This project is funded by the European Union

Breaking the Silence:

Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

PEER-TO-PEER REGIONAL MEETING OF PUBLIC INSTITUTIONS

'Improved whistleblower protection through better laws and enhanced transparency'

SECOND ANNUAL REGIONAL MULTI-BENEFICIARY TRAINING ON WHISTLEBLOWER PROTECTION

'Whistleblower Disclosure and Protection in Practice: Discussion of Challenges and Solutions'

ANNUAL MEETING OF THE SEE COALITION ON WHISTLEBLOWER PROTECTION

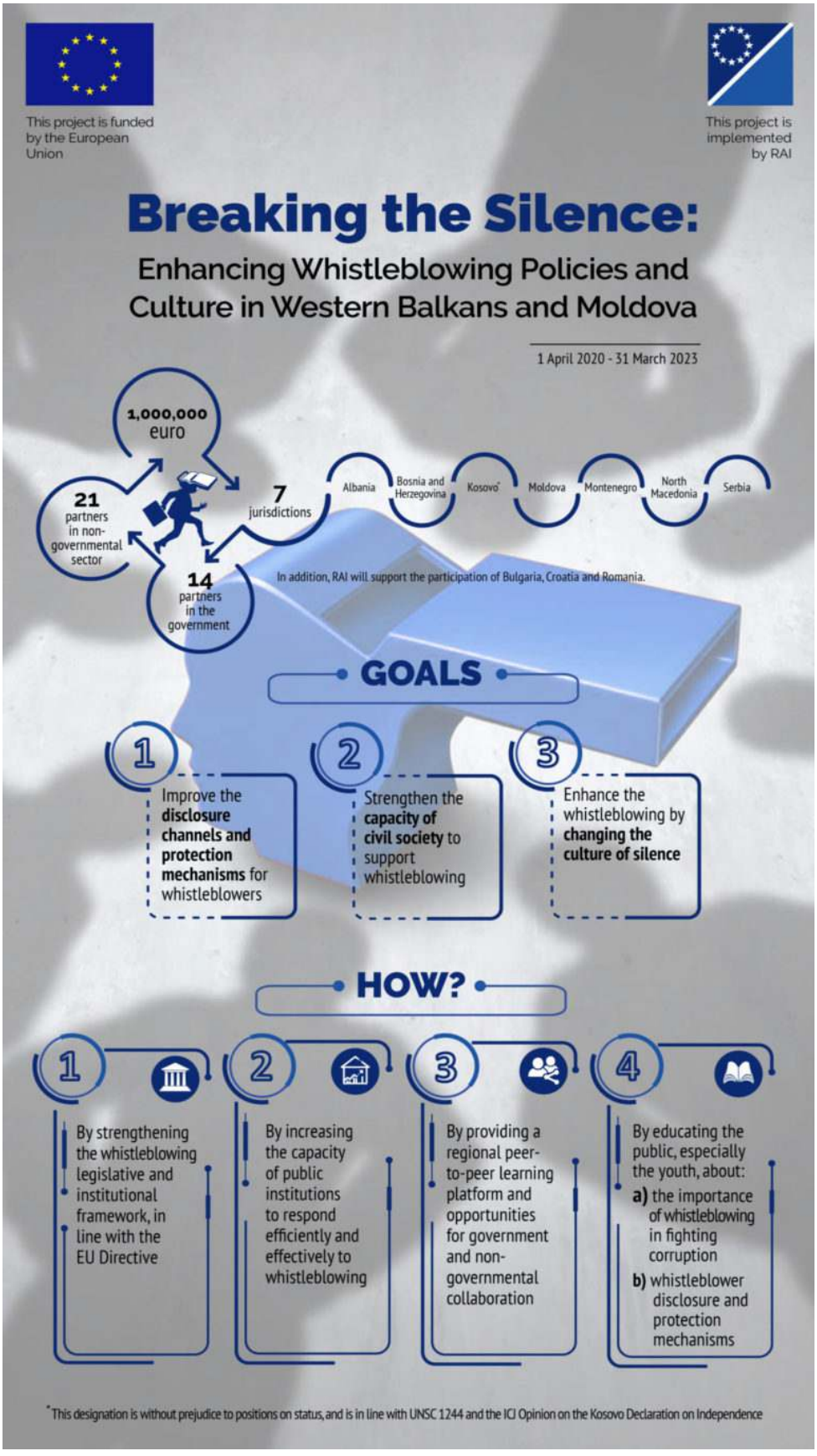
'Whistleblowing and Whistleblower Protection in SEE: Challenges and Opportunities

