advanced tools - the reliance on established tools like phone lines, email, and spreadsheets is a common theme.

Some other findings from this research which have informed design of The Whistle:

- “Top down” approaches that assume levels of technical literacy on the part of respondents haven’t worked well
- Approaches that require respondents to learn how to use tools that don’t integrate with existing practices and work flows haven’t worked well
- The diffusion of different tools and the non-standard availability of meta-data has made the use of new tools difficult
- The lack of consistent support over time from tool makers has resulted in hesitance to try or to make commitments to new tools
- Technical challenges experienced by NGOs that are unrelated to verification tools - for example, difficulties managing databases and tracking data - can make existing workflows especially difficult environments to integrate new tools

The research suggests that there are opportunities to significantly improve the efficiency of these practices within organisations, but that each organisation is reluctant to re-structure their approach to better align with existing tools. The Whistle aims to facilitate the work of partner NGOs on collecting, verifying and making use of civilian witness reports. Where an NGO already has an approach that works in their context, it would

be counterproductive to ask them to restructure this approach to fit with The Whistle (as such restructuring would have a cost which the NGO would have to bear). Instead, The Whistle should be designed to fit into these existing workflows where possible.

Taken in culmination, the WP2/WP7 research argues strongly against designing and developing a general-purpose tool that would fit the ChainReact ecosystem but would ultimately reflect a prescriptive approach. Without buy-in from relevant organisations, such a tool would not have any users.

Since the earliest stages of the project, the intention has been that each reporting campaign will have flexible elements which tailor it to the specific reporting context (i.e. reporters' access to ICTs, security concerns). On the basis of WP2/WP7 work, we have decided that the best approach is to take this a step further and develop The Whistle itself in partnership with the NGOs that will run reporting campaigns. This approach has a number of advantages.

- 1) This approach offers an attractive proposition to potential reporting campaign partners. If we can agree on the details of a reporting campaign they wish to run, and they are willing to let us study their existing information collection and verification practices - we will build a platform that is specifically geared towards the successful execution of their campaign, which takes into account their practices and resources, and which allows for thoughtful iteration of future versions in order to make concrete improvements.
- 2) This approach makes good use of the skills of the research team, whose members have a deep understanding of the issues around human rights report collection and verification, and also experience of designing technological solutions for established problems. The proposition to reporting campaign partners, of developing the platform to serve their specific campaign, offers an incentive for them to grant the level of access required to conduct this research well. This in-depth research is vital for informing the design of The Whistle so that it meets the needs of NGO partners.
- 3) The best way to promote The Whistle as a tool for facilitating report collection and verification is to present a strong demonstration of the platform in action and producing a successful outcome. A successful use case is predicted to make it easier to attract subsequent partners - developing the platform specifically to serve these early use cases offers the best chance of a successful outcome for the product and the development of an NGO partner who will be willing to strongly endorse both product and process to others in the field .
- 4) This approach will make make optimal use of development resources available within the project, by prioritising the features required for the test reporting campaigns and avoiding the prospect of developing features which may in the end be superfluous to the test reporting campaigns. So far very few resources have been expended on WP3, and much of the technical advice received and development of prototypes has been obtained on a pro bono basis. Resources for development of The Whistle proper are being reserved for deployment once the first reporting campaigns are finalised, at which point we are well placed to make rapid and efficient progress.

The following sections will present the overall design of The Whistle. The approach of working directly with NGO partners to develop the platform is a way of navigating this design more efficiently, prioritising features for development in line with the needs of these campaigns, and establishing pragmatic and effective solutions

for concrete use cases. As we develop The Whistle for each campaign, and study its effectiveness in facilitating the execution of these campaigns, we will also be progressing towards, and refining, the overall design of the platform with an eye towards scalability and flexibility for a larger variety of use cases.

2.2 Aims of The Whistle

Today, NGOs that deal in the reporting and analysis of human rights violations (HRVs) gather most of these reports manually - by talking to witnesses on the ground, or by looking at reports over social media. This current process, while effective, is time consuming and limited by the availability of person-to-person interaction¹; it is very time consuming for NGOs to gather and verify these reports.

The Whistle seeks to address problems of limited reporting data, fewer sources of data and the difficulties analyzing reports with the Whistle App, a web and mobile app that allows end-users who have witnessed human rights violations to report the issue and send their information to the appropriate NGOs, who track and verify such reports.

Digital verification is a rapidly evolving field that requires expertise in new and often diffuse tools and techniques. By bringing many of these tools and techniques into one workspace, the Whistle enables NGO fact-finders to leverage these tools simply and efficiently. Specifically, the Whistle App will aggregate reports by label and will automate much of the cross-checking with other methods and sources that underpin the practice of verification, in order to help facilitate and prioritize the comprehensive validation work that must be done by NGO fact-finders. Additionally, by providing a simple and accessible app-based process by which witness reports can reach NGOs, the Whistle Project will increase the pluralism of reports, reporters, and responders.

Using the Whistle dashboard, NGOs will be able to view individual and aggregated reports along with the results of the cross-check indicators. This dashboard allows NGOs to view reports by label or by searching for keywords in reports. Top labels will include date, geographical location, type of abuse, descriptive characteristics of the witness, type of evidence, and other labels and tags created by the NGO. The dashboard will also allow NGO users to add their own verification data, marking reports as “verified” in their personal dashboard. Verified reports, or aggregated/abstracted information about these, can be exported to third parties. The priority for external integration will be with the WikiRate platform, where information that is relevant to companies and their supply chains will be exported.

The aims of The Whistle can be summarised as follows:

- 1) Increase the total reports of human rights violations available to NGOs
- 2) Increase the pluralism of witnesses of human rights violations available to NGOs
- 3) Facilitate NGO analysis of these reports by showing the results of automated cross-check indicators to help NGO fact-finders speed and prioritize report verification

¹ UNHRC, ‘Interim Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Philip Alston’ (23 August 2010) UN Doc A/65/321.

-
- 4) Facilitate NGO analysis of these reports by allowing NGO fact-finders to view reports by label or tag

2.3 High-level design

The Whistle's design has four components.

- 1) Civilian witness reporting front-end (app/interface/method)
- 2) NGO dashboard for accessing reports
- 3) Integration with verification-aiding tools through the dashboard
- 4) Methods for exporting reportable data (e.g. API)

Figure 1 shows a schematic overview of The Whistle's components

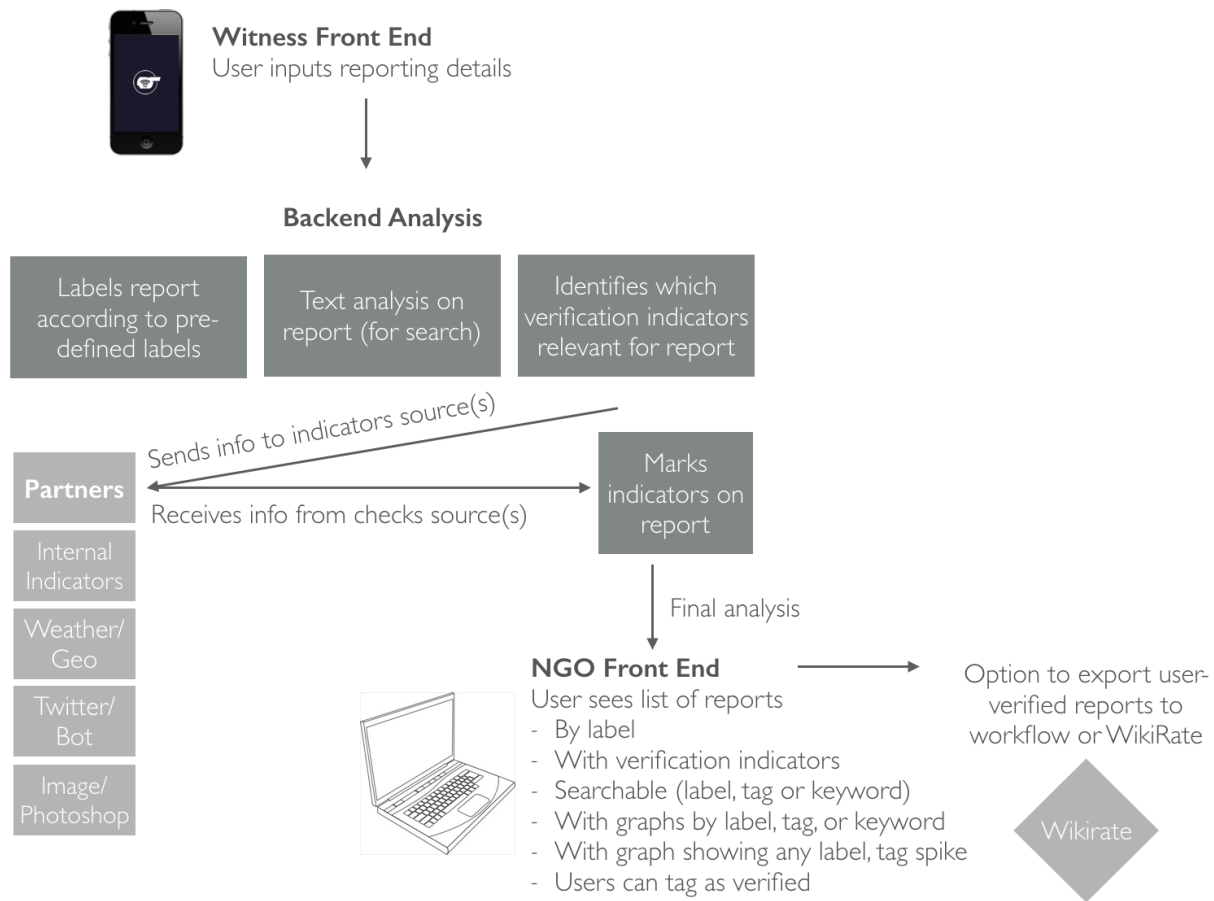


Figure 1. Schematic overview of The Whistle incorporating backend processing of reports, integration with external verification-aiding tools, and display of reports on the NGO front end.

