Handbook: The 3L Whistleblowing Platform

July 2020

Authored by Panayotis Yannakas (3L NPO)
Naomi Colvin (Blueprint NPO), with material from EAT Project.

blueprint for FREE SPEECH

E.A.T. EXPANDING ANONYMOUS TIPPING

3L LEGAL · LEGION · LOYALTY

Contents

Introduction 4

Things we consider 6

We Respect Anonymity 6

We verify material based on the value of the information, not on our our opinion 6

We will escalate concerns to authorities where appropriate 7

We securely delete data 7

When you send a disclosure 8

Social risk 8

Minimizing social risk 8

Technological risks 9

3L Investigation Model 11

The content of this handbook represents the views and working practices of 3L and we take sole responisbility for its content. The EAT Project does not accept any responsibility for the contents of this document.

Introduction

Legal Legion (loyalty) NPO launched a high-security digital platform based on Tor Network in January 2020, in order to protect any citizen who wants wants to report wrongdoing, malpractices, crimes or other acts against the public interest.

The 3L whistleblowing platform looks forward to encouraging citizens to report through a secure digital and dropbox to protect the information and the integrity of the reporting person.

Our software and hardware infrastructure allows sources to stay anonymous while submitting sensitive information in a secure and safe way. Data being transmitted, and data stored using our platform is always encrypted.

Whistleblowers are individuals who speak up about any kind of wrongdoing that can harm the public interest. Whistleblowers might make reports about actual or potential harm to the environment, public health, consumer safety or public finances.

Legal protections for whistleblowers are currently fragmented. At the time of writing, no more than 10 EU countries have a comprehensive law protecting whistleblowers. The new EU Directive (2019/1937) will change this, at least for whistleblowers with reports about their workplace.

As 3L, we recognise and welcome the reverse trend. A study carried out in 2017 for the Commission estimated the loss of potential benefits of not protecting whistleblowers, in public procurement alone, as being in the order of €5.8 to €9.6 billion each year for the EU as a whole.

Whether the trends towards better protections are real or just another political aspiration, we strongly believe that, as a non-profit, non-corporate and non-compromised entity and team, we take our own practical steps to protect whistleblowers. Deeper questions of whistleblowing, the whistleblower's moral responsibility or about the aspect of confidentiality and civil disobedience are grounded

themselves in an amoral mindset. Above any laws, constitution or system of rules, shall be the well-functioning and harmony of the State, of the People and of the Peace.

The Tor Network is an extremely beneficial technology. However, the often illegal uses allege the Tor Network with the packaging of crimes and urban disorders. Nobody must forget that the spark of the Tor Network was born inside the U.S. Naval Research Lab (NRL). The 3L wants to become a healthy inspiration for a new generation uses of the Tor Network, of the anonymity and the other privacy tools.

Staying focused on the above goal, in July of 2020, we reach an agreement with a pan-European whistleblowing network. The propose of agreement mainly is the access in a unique and powerful scheme of anti-corruption activists and government-relative scientists and professionals. The new 3L whistleblowing platform is created thanks to the support of the EAT (Expanding Anonymous Tipping) project, co-financed by the Internal Security Fund at the European Commission

We strongly believe that as public interest lawyers who are not beholden to any special interest group, we are the right people for you to entrust your story, and your evidence to.

Things we consider

We Respect Anonymity

Even when the reporting person includes, partial or no, personally identifying information in their report, 3L will assume that the reporting person still wanted to stay anonymous. Any initial investigations are undertaken without identifying information being required or stored.

We strongly believe that once a whistleblower has confidence that an investigation is being undertaken in a way that protects his/her confidentiality minimising the risks to suffer retaliation, that they may be more comfortable to collaborate with us.

In order to increase confidence, we give whistleblowers feedback about the progress of an investigation. We are clear with them about what they can expect to receive from us in terms of support and assistance.

Retaliation is a real threat for many whistleblowers. For each case, we design the investigative procedure that will minimise those risks.

The new EU Whistleblower Directive makes stipulations about investigation procedures and timelines that should be regarded as a baseline standard: 7 days as confirmation of receiving the submission and 90 days sending out the proposal on further steps, offering our opinion or solution or request extra information.

We verify material based on the value of the information, not on our our opinion

We will judge any report on its merits. In the final analysis, it is quality and verifiability of the information supplied that is most important.

Assessing the motivation of the source is important only insofar as it assists in judging the veracity of a report.

We will escalate concerns to authorities where appropriate

We understand that some issues carry an obligation to pass concerns to regulators or other authorities.

We are willing to involve the appropriate authority when this becomes necessary. This is assessed on a case-by-case basis.

We securely delete data

We except that sometimes a report may include personally identifying data, both of the reporting person and potentially also of those who are the subject of the report.

While the preservation of these data will be required for a certain time in order to make sure that reports are adequately investigated, the material will eventually be deleted in accordance with data protection standards. This commitment also applies to metadata.

When you send a disclosure

When submitting sensitive information, you must consider the risks related with taking that action in revealing the truth, as you may be subject to retaliation by parties that do not like what you have to say. That is why you must take all possible actions to preserve your anonymity.

Anonymity technology cannot give you a complete guarantee of security. You should try to be aware of the technical risks and think about the potential social impact before you act, and take the right countermeasures to protect yourself. What those protection strategies are will depend on your particular situation.

Social risk

Before submitting any information, you should consider what will happen after the information has been sent. For example, you should consider what might happen if the issue you are making a report about comes to public attention.