16 - 19 November, 2021

Sarajevo, Bosnia and Herzegovina

Contents:

1. ABOUT THE PROJECT (PROJECT INFOGRAPHIC)



2. CONCEPT PAPER AND AGENDAS

Background

The RAI Secretariat regional project 'Breaking the Silence: Enhancing the Whistleblowing Policies and Culture in Western Balkans and Moldova' (hereinafter: the Project) is an EU-funded project which covers the following jurisdictions: Albania, Bosnia and Herzegovina (BiH), Kosovo*, Moldova, Montenegro, North Macedonia and Serbia, with participation of Bulgaria, Croatia and Romania. The project implementation commenced on April 1, 2020 and will end on March 31, 2023. The aim of the Project is to help its partners in the government and non-governmental sector to improve whistleblower protection through better laws, but also through improved application of current laws, in line with the EU Whistleblower Protection Directive[1]. Finally, the Project aims at informing and educating the public, in particular the youth, on the key role that whistleblowers play in the fight against corruption.

Under the Project *Output 1.3: Strengthened capacities, peer-to-peer and cross-sectoral exchanges with and among selected public institutions, free legal aid providers, and other identified CSOs,* RAI Secretariat is to engage with public institutions, CSOs and other stakeholders in knowledge building, knowledge sharing, outreach and advocacy.

To that end, among other things, RAI Secretariat is to deliver:

1) Peer-to-Peer regional Meetings of Public Institutions focused on structured dialogue and expertise exchange, at a technical level, about whistleblowing and whistle-blower protection;
2) Annual Meeting of the SEE Coalition on Whistleblower Protection.

Objectives:

Peer-to-Peer Regional Meeting of Public Institutions

In September 2021, RAI Secretariat published the Gap Analysis of Whistleblower Protection Laws in the Western Balkans and Moldova (hereinafter: Gap Analysis), which examines whether and to what extent EU Whistleblower Protection Directive standards are incorporated in whistleblower protection laws of these jurisdictions.

According to the findings of the Gap Analysis the following standards were often inadequately incorporated in the laws of these jurisdictions: 1) the "reasonable grounds to believe that the reported matter is true" standard for whistleblower disclosures; 2) the protection of whistleblower disclosures made to the public; 3) types of misconduct that may be reported under the law; 4) the scope of protection for all potential whistleblowers with significant evidence; 5) clarity and accessibility for anti-retaliation protection; 6) relief through legal remedies; 7) reverse burden of proof on employers to show actions taken against employees are not linked to whistleblowing; 8) penalties for retaliation and other actions; 9) the protection of whistleblower against civil and criminal liability; 10) credible reporting channels that enfranchise whistleblowers to follow up on reports; and 11) transparency of the law's results, in terms of impact from whistleblowing reports and effectiveness against retaliation.

The regional meeting will aim at equipping professional staff who participate in whistleblower protection policy making, oversight and enforcement with:

This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration on Independence

[1] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, https://eur-lex.europa.eu/eli/dir/2019/1937/oj

1) *Legislative solutions relevant to achieving improved whistleblower protection*, which will include suggested legislative language to address shortcoming identified through the Gap Analysis, dos and don'ts and examples from practice to support these solutions.

2) *Practical knowledge about transparency requirements and solutions relevant to assessing the impact of whistleblower protection laws* – According to the EU Whistleblower Protection Directive, member States will be required to report on: (a) the number of reports received by the competent authorities; (b) the number of investigations and proceedings initiated as a result of such reports and their outcome; and (c) if ascertained, the estimated financial damage, and the amounts recovered following investigations and proceedings, related to the breaches reported.

Finally, the regional meeting of public institutions will enable the *peer-to-peer exchange of experiences and lessons learned for purposes of identifying best practice solutions and translating them into action leading to better whistleblower protection*.