2.4 Civilian Witness Reporting interface

The method through which civilians submit reports to The Whistle is one of the most important and context-dependant aspects of design. It is vital that the target reporters for a given campaign have the necessary means of interacting with The Whistle to submit reports. This is further complicated by issues related to the need for pluralism in reporting - where one of the aims of the project is to give voice to those who are presently marginalised, whose perspectives and experiences do not reach Human Rights Organizations (HROs). Thus it is important not only to consider whether the population of potential reporters has access to the means of making a report, but how this access is distributed among the population. For example, if only community leaders or the relatively well off tend to have access to a smartphone, then a reporting interface which relies on a smartphone will likely only receive reports from (or filtered by) these groups, and fail to achieve the aim of pluralism.

Possible methods of receiving civilian witness reports:

- 1) Exchange of SMS and or MMS messages
- 2) Exchange of Smartphone messages
- 3) Web forms (accessible via mobile)
- 4) Installable Smartphone app
- 5) Mesh networks

2.4.1 SMS/MMS Messages

The prevalence of mobile phones which have the capacity to send and receive SMS messages makes this an attractive option - although it cannot be assumed that this technology will be widely available in all target reporting populations.

One major disadvantage of SMS reporting is that these cannot be encrypted or secured, if malevolent actors can gain access to the mobile service providers' records they could determine the identity of reporters and content of their communications. This risk could be mitigated to a degree through the use of pre-pay "burner" phones. A system which relies on SMS reporting is also limited with respect to the kind of evidence that can be provided to support reports (i.e. cannot provide image/video).

There is also an issue with the cost of reporting via SMS where reporters pay per each message sent, in some populations the cost of sending a series of messages to make a report would be prohibitively high. This could potentially be mitigated by setting up free to text numbers or "short codes" that would allow the NGO to cover costs of SMS reporting for their campaign.

Despite the disadvantages noted, a reporting system which can collect reports from civilian witnesses via SMS is highly desirable because this offers the greatest possible reach in terms of target reporting populations. This fits well with the aim of increasing the pluralism of reports. There may be reporting contexts in which the disadvantages of SMS reporting are less relevant (for example in some contexts surveillance by service providers is not a concern), and/or where basic feature phones are the only means of telecommunication for prospective reporters.

Finally, from a technical perspective the approach of creating reports based on an exchange of text messages entails a set of challenges which are agnostic with regard to input modality - interpretation and storage of input received, choosing the next step in the dialogue. A similar version of this approach could likely be deployed with SMS messages and smartphone instant messages (through a client like WhatsApp).

2.4.2 Smartphone messaging clients

The receipt of reports from smartphones has a number of advantages, the major disadvantage being that they are not commonly available in some reporting populations. One possibility is to receive reports through an existing popular messaging app such as Whatsapp. In principle these messages are encrypted, although a recently uncovered vulnerability with the Signal protocol calls the level of security this provides into question². The use of a popular smartphone messaging app would also provide a level of camouflage for

² <https://www.theguardian.com/technology/2017/jan/13/whatsapp-encryption-backdoor-snooping-signal>

reporters - simply having the app installed would not identify an individual as a likely reporter. Smartphone messaging apps would also allow for the submission of image/video evidence to support a report.

SMS and Smartphone messaging share a vulnerability in that both naturally leave traces on the device which is used. If the device were to be compromised, the presence of sent/received messages could identify the reporter. Instructing reporters to delete these traces would be an important step towards mitigating this risk, but still could not be relied upon completely. Smartphones are much more flexible, and messages can be set to self-destruct in certain clients (notably snapchat).

2.4.3 Web forms

Simple web forms that could be easily accessed on a smartphone are another possibility for receiving reports. These would have the advantage of easy implementation, but there are barriers to securing this communication. Although commonplace HTTPS encryption can secure the contents of the communication, service providers would have a record that communication took place between the reporter and the form (and malevolent actors could also detect this communication). Such communication would also naturally leave a history trace on the reporter's device, but instructions could be given for preventing or deleting such a trace.

Proxy apps like Tor and Orbot (which provides a mobile interface to Tor) allow for more secure and anonymised communication - by encrypting communications and bouncing them around in a secure network, making it very difficult to identify the IP address from which the communication originated. These apps have the disadvantage that potential reporters would have to install them and use them correctly to obtain the protection they offer - raising the barrier to reporting. The presence of these apps on a reporter's device could raise suspicion if the device was compromised. Finally, these apps do not provide a guarantee of anonymity, particularly if the way in which they have been configured by a reporter is unknown - offering a sense of security to reporters where this cannot be guaranteed could actually increase the risk to reporters (if they make reports containing sensitive information because they believe they are not at risk).

Using a web form to collect reports would mean that only people who have access to the internet could submit reports - either on a computer or smartphone. In some contexts reporters may only have access to the internet through internet cafes or other shared spaces which are not locally private - others in the venue could potentially see the report being made.

In some contexts, being identified as a reporter locally by known parties (e.g. spotted submitting a report in an internet cafe) is of much greater concern than being identified remotely through technical means (e.g. tracing an IP address to a service plan and customer). The differing nature of security concerns in different reporting contexts argue in favour of a modular approach where different methods of creating reports can be connected to The Whistle, allowing appropriate input modules to be selected for a particular campaign.

2.4.4 Installable Smartphone App

The option of an installable smartphone app is one that we will hesitate to pursue. Such apps have already been developed (e.g. CameraV and Eyewitness to atrocities), and while they have the advantage of providing

robust meta-data that aids verification, they suffer from a number of disadvantages. These include, but are not limited to:

- Only individuals who have already installed the apps (decided they want to be “a witness”) are in a position to use such apps to record evidence of and report on incidents
- These apps require a certain level of technical literacy, and at the very least, assume good internet connectivity
- Apps are hard to disseminate as they may be incompatible with certain devices, and require awareness of the app in the first place
- Currently available apps do not allow for two-way communication between the human rights organization and the witness - thus, trust becomes a potential problem, and opportunities are missed vis-a-vis educating witnesses on security
- The presence of such an app on an individual’s smartphone is also an indicator that they are a likely reporter, making the apps unsuitable for many prospective reporting populations
- On existing apps, It is unclear where gathered information goes, after the reporting stage. With the exception of *Martus*, existing apps either store evidential information on offline servers for an indefinite amount of time, or lock-in metadata and expects the civilian to know what to do with the data.

2.4.5 Mesh Networks

Mesh networks are being explored as a possible way of enhancing the security and accessibility of reporting campaigns. Wireless mesh networks allow for decentralised communication between devices through bluetooth and WiFi protocols, without requiring internet access. Messages and data can hop between nodes in the network until they reach their intended recipient(s) or a gateway to the internet.

Firechat is a messaging app built on mesh networking principles. It was adopted by large numbers of pro-democracy protesters in Hong Kong in 2014³ and used to run large public chat-rooms which could be accessed directly by any individual with the app who was in range of the network. Users of the firechat app form a mesh network, with each node (usually smartphones) acting as both a receiver of information and a relay of information. Wireless technology limits the range between nodes to around 200 feet, but the size of the mesh network scales according to the number and distribution of nodes - a signal can hop between as many nodes as required to reach its destination.

The attraction of mesh networks is that they do not rely on infrastructure beyond the individual wireless devices. This makes them robust to state intervention which would target communications infrastructure to disrupt communication (attractive to the protestors in Hong Kong). The same characteristic makes mesh networks useful in scenarios where infrastructure has been damaged, such as in the aftermath of natural disasters. The makers of Firechat have recently released Firechat alerts⁴, a deployment of the technology

³ <https://www.theguardian.com/world/2014/sep/29/firechat-messaging-app-powering-hong-kong-protests>

⁴ <https://www.opengarden.com/alerts.html>

geared towards governments and NGOs that need to reach a population when centralised communications infrastructure is damaged or unavailable.

There are two obstacles to using mesh networks as a conduit for receiving civilian witness reports. Firstly, we would need to better understand the implications for security and anonymity of reporters. At the time of the Hong Kong protests in 2014, Firechat only offered communication in public chat rooms via the local mesh network. As these chat rooms are open, they are vulnerable to surveillance and infiltration⁵. Open Garden have since added encrypted private messages to Firechat which can propagate through the mesh network⁶, passing from node to node but with only the intended recipient being able to decrypt them, but it is not clear how well this protects the identity of users and the content of their messages. From a security perspective, the advantage of mesh networks is that they bypass centralised infrastructure (which may be under surveillance) - but the mesh network itself may be susceptible to surveillance by agents in the local area.

The second obstacle to the use of mesh networks by The Whistle lies in the need for an installed base of devices in close proximity. For a mobile phone to be part of a mesh network, it must be within range of other nodes on that network (around 200 feet for WiFi, much less for bluetooth). Mesh networks are well suited to crowds, where if even a fraction of members are participating as nodes, the network will likely be dense enough to function well. Reporting scenarios where mesh networking technology could be useful would involve groups in close proximity (e.g. a campaign related to the treatment of protestors by authorities), or potentially campaigns that are tied to specific locations (where the partner NGO may be able to seed the network with enough nodes to make it useful).