Ask yourself the following questions to understand the degree of risks you face:

- Do people other than you have access to the information you are going to submit?
- If the information you submit comes to public attention, are you likely to be asked about it?
- Are you able to cope with the stress of an internal or external investigation around your submission?
- Are you ready to handle possible negative publicity based on misinformation, or abuse online?

You should consider submitting to the 3L Whistleblowing Platform only after a full understanding and deep reflection on the previously illustrated points.

Minimising social risk

From a social protection perspective, you should try to take precautions like the following:

- Before you make a submission, do not express your intention to anyone.
- After you make a submission, do not reveal what you have done to anyone.
- If news based on your submission becomes public, be really careful in expressing your opinion about it with anyone.
- Be sure that there is no surveillance system (cameras, surveillanced network, etc.) in the place where you acquire and submit the information.
- Do not look around on search engines or news media website for the information you submitted – this would reveal that you knew about it earlier.
- Consider the possibility that your family, friends, or close colleagues may also face risks.

Technological risks

You must be aware of the fact that while using a computer and the Internet to exchange information, most of your actions have the potential to leave traces and computer logs, that could lead an investigator to identify where you are and who you are.

For this reason, you must consider the risks, mitigation strategies and adopt specific precautions to avoid leaving technological traces about your actions online.

The complexity of network system means that fully understanding the technological risks associated with a disclosure can be difficult. While no technology can offer a 100% guarantee of security, there are recognised procedures for the mitigating the risks.

However, by strictly following the procedures and tips reported below, you should be safe enough:

- Submit information using Anonymous Web Browsing software Tor Browser.
- Do not submit information from the personal computer provided to you by your employer.
- Keep the receipt with your key of your submissions safe and destroy this information when you don’t need it anymore.
- Do not keep a copy of the information you submitted.
- While acquiring the information to be submitted, try to ensure that that you are not leaving a trail could lead back to you (e.g.: if you use files on a USB key to make

a submission, delete those files after making your submission and fill the device with innocuous files).

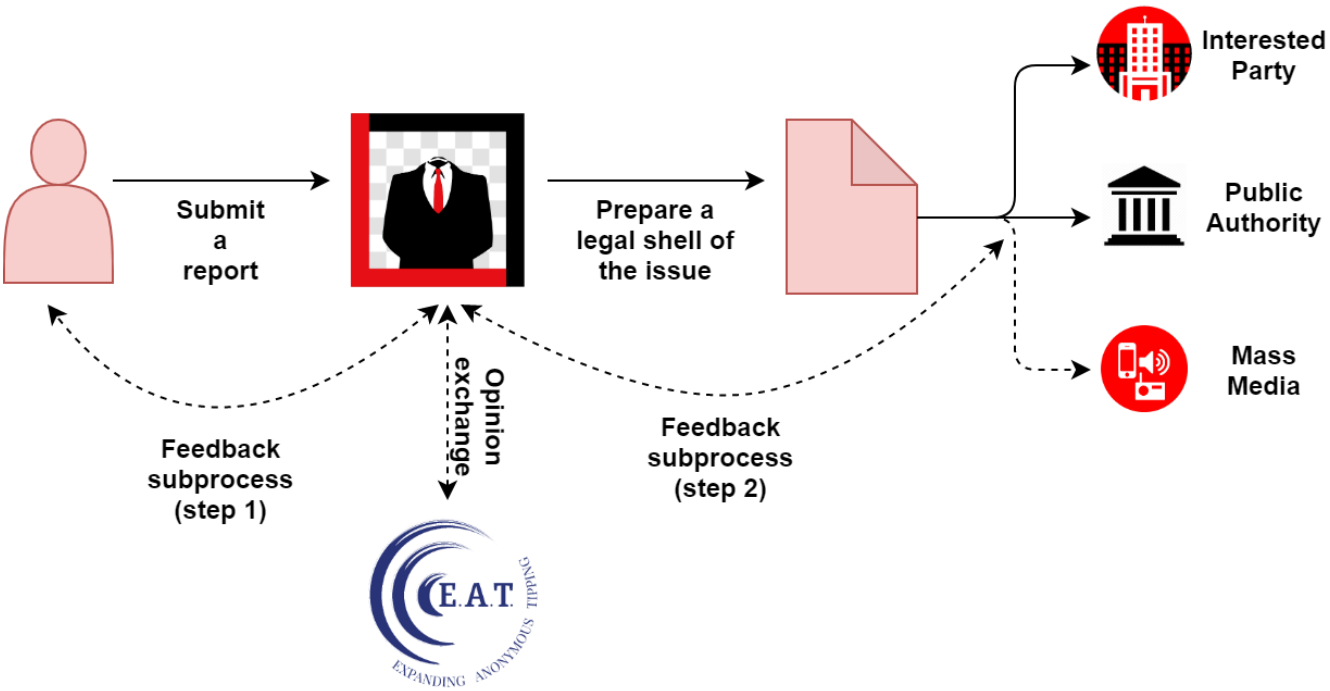
- Be aware of the fact that “metadata information” may be present in some of the data you are submitting.
- Consider converting all the data you are sending us into the standard PDF format.

3L Investigation Model

The vast majority of the 3L members are Lawyers with secondary studies in fields like Government Management or Business Administration. We also have expertise in areas such as Money Laundering.

We believe that our involvement is necessary in order to keep identities confidential. From our work experience, we understand how difficult it can be to come forward with concerns. We aim to provide legal support and give advice on other ways to have your report resolved.

After the understanding of the wrongdoing, a process which may also include a feedback subprocess with the reporting person, we will decide if it is more suitable to forward the case at the interested party, at the competent public authority or both of them, without excluding the support of mass media.



How 3L NPO handle a report