Second Annual Regional Multi-Beneficiary Training on Whistleblower Protection

In line with beneficiary input provided through the evaluation of the first training, the **Second Annual Regional Multi-Beneficiary Training on Whistleblower Protection** will focus on 'Whistleblower Disclosure and Protection in Practice: Discussion of Challenges and Solutions'. The objective of the training is to equip trainees with practical knowledge and tools relevant to enabling effective whistleblower disclosures and protection in general. Additionally, specifics of the enforcement of whistleblowing in the education and health sector will be addressed.

The training will aim at responding to the following questions:

1) what is required to build an organizational culture in which whistleblowers feel safe to report misconduct, including how to identify and mitigate factors which deter employees from blowing the whistle and how to inform and educate employees to address underreporting caused by negative perceptions about whistleblowing and whistleblowers (dos and don'ts, roleplays, practical exercises),
2) how to improve whistleblower disclosure channels, whistleblower protection and the investigation of whistleblower disclosures by focusing on results rather than procedure (dos and don'ts, case study of an effective system in EU and US),
3) effective legal aid programmes for whistleblowers and their judicial protection (dos and don'ts, case study of an effective system in EU and US) and
4) how to deter retaliation (e.g. effective sanctions, anti-retaliation training for employers/management and similar).

Finally, the training will enable *intersectoral exchange of experiences and lessons learned for purposes of identifying opportunities for mutual collaboration on effective whistleblower disclosure and protection, with the goal of properly protecting citizens from retaliation and investigating reports of misconduct*.

Annual Meeting of the SEE Coalition on Whistleblower Protection

The **Southeast Europe Coalition for Whistleblower Protection** (hereinafter: Coalition) **annual meetings**[2] are dedicated to the strengthening of the Coalition, membership expansion, and diversification. The annual meetings serve as a platform for discussion of common challenges, strategies and solutions for improving the protection of whistleblowers, as well as on how to best utilize the Coalition resources. Finally, meetings are an opportunity to celebrate success and capture lessons learned.

Event Format

The **regional meeting** will be delivered in-person and will take place in a mixed environment of representatives of public institutions responsible for policy making/legislative drafting, oversight or the enforcement of whistleblowing. In order to encourage a structured and solution orientated discussion, RAI Secretariat international experts will produce and present a paper on best practice legislative solutions in whistleblower protection and transparency requirements, to be provided to the participants in advance.

The expert presentation will be followed by a Q&A session, tour-de-table presentations of experiences and lessons learned, structured discussion, recommendations and conclusions. As such, the regional meeting will be interactive and will effectively enable the definition of best solutions based on experiences and expertise of the entire region.

The working language of the regional meeting is English. No interpretation will be provided.

The training will be delivered in-person[3], in a mixed environment of representatives of public institutions responsible for policy making, legislative drafting or the enforcement of whistleblowing, and representatives of CSOs involved in whistleblowing enforcement and advocacy.

The training will be delivered by international experts on whistleblowing. It will combine trainer introductory remarks, roleplaying, case studies, trainer and trainee reflections, structured discussions, recommendations and conclusions. As such, the training will be interactive and will effectively enable learning from experiences and expertise of the entire region.

Participants will be provided with relevant materials at training. The training will be evaluated at the end, and it will be re-evaluated in six months to measure retention of training outcomes. Trainees will be asked to provide inputs for the next cycle of training.

The **Coalition meeting** will be delivered in-person and co-hosted by the Foundation Infohouse (infohouse.ba), a member of the Coalition from Bosnia and Herzegovina.

The Coalition meeting will take place in a mixed environment of representatives of: a) CSOs from SEE involved in public policy advocacy, legal aid and other support to whistleblowers, and b) CSOs from SEE who wish to learn and engage in the promotion of whistleblowing in their respective sectors (e.g. health, education, environment).

[2] The first such meeting supported by RAI Secretariat under the Project was held online on November 30, 2020, and co-hosted by the Centre for the Study of Democracy and Governance, a member of the Coalition from Albania.
[3] In case of travel restrictions imposed on registered participants due to COVID-19, or other force majeure, a hybrid format of the training shall be considered.