2.5 Civilian witness reporting interface – prototypes

2.5.1 Messaging approach

Two-way approaches to digital human rights reporting between civilians and organizations haven't been fully explored (Alston, 2013⁷). Thus far, any attempt to communicate human rights violations in a two-way manner has been between fact-finders or trained citizen-journalists, and NGOs and other organizations. Drawing on the methodology of UNICEF, UN Global Pulse, and Africa's Voices Foundation, new opportunities are presented by tools such as Rapid Pro, which allows for the aggregation of two-way survey-based data through text-messaging.

⁵<https://advox.globalvoices.org/2014/10/02/hong-kong-protesters-shore-up-mobile-communications-tools-in-face-of-technical-threats/>

⁶ <http://www.bbc.co.uk/news/technology-33718318>

⁷ Alston. "Third Generation Human Rights Fact-Finding." *Am. Soc'y Int. L. Proc.* (107: 2013.)

We are developing a messaging bot prototype running on ruby on rails as a proof of concept. This bot reads questions from a file and stores answers as a JSON object. It performs some validation checks on responses (e.g. using the google maps API to check if an inputted address can be resolved to a particular location), and has some rudimentary logic for steering the “conversation” through appropriate questions given the answers provided. This messaging bot is in the early stages of development, it currently runs in a local terminal and the validation checks and steering logic have ample room for improvement. If interacting with this bot can produce useful reports in an efficient manner for a particular context, that would constitute a proof of concept that the approach has merit, and the bot could then be integrated with methods for receiving and responding to messages from SMS and other sources (e.g. WhatsApp), and storing these securely.

Through this more sophisticated response mechanism, witnesses would be able to report as much as they feel comfortable reporting, all the while receiving security recommendations from our chatbot engine. This also eliminates the need for a smartphone (this approach is nevertheless flexible and adaptable to existing messaging apps such as WhatsApp).

Our chatbot engine would aggregate incoming information and interface with The Whistle API to catalogue incoming information in a user-friendly format for the NGO to view on a dashboard. Incoming mentions of locations can also be autonomously converted to coordinates and displayed on a map. Reports are furthermore cross-referenced with existing databases of incidents in order to render a more holistic overview of the potentially emerging patterns.

Figures 2, 3 and 4 show how the messaging approach could be integrated with The Whistle, and what the user experience would be like for reporters.

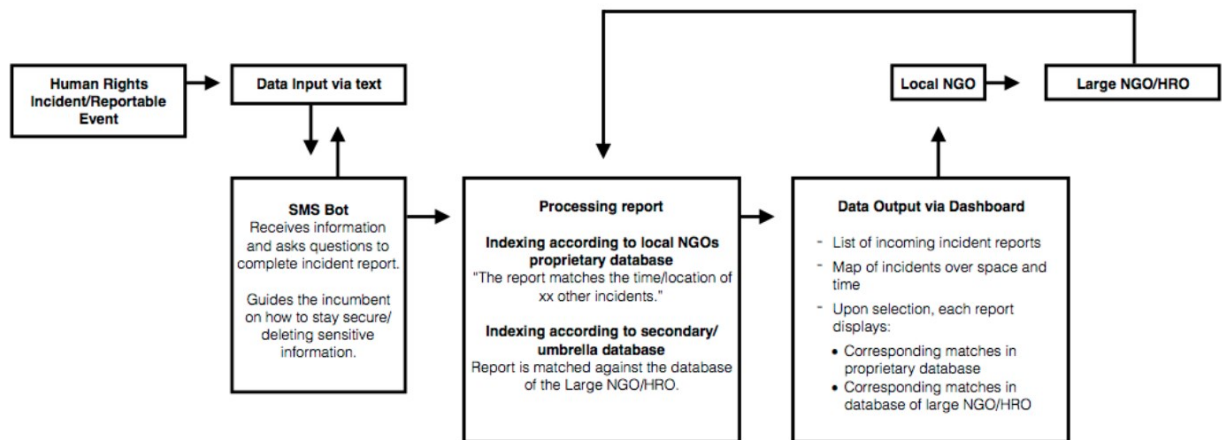


Figure 2 - Schematic view of how a messaging bot would be integrated into The Whistle

SMS Bot Setup

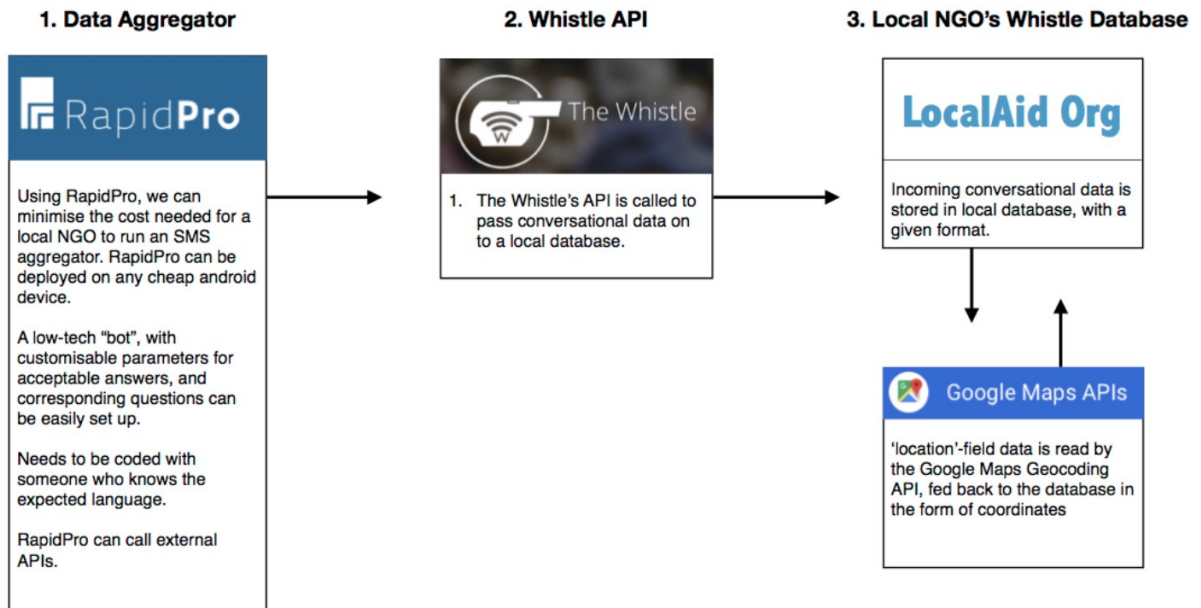


Figure 3 - Using RapidPro to develop an SMS bot prototype

Data Input via SMS

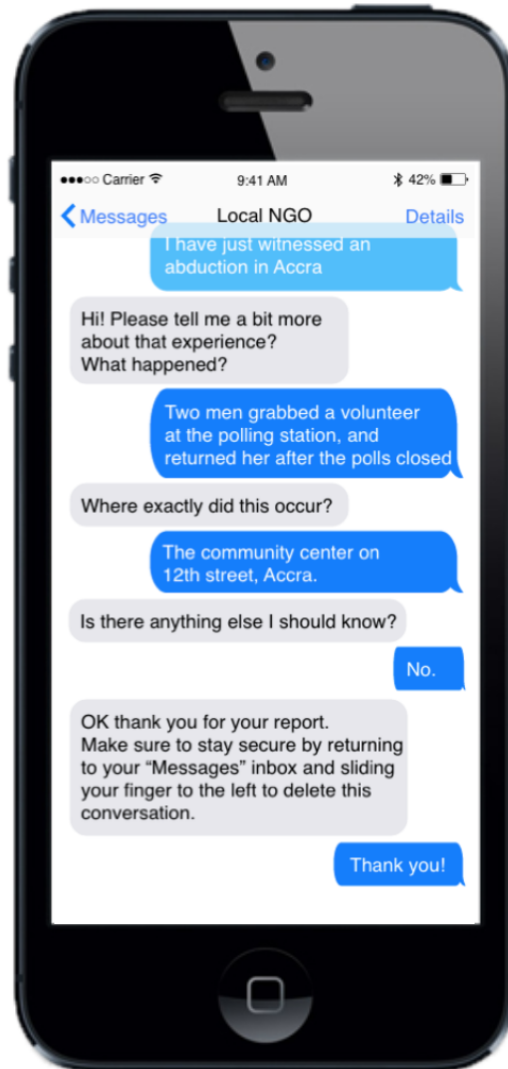


Figure 4 - Example showing how an SMS reporting mechanism would appear to reporters.

Figures 5 and 6 show an early prototype of the messaging bot approach with an example reporting interaction. At the point where the civilian witness provides a location for the incident, a map window is popped up which attempts to locate this address as a set of coordinates (Figure 6), and the witness is asked to confirm whether this location is accurate. This is the first of many ways in which the interactive nature of message bot reporting could be leveraged. In addition to logic trees that attempt to validate information and ask appropriate follow-up questions, there is great potential to use this approach to provide civilian witnesses with information that is relevant to their situation. For example, depending on the nature of the reported incident, The Whistle could offer to provide the witness with information about resources they could access in the local area (e.g. medical care, legal representation, relevant NGOs).

```
>>> Welcome to the Whistle! Our researchers are trained in handling sensitive information securely, and our reporting platform, The Whistle, works to maintain high security standards for the communication, handling, and storage of your reports. Even so, communicating online is never risk-free. Out of an abundance of caution, we urge you to approach submitting a report via The Whistle as if you were saying it out loud in public. Even if you submit a report anonymously, it may still be possible for it to be traced back to you. If reporting it would put you at risk, please do not submit a report. Have you read and understood this, and do you wish to proceed?
/
>>> Sorry. The required answer for this question is 'yes'.
yes
>>> Thank you for that. Please describe the incident with chronological detail:
Police beat me up.
>>> Thanks. How do you know this: eyewitness, hearsay?
1: eyewitness
2: hearsay
1
>>> Why were you there?
I went shopping.
>>> Where were you standing?
On the sidewalk
>>> I appreciate that. Knowing where the incident happened allows us to cross-reference your report with other reports and is key to making a case for courts or advocacy. What is your address?
Lagos, Nigeria
>>> I have located you at Lagos, Nigeria. I opened a browser window with your location, or alternatively copy-paste this line:
http://maps.google.com?q=6.5243793,3.3792057
>>> Is this location exact?
1: yes
2: no
2
>>> I'm sorry, I couldn't locate you. Please try again. I appreciate that. Knowing where the incident happened allows us to cross-reference your report with other reports and is key to making a case for courts or advocacy. What is your address?
Alaka St, Lagos, Nigeria
>>> I have located you at Alaka St, Lagos, Nigeria. I opened a browser window with your location, or alternatively copy-paste this line:
http://maps.google.com?q=6.583595,3.3036037
>>> Is this location exact?
1: yes
2: no
1
>>> This is good. Now, knowing when the incident happened allows us to cross-reference your report with other reports and to establish a time-line that is key to making a case for courts or advocacy. What date did the incident occur?
Today
>>> What time was it where the incident took place?
11am
>>> What happened just before the incident took place?
I saw a government convoy.
>>> What happened just after the incident took place?
I went to the hospital.
>>> Great. We are happy for you to submit your report anonymously. Providing contact information, however, if safe, allows us to follow up with more questions if we have them. Providing identity details allows us to understand more about you, how you have the information in your report, and why you are sharing it with us. Only supply identifying and contact details for you, the subjects of your report, and/or corroborating witnesses if it is safe to do so! Would you like to provide personal information?
1: yes
2: no
1
>>> What is your name?
Ifemulu Odenigbo
>>> What is your email?
ifemulu.odenigbo@email.com
>>> What is your phone number?
01 123 1234
>>> What is your social media account?
@odenigbo
Thank you, I was able to save your answers. Bye bye now!
```

```
"Datetime": "2017-02-17 15:19:41 +0000",
"Welcome to the Whistle! Our researchers are trained in handling sensitive information securely, and our reporting platform, The Whistle, works to maintain high security standards for the communication, handling, and storage of your reports. Even so, communicating online is never risk-free. Out of an abundance of caution, we urge you to approach submitting a report via The Whistle as if you were saying it out loud in public. Even if you submit a report anonymously, it may still be possible for it to be traced back to you. If reporting it would put you at risk, please do not submit a report. Have you read and understood this, and do you wish to proceed?": "yes",
"Thank you for that. Please describe the incident with chronological detail:": "Police beat me up.",
"Thanks. How do you know this: eyewitness, hearsay?": "eyewitness",
"Why were you there?": "I went shopping.",
"Where were you standing?": "On the sidewalk",
"I appreciate that. Knowing where the incident happened allows us to cross-reference your report with other reports and is key to making a case for courts or advocacy. What is your address?": "6.583595,3.3036037",
"This is good. Now, knowing when the incident happened allows us to cross-reference your report with other reports and to establish a time-line that is key to making a case for courts or advocacy. What date did the incident occur?": "Today",
"What time was it where the incident took place?": "11am",
"What happened just before the incident took place?": "I saw a government convoy.",
"What happened just after the incident took place?": "I went to the hospital.",
"Great. We are happy for you to submit your report anonymously. Providing contact information, however, if safe, allows us to follow up with more questions if we have them. Providing identity details allows us to understand more about you, how you have the information in your report, and why you are sharing it with us. Only supply identifying and contact details for you, the subjects of your report, and/or corroborating witnesses if it is safe to do so! Would you like to provide personal information?": "yes",
"What is your name?": "Ifemulu Odenigbo",
"What is your email?": "ifemulu.odenigbo@email.com",
"What is your phone number?": "01 123 1234",
"What is your social media account?": "@odenigbo"
}
```

Figure 5 – Example messaging bot reporting interaction

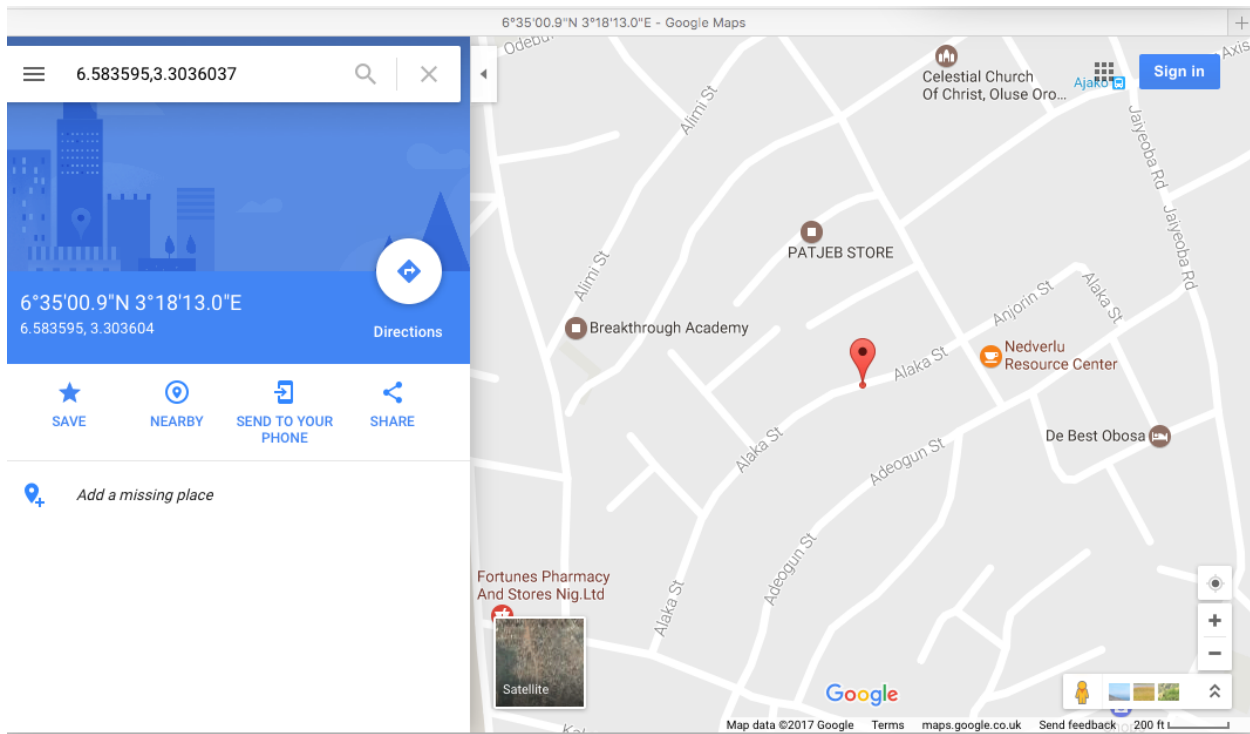


Figure 6 – Location verification pop-out that occurs during reporting interaction

2.5.2 Web form approach

It would be quite straightforward to use web forms as the civilian witness reporting front-end of The Whistle, making efficient use of development resources. Being the most straightforward approach to implement, a web form can be thought of as the “default” approach, and was the first to be explored. Appendix 4.1 contains mock-ups of a web form reporting interface. These mock-ups illustrate the kind of information which would be sought from reporters, and the kind of guidance they would be given on providing more useful (verifiable) reports and protecting themselves. As part of the research for WP2, we have learned that some NGOs already use web forms like this to collect information, but that these tend to be underused by reporters.

The major drawback of this approach is that this mode of input would limit the reporting population to those who have more advanced technology than a basic mobile phone (i.e. smartphone, tablet, pc) - which depending on the reporting context may make this approach unattractive. Nonetheless, the ease of implementation means that web forms are likely to be offered as an alternative or backup method of creating reports for some campaigns. The prescriptive nature of a web form would make creating this a useful step in designing a campaign - as it would require a clear definition of the properties and fields that an incoming report should have.

In testing, a web form can also be used as a kind of baseline that other methods can be compared to. For example, an SMS bot might be preferred for a campaign because it is more accessible for the target population - ideally the process of creating a report through this method will be as straightforward as using a form, and result in reports that are of similar quality.

2.6 Facilitating verification

One of the ways in which The Whistle can facilitate the work of NGOs is by integrating access to tools and services that can aid verification of reports. API calls can be used to automate the process of using some of these tools/services, this would allow an NGO representative to easily run checks on a report without having to learn the specifics of how each service should be called, and would allow for the outcomes of these checks to be automatically recorded on The Whistle's dashboard.

2.6.1 Verification-aiding services

Table 1 contains a list of verification-aiding services which could be integrated with The Whistle via API. These have been broken down into a number of types, based on the attribute of a report or supporting evidence that they are applied to.