The guest presentations will be followed by tour-de-table presentations of experiences and lessons learned of CSOs, structured discussion, recommendations and conclusions. As such, the Coalition meeting will be interactive and will effectively enable the definition of best solutions based on experiences and expertise of the entire region.

The working language of the training and the Coalition meeting is English. No interpretation will be provided.

Participants:

Regional Meeting

Participants are professionals from Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Kosovo*, Moldova, Montenegro, North Macedonia, Romania and Serbia. At regional meeting, each of the jurisdictions will be represented by two public institutions responsible for policy making/legislative drafting, oversight or the enforcement of whistleblowing. The maximum number of participants per public institution is one staff member. Priority should be given to middle management and staff who directly develop or implement whistleblowing policies and procedures.

Training

Training participants are professionals from Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Kosovo*, Moldova, Montenegro, North Macedonia, Romania and Serbia. At training each of the beneficiary jurisdictions will be represented by two public institutions and three CSOs.

The training is intended for:

1) staff of public institutions involved in policy making, legislative/regulatory drafting or the enforcement of whistleblowing from ministries of justice, anti-corruption agencies (or other whistleblowing oversight bodies), ministries of education and public health sector institutions.
2) staff of CSOs involved in whistleblowing enforcement, promotion of education or public health.

The maximum number of trainees per public institution or CSO is one staff member. Priority should be given to middle management and staff who directly implement whistleblowing policies and procedures.

Coalition Meeting

Participants are CSOs from Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Kosovo*, Moldova, Montenegro, North Macedonia, Romania and Serbia. Additionally, the participation of Coalition members from Hungary, Slovakia, Czech Republic, Greece and SEEMO will be enabled through the Coalition project funded by NED.

Each of the jurisdictions will be represented by maximum three CSOs. The maximum number of participants per CSO is one staff member.

*This designation is without prejudice to positions on status, and is in line with UNSCR 1244(1999) and the ICJ Opinion on the Kosovo declaration of independence.

Peer-to-Peer Regional Meeting of Public Institutions

Improved whistleblower protection through better laws and enhanced transparency

Tuesday, 16 November, 2021	
09:30 – 10:00	**Registration and welcome coffee**
10:00 – 10:10	**Opening Remarks** *Ms. Desislava Gotskova, Head of RAI Secretariat* *Mr. Enrico Visentin, Program Manager, EU Delegation to BiH*
10:10 – 10:40	**Presentation of legislative solutions to address shortcomings identified in the Gap Analysis: Dos and Don'ts, Examples from Practice** *Mr. Tom Devine, Whistleblowing Expert* *Mr. Mark Worth, Whistleblowing Expert*
10:40 – 11:00	**Questions & Answers**
11:00 – 12:00	**Tour-de-table presentations of experiences and lessons learned** *Participants*
12:00 – 12:40	**Discussion and Conclusions**
12:40 – 13:40	**Lunch**
13:40 – 14:10	**Presentation of transparency requirements and solutions relevant to assessing the impact of whistleblower protection laws: Best practice case study and lessons learned** *Mr. Tom Devine, Whistleblowing Expert* *Mr. Mark Worth, Whistleblowing Expert*
14:10 – 14:30	**Questions & Answers**
14:30 – 14:45	**Coffee break**
14:45 – 15:45	**Tour-de-table presentations of experiences and lessons learned** *Participants*
15:45 – 16:15	**Discussion and Conclusions**