Image verification services can analyse an image to ascertain whether it has already been published on the web (e.g. TinEye⁸) or whether there are signs that it has been manipulated (e.g. Izitru⁹). Integrations with tools like Google Maps and Yomapic can facilitate the verification of a location where an incident is alleged to have taken place. Where photos are provided in support of a report, one can check whether features in these photos are consistent with aerial views or photos from photo-sharing platforms depicting the location where an incident is described as occurring. Taking this a step further, one can also consider the weather at the time of the incident and the direction of shadows. For information coming from twitter, tools like TweetCred can automatically profile the tweet (and tweeter) to estimate its credibility based on a number of relationships between tweet characteristics and credibility. In contexts where the reporter's identity is known, services like Spokeo and Facebook Graph offer tools which can be used to facilitate verification of their identity.

The choice of which tools/services The Whistle should integrate is one which is again highly context-dependant. This depends firstly on the type of supplementary evidence that is provided along with reports. For example, a reporting campaign focusing on how protesters are treated by authorities, in a location where smartphones are common, might receive many reports accompanied by photographs taken outside - in which case image and location verification tools would be a priority. Integrating and maintaining the API links to these tools will require engineering resources, and we have opted to wait until we know what the first reporting campaign(s) will involve before choosing a set of tools.

There is an additional security consideration around links to external tools. Using these tools involves transmitting files or information to the external service, care must be taken to do this in a secure manner which does not expose the material to unwanted attention.

⁸ <https://www.tineye.com/>

⁹ <https://www.izitru.com/>

Name	Function
Verified Pixel	Image verification
Izitrü	Image verification
PHEME	
Google Reverse Image Search	Image verification
Google Maps	Location verification
CrowData	Document verification
TweetCred	Twitter verification
MIT/CMU	Twitter verification
Picasa	Image verification, Location verification
TinEye	Image verification
Wolfram Alpha	Location verification
FotoForensics	Image verification
FindEXIF	Image verification
Spokeo	Source verification
DomainTools	Source verification
Google Earth	Location verification

Yomapic	Location verification
Facebook Graph Search	Source verification
WebMii	Source verification
Flickr	Location verification
FreeOCR	Location verification
Panoramio	Location verification

Table 1 - List of possible verification-aiding tools that could be called by API

2.6.2 Youtube Multitool prototype

A prototype of a tool which can be used to analyse videos and facilitate the verification of their authenticity has been developed. This “Youtube Multitool” prototype can be accessed at <http://whistle.gbo.pw>, it is used to automatically extract metadata for youtube videos about the channel, video, source, and location of a video the user is seeking to verify, as well as frames that can be cross-referenced against image databases to see if the video has appeared online previously (the most prevalent type of manipulation of human rights related-video is repurposing it to claim it represents a new violation).

The youtube multitool prototype has been developed as a proof of concept. With further development, it could be integrated as one of the verification-aiding tools offered by The Whistle. As with other possible integrations, it will only be included when it serves a particular reporting campaign - in this case a campaign that is likely to see videos submitted as supporting evidence.

2.7 NGO Dashboard

Digital verification is a rapidly evolving field that requires expertise in new and often diffuse tools and techniques. By bringing many of these tools and techniques into one workspace, the Whistle will enable NGO fact-finders to leverage these tools simply and efficiently. Specifically, the Whistle App will aggregate reports by label and will automate much of the cross-check information with other methods and sources that underpin the practice of verification, in order to help facilitate and prioritize the comprehensive verification work that must be done by NGO fact-finders. Additionally, by providing a simple and accessible app-based process by which witness reports can reach NGOs, the Whistle Project will increase the pluralism of reports, reporters, and responders.

Using the Whistle dashboard, NGOs will be able to view individual and aggregated reports along with the results of the cross-check indicators. This dashboard allows NGOs to view reports by label or by searching for keywords in reports. Top labels will include date, geographical location, type of abuse, descriptive

characteristics of the witness, type of evidence, and other labels and tags created by the NGO. The dashboard will also allow NGO users to add their own verification data, marking reports as “verified” in their personal dashboard. Aggregations or abstractions of verified reports can be exported to third parties (with the priority being export to WikiRate when a report contains information about a company).

To do this, the Whistle analysis engine will 1) aggregate reports by label and tag (labels are automatically applied marks when certain conditions are met, tags are manually applied for custom workflow) and 2) support verification decisions through automating cross-referencing with other methods and sources (“cross-check indicators”), some of which will be provided by third party partners, in order to facilitate the manual NGO validation process, while the Whistle NGO dashboard helps fact-finders process the incoming reports, easily view trends, search for keywords and labels, and view cross-check indicators. This dashboard will show individual reports along with the results of the automated processing steps (verification indicators) and in addition to aggregated reports by label. Labelling will be defined by certain markers, possibly geographical location or particular keywords used. A search function allows fact-finders to search by existing labels, values or by keywords present in the report.

Once NGO users have verified a report using additional sources, they can mark the report as verified. “Verified” is therefore a final filter that can be used to look at trends in aggregate (for example, a user could look at all reports in Georgia, or she could look at the reports she has verified, compared to the reports that have not yet been verified). Verified reports can be exported simply (stripped of sensitive data if necessary) to a second site, an archive which can be used by parties such as WikiRate as an authoritative and signed source. In addition, a general export feature allows the user to export the data in the format that is most appropriate for his or her workflow (and that presumably this exported data could also be sent to others by the NGO user, according to what’s allowed under their organization’s security rules).

In the same way that the civilian witness reporting front-end will be developed with the context of the first reporting campaign in mind, the NGO dashboard will be developed to suit the workflow and needs of the NGO partner. The purpose of the NGO dashboard is to provide information about incoming reports in a way which suits the intended use of this information by the NGO. It is likely that early versions can be streamlined to provide this information in the specific format that will be most useful to the NGO.

We have however produced design mock-ups which illustrate a longer-term vision of how the dashboard is likely to work.

Processing Report

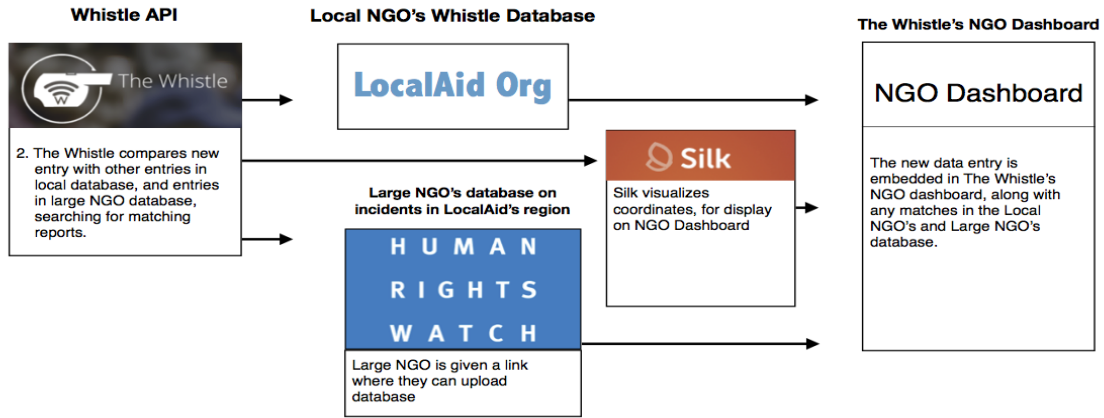


Figure 7 - Overview of how reports will be processed using The Whistle, in a scenario where a smaller local NGO runs a campaign in collaboration with a larger umbrella NGO which already has relevant information that can be cross-referenced against incoming reports.

Data Output via Dashboard 1/3

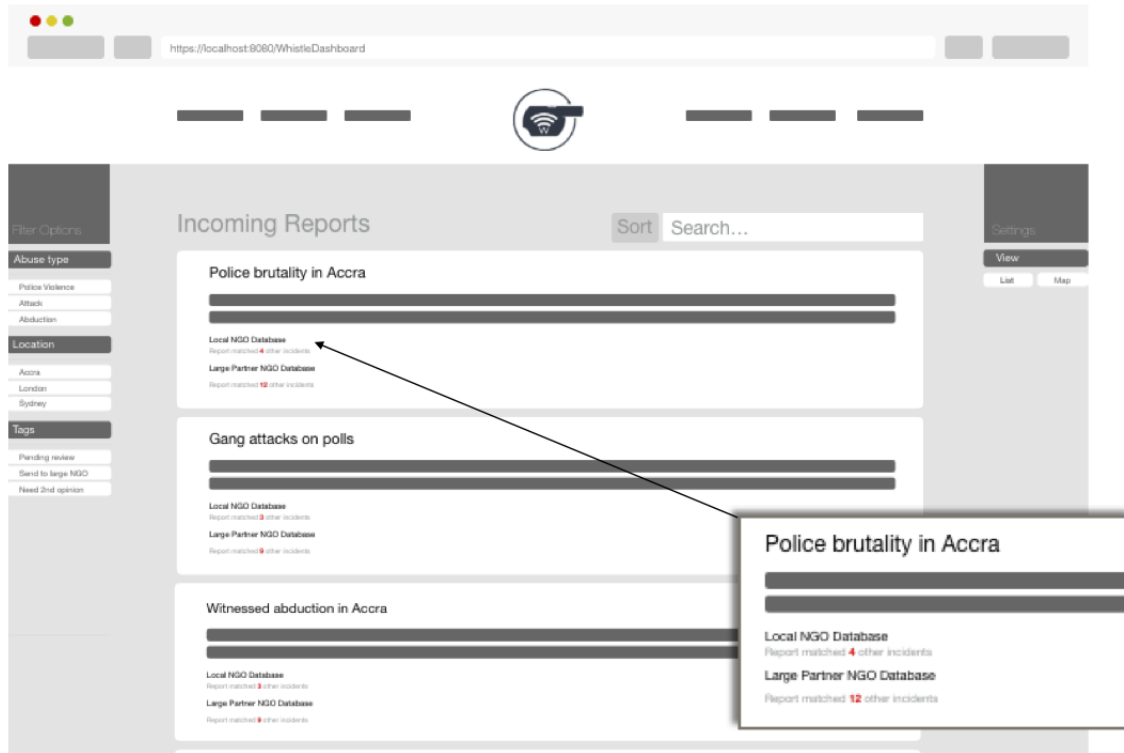


Figure 8 - Mock-up showing report browsing interface

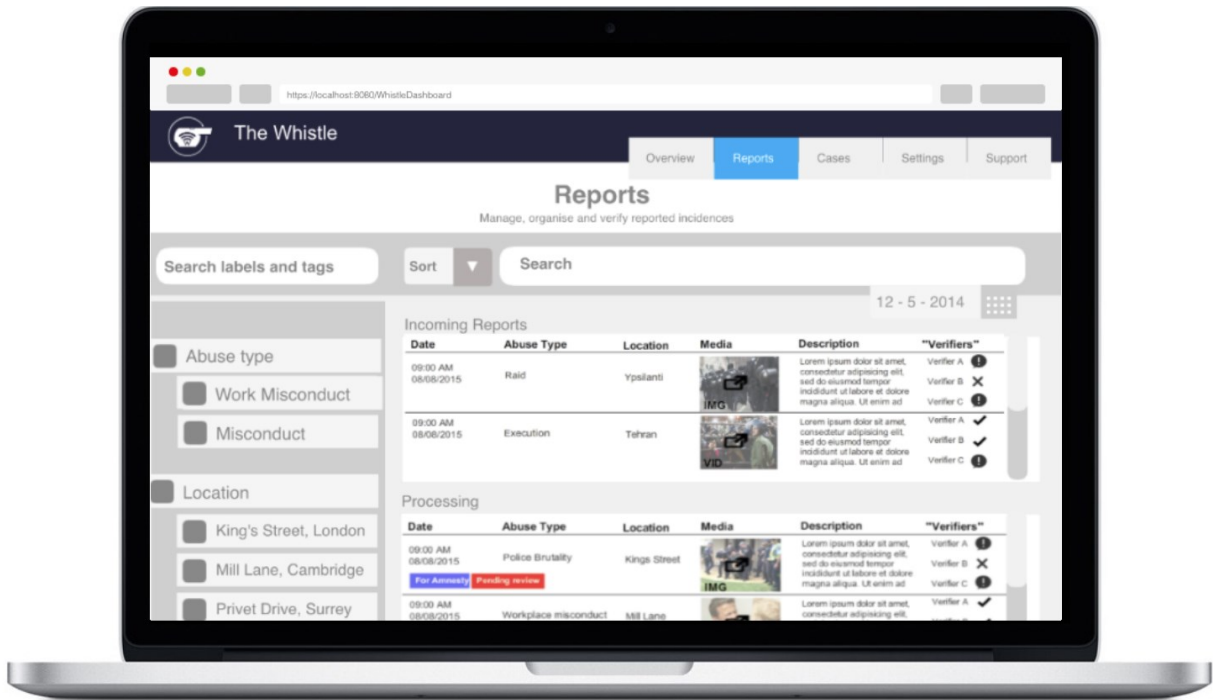


Figure 9 - Mock-up showing alternative detail view for incoming reports.

Data Output via Dashboard 2/3

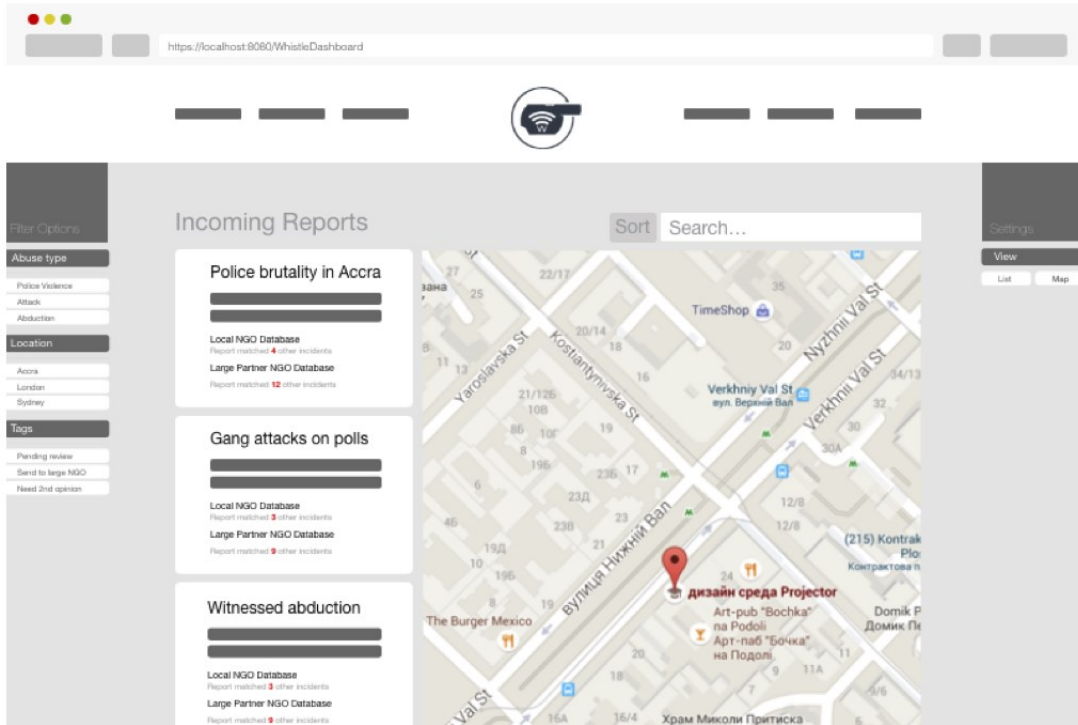


Figure 10 - Mock-up showing map integration to depict locations of incidents

Data Output via Dashboard 3/3 (individual view)

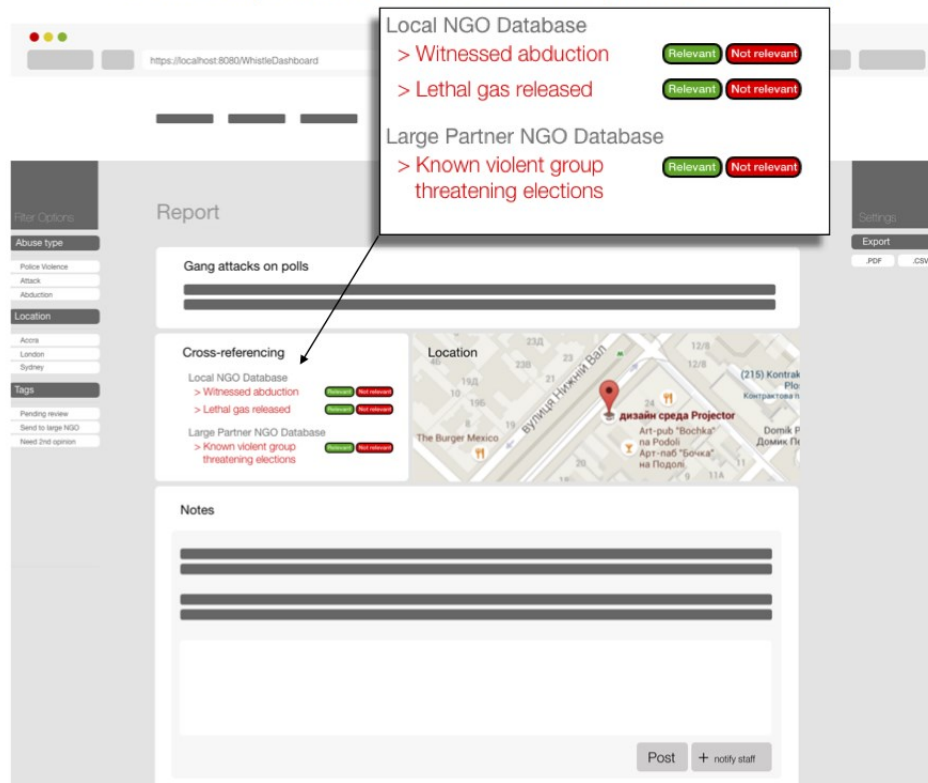


Figure 11 - Mock-up showing some NGO report processing options

2.8 Data handling and external publication

2.8.1 Report storage

Reports received by The Whistle reporting campaigns will be stored securely and access to these raw reports will be highly restricted. The details of how reports will be secured will be determined in collaboration with partner NGOs. Research for WP2 suggests that many human rights organisations have their own advanced security procedures, and that when this is the case the best place to store reports would be on a server on the NGO's own network behind their firewall.

2.8.2 External publication

While access to reports themselves will be heavily restricted, The Whistle will offer means of automatically exporting analyses or aggregations based on verified reports to external sites. Depending on the purpose of the campaign, the capacity to provide a live view on how it is developing to interested parties could be of great value. Decisions about which aspects of reports to publish information about will be taken on a campaign by campaign basis, but these will always be sufficiently broad as to mitigate any possibility of a reporter being identified. For example, a campaign might export a live feed of the number of

submitted/verified reports, a breakdown by type if the campaign covers different types of violations, and a geographical breakdown at the city/county level.

Integration with WikiRate in this manner will take priority for every reporting campaign that will gather information on business and human rights or other aspects of company behaviour. Figure 12 shows an overview of how The Whistle integrates with the ChainReact data ecosystem.

The integration with WikiRate can be illustrated by re-visiting one of the scenarios described in the DoA – that of a fast-food worker in Scotland responding to a living wage campaign (Fig. 1-3 in DoA). In that scenario the fictional Andy submitted a report about his working conditions at a particular McDonalds branch, his contract type, average hours per week, hourly wage and an optional description of his working conditions. Andy also redacted an image of his most recent payslip and uploaded this as evidence in support of his report. In the initial description of the TalkFree platform, this information was immediately published as a “report” that was open to community review, and the responses within reports were publicly available as data-points (mapped to geographical locations). In this scenario, the reporter was responsible for protecting their identity by redacting their payslip and not revealing too much about themselves in the written description.

Our updated approach to this scenario with The Whistle would be for the reports to be reviewed by the partner NGO, whose representatives would then make a decision about whether each report appeared to be legitimate (in this case by checking the reporter's uploaded payslip). When reports are verified, some parts of them could be used to create a “source” entry on WikiRate. In the above example Andy's report might be condensed into a source saying that a **male** worker at **McDonalds** in **Scotland** earns **£6.50** per hour. This data-point would then be available to anyone that wants to analyse companies' performance in relation to issues like the Living Wage or gender pay parity – while only the NGO representatives will have access to the full detail of the original report.

Alternatively, the point of integration with WikiRate could be the output of a query about verified reports. For example, the **number of reports** submitted about **McDonalds** in **Scotland**, and/or the **average wage** reported for workers in **McDonalds** in **Scotland**.

Sources from The Whistle on WikiRate would be presented as coming from a specific Whistle reporting campaign and having been verified by whichever NGO performed that task. With this approach, data flowing from The Whistle to WikiRate can be treated as a trusted source (as trustworthy as the NGO performing verification), without having to make the accompanying evidence available. Reporting campaigns will be tailored so that only relevant variables that are safe to display can appear on WikiRate, and these will be passed through a human filter before doing so.

ChainReact

consortium roles and data flows

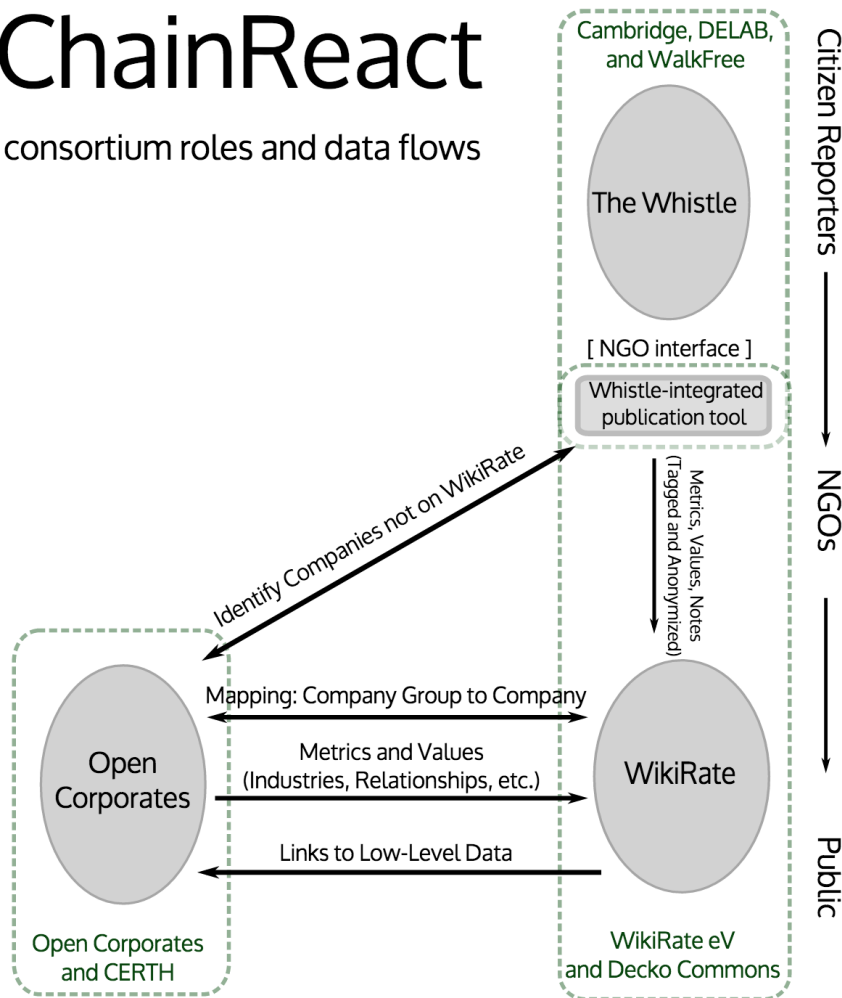


Figure 12 - Integration of The Whistle within the ChainReact data ecosystem

2.8.3 Distributed Ledger and Blockchain

We are exploring the role that distributed ledger technologies like Blockchain could play for The Whistle. As part of this exploration we have been consulting with a group at the University of Cambridge's Computer Lab who are researching novel applications of distributed ledger technology.

For The Whistle, the purpose of using a distributed ledger technology would be related to preserving and ensuring the integrity of submitted reports. The decentralised nature of these approaches, and the fact that records would be distributed across many peers, make them unsuited to handling sensitive data that could identify a reporter. As such, were a technology like Blockchain to be integrated it would be used with only certain aspects of reports that were deemed safe for sharing in this way.

As we continue to explore the affordances of Blockchain, we will be better placed to determine how this approach could be used. One possibility is that it could serve as the mechanism for external publication of data on reports (see 2.8.2 above), with blocks being added to the chain only after the NGO has verified reports. This would have the advantage of a human filter to ensure that sensitive information or information that could be used to identify the reporter is not published. The blockchain could then be presented as a robust public record of verified reports received by The Whistle campaigns. In this scenario, external users of campaign data would acquire it by querying the blockchain, rather than through API calls to a server storing non-sensitive abstractions of reports.

3 WP3 SMART targets

The main target around which WP3 work is being planned is “ST7 - Alpha product ready and tested”, which is scheduled to be completed by M18. Depending on how quickly a firm agreement can be reached with the NGO partner for the first reporting campaign, and the nature of the challenges this campaign presents, this target could still be achieved.

Two factors are delaying progress towards this target. Firstly, we are yet to secure a firm commitment from the NGO partner for the first reporting campaign (ST9, due for completion by M15). Discussions are ongoing with several NGOs, and have reached an advanced stage with two. It is anticipated that the details of the first reporting campaign will be confirmed in a matter of weeks. The choice of which reporting campaigns to embrace is a strategic one that will have a big impact on the success of the project. Finding a good fit between these campaigns and The Whistle, and producing successful outcomes, are our top priorities.

Secondly, a lead developer has not yet been hired (ST5, was due to be completed by M12). Recruitment for a lead developer was initially being conducted through DELAB, but no suitable candidates applied for the position. Recruitment efforts have since been extended to Cambridge and Decko Commons, and while suitable candidates have applied and been interviewed none of these have been sufficiently impressive to warrant an immediate hire. The role of lead developer for The Whistle is an important one which will shape the technical architecture of the platform. While we are waiting to confirm the details of the first reporting campaign, hiring a lead developer is not the top priority. There are advantages to hiring for this position after the details of the campaign are confirmed - this will allow us to give the developer a very clear brief on what the platform needs to support by the launch of the first reporting campaign. Giving the expanded search additional time also increases the chances that we can find even more skilled candidates for the role.

We are confident that once the details of the first reporting campaign(s) are agreed with partner NGOs, development work will not significantly slow down the timeframe to deployment. Our plan calls for close partnership with these NGOs on design specifics, and this will dictate the pace of development. We are very confident that the project’s aim of running three test reporting campaigns within the duration of the project will be met, and expect to exceed this target.

As noted in the executive summary, it is our intention to submit an updated version of this deliverable ahead of the project’s interim review – deliverables for WP3 were scheduled in the expectation that reviews would be annual, we anticipate making significant progress in WP3 before M18 and will communicate this in an

updated report ahead of the review. This updated version of the deliverable will detail new SMART targets and progress against existing targets.

4 Appendix

4.1 - Web form civilian witness front-end mock-ups

The following mock-ups illustrate the kind of information which may be requested and provided as part of a reporting campaign, structured as a web form.

Submit your report

To collect eyewitness report on the situation in X, ABC NGO is using The Whistle, a digital reporting platform for witnesses of human rights violations based at the University of Cambridge.

Your eyewitness reports are very valuable to us. Before we are able act on any information, including yours, we must verify it. This allows the information to stand up in the courts of law and public opinion.

This reporting platform will prompt you to supply a variety of information that we need to verify your report. It will ask for you to enter information over a few pages that correspond to the four key questions that must be answered to verify information: What, Where, When, and Who. Please fill out as much as you know and is safe.

[Enter The Whistle's reporting platform](#)

What happens to your report?

One of our researchers will read your report carefully. If you have provided identifying information, the researcher may contact you.

Your reports help us document the situation in X and to advocate for change. [Click here](#) for our work to date on the situation.

Your report will be stored on The Whistle's server and will be accessible both for human rights work on this situation and for future research by trusted partners.

Powered by



The Whistle

WARNING!

Our researchers are trained in handling sensitive information securely, and our reporting platform, The Whistle, works to maintain high security standards for the communication, handling, and storage of your reports.

Even so, **communicating online is never risk-free**. Out of an abundance of caution, we urge you to approach submitting a report via The Whistle as if you were saying it out loud in public. Even if you submit a report anonymously, it may still be possible for it to be traced back to you. **If reporting it would put you at risk, please do not submit a report.**

I have read and understood the above.

Find out more about
your risks online

Learn how to communicate
more securely online

Proceed to submitting
your report

What

Knowing what happened is crucial to the report. Please provide as much detail as possible.

Title:

Description (please provide chronological detail):

How do you know?

Why were you there?

Where were you standing?

Upload photos, videos, documents documenting the incident (originals preferred):

Page 1 of 5

Where

Knowing where the incident happened allows us to cross-reference your report with other reports and is key to making a case for courts or advocacy.

What is the closest city or town to the incident? Please describe the closest significant landmark



Where are you now?

If you are at the scene of the incident, please upload a photo of it now, at the time of your report:

Please click on the location on the map above.

What is the address of the incident?

When?

Knowing when the incident happened allows us to cross-reference your report with other reports and to establish a time-line that is key to making a case for courts or advocacy.

What date did the incident occur?

What time was it where the incident took place?

What happened just before the incident took place?

What happened just after the incident took place?

Who?

Only supply identifying and contact details for you, the subjects of your report, and/or corroborating witnesses if it is safe to do so!

We are happy for you to submit your report anonymously. Providing contact information, however, if safe, allows us to follow up with more questions if we have them. Providing identity details allows us to understand more about you, how you have the information in your report, and why you are sharing it with us.

YOU

Name:

Email:

Phone number:

Social media accounts:

Any institutional affiliation (school, university, job):

SUBJECT 1 of YOUR REPORT

Name:

Email:

Phone number:

Social media accounts:

Any institutional affiliation (school, university, job):

CORROBORATING WITNESS 1

Name:

Email:

Phone number:

Social media accounts:

Any institutional affiliation (school, university, job):

ADD another SUBJECT

ADD another WITNESS

Corroborate and submit your report

It helps us move more quickly if you can provide links to corroborating reports, whether from civilians or from the media.

Seeing how others respond to social media posts can provide us with some verification cues, as can the media's decision to cover and manner of covering the incident.

Have you or others posted about this incident on social media? If yes, please provide the link(s) here:

+

Has the incident been reported in the news? If yes, please provide the link(s) here:

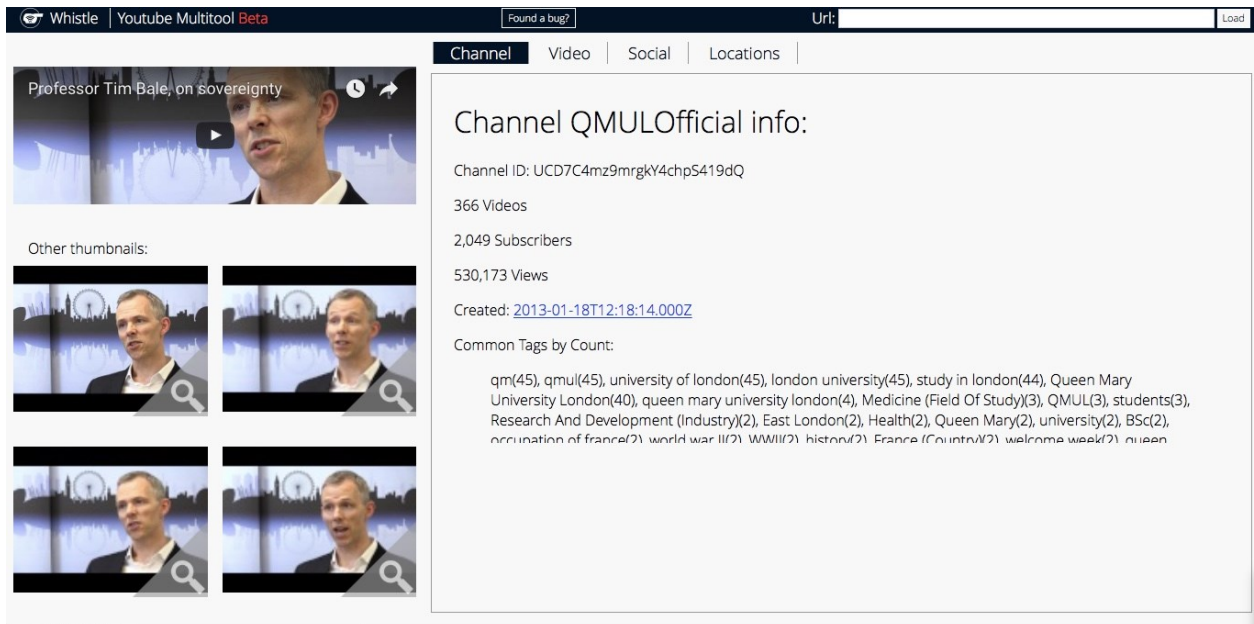
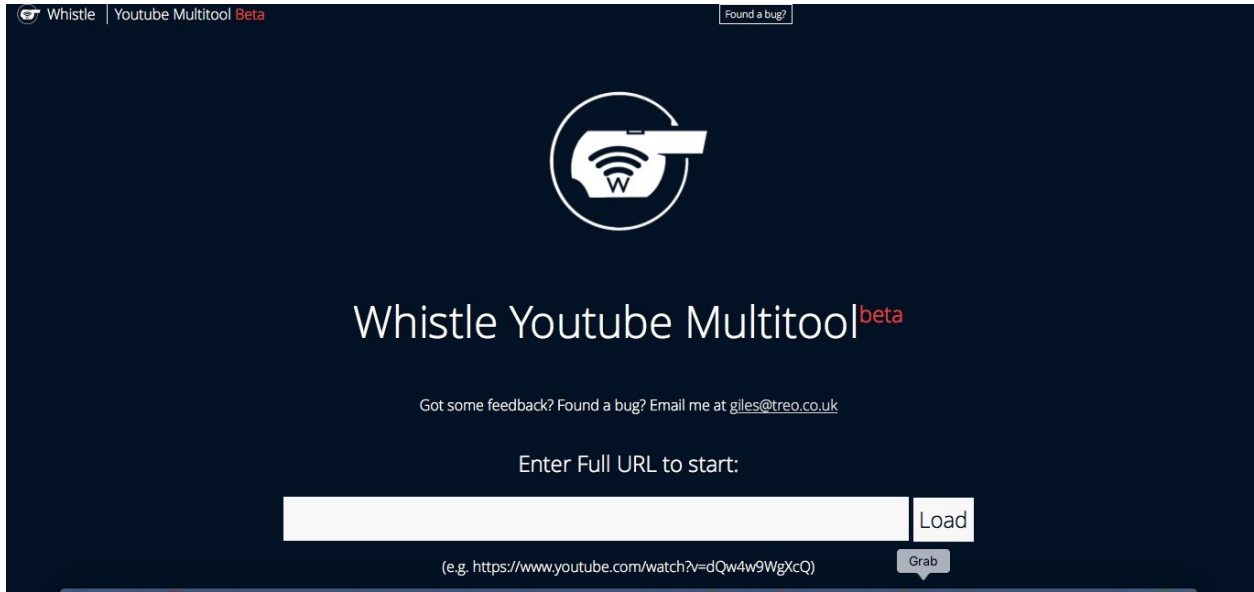
+

SUBMIT YOUR REPORT

Page 5 of 5

4.2 - Youtube Multitool


The following images show the Youtube Multitool prototype in use.







Whistle | Youtube Multitool Beta | Found a bug? | Url: | Load

Channel | **Video** | Social | Locations

Professor Tim Bale, on sovereignty



Other thumbnails:




Video info:

Title: Professor Tim Bale, on sovereignty
Video ID: Oo6h6xp9Uxw
Published: [2016-05-16T15:33:43.000Z](#)
Description:
Professor Tim Bale from QMUL's School of Politics and International Relations speaks about sovereignty. [Add playlist link if necessary] In this video [insert description]
Tags: sovereignty, QMUL, Tim Bale, Mile End Institute
Views: 204
Likes: 0 Dislikes: 0
Comments: 0
Video location: [Lat: 51.52366 Long: -0.04061](#)





Whistle | Youtube Multitool Beta | Found a bug? | Url: | Load

Channel | Video | **Social** | Locations


Professor Tim Bale, on sovereignty



Other thumbnails:



Profile links:

- <https://plus.google.com/112910016137829425327>
- <https://www.facebook.com/QMUL>
- <http://www.twitter.com/qmul>
-  9440 Tweets - Follows: 1193 - Followers: 1193
- <http://instagram.com/officialqmul>
- <http://www.linkedin.com/company/9911?trk=tyah>
- <http://www.qmul.ac.uk>

Whistle | Youtube Multitool **Beta** | Found a bug? | Url:

Channel | Video | Social | **Locations**

Professor Tim Bale, on sovereignty

Other thumbnails:

Locations mentioned in tags:

Found using 'http://nominatim.openstreetmap.org/search.php'