Second Annual Regional Multi-Beneficiary Training on Whistleblower Protection

Whistleblower Disclosure and Protection: Discussion of Challenges and Solutions

Day 1 Wednesday, 17 November, 2021	
09:30 – 10:00	**Registration and welcome coffee**
10:00 – 10:10	**Opening Remarks** *Ms. Elmerina Ahmetaj Hrelja, Project Manager – Anticorruption Expert*
10:10 – 10:40	**Discussion: Taking Stock** - A wide-angle view of recent developments in whistleblower protection, current issues and future efforts *Moderators: Mr. Tom Devine, Mr. Mark Worth and Mr. Thad Guyer , Whistleblowing Experts*
10:40 – 11.45	**Discussion: Review of recent and ongoing whistleblower cases and retaliation complaints** - How public institutions are assessing and responding to whistleblower reports, and a discussion about improving protections and investigations *Presenters/Moderators: Mr. Thad Guyer and Mr. Tom Devine*
11:45 – 12:30	**Worksheet and discussion: Handling whistleblowing reports or disclosures and retaliation complaints objectively and fairly, to minimize retaliation and maximize impact** - How to ensure whistleblower protection laws achieve their goals: protection, corrective actions and justice *Moderators: Mr. Mark Worth and Mr. Tom Devine*
12:30 – 13.30	**Lunch**
13:30 – 14:00	**Closing the loop: Putting public officials in the shoes of the citizens to improve protections and fair treatment** *Presentation and discussion with Ms. Wendy Addison of SpeakOut SpeakUp*
14:00 – 15:30	**Role-playing an interaction with a witness in the workplace** - Participants will play the role of citizens and managers in order to engender the sense of fairness and objectivity required to effectively protect whistleblowers and investigate misconduct *Moderator: Mr. Mark Worth*
15:30 – 15:45	**Coffee break**
15:45 – 16:15	**The Whistleblower Dilemma: Understanding the nature, legal dimensions and control of 'information'** *Presenter: Mr. Thad Guyer*

Day 2 **Thursday, 18 November, 2021**	
09:30 – 10:00	**Registration and welcome coffee**
10:00 – 10:30	**Opening Remarks** - Participants will discuss how they would handle current and recent cases differently in light of the Day 1 discussions *Moderator: Ms. Elmerina Ahmetaj Hrelja*
10:30 – 11:30	**Discussion: Lifecycle of a Whistlebower Case** - The questions and challenges that arise in a retaliation case, and the proper responses to retaliation complaints *Moderator: Mr. Mark Worth*
11:30 – 12:30	**Discussion: Recognizing retaliation** - How to identify retaliation through the rules of evidence, experience and common sense *Moderator: Mr. Tom Devine*
12:30 – 13:30	**Lunch**
13:30 – 14:00	**Worksheet and discussion: Whistleblowing and public disclosure** - When is it justified to bypass workplace and regulatory disclosure channels, and make a report directly to the public or the media? *Moderator: Mr. Tom Devine*
14:00 – 14:30	**Discussion: Overcoming instinctual reactions and biases toward witnesses in the workplace** - The essential role of laws and frameworks in counterbalancing the societal and official scepticism toward whistleblowers *Moderator: Mr. Mark Worth*
14:30 – 15:00	**Legal and Cultural Contexts Influencing Whistleblower Outcomes** *Presenter: Mr. Thad Guyer, Whistleblowing Expert*
15:00 – 15:15	**Coffee break**
15:15 – 16:05	**Conclusion and Closing Remarks** - Participants will discuss how they will strengthen their commitment to assist citizens, protect them from retaliation, and ensure the letter and spirit of whistleblower protection laws are followed *Moderator: Ms. Elmerina Ahmetaj Hrelja*
16:05 – 16:20	**Training Evaluation** through a questionnaire to be filled out by all participants

Annual Meeting of the SEE Coalition on Whistleblower Protection

Whistleblowing and Whistleblower Protection in SEE: Challenges and Opportunities

Friday, 19 November, 2021	
09:30 – 10:00	**Registration and welcome coffee**
10:00 – 10:15	**Welcome and Introductory Remarks** *Mr. Arjan Dyrmishi, Coalition Coordinator* *Ms. Dzenana Aladjuz, Director, Foundation Infohouse* *Ms. Desislava Gotskova, Head of RAI Secretariat* *Mr. Nicolas Bizel, Head of Operations Section I (Justice and Home Affairs, Public Administration Reform), EU Delegation to BiH*
10:15 – 10:45	**Tour-de-table introductions by members of the Coalition**
Guest Presentations and Discussion:	
10:45 – 11:00	**Overview of activities, findings and results of the regional project *'Breaking the Silence: Enhancing Whistleblowing Policies and Culture in the Western Balkans and Moldova'*** *Ms. Elmerina Ahmetaj Hrelja, Project Manager – Anticorruption Expert*
11:00 – 11:30	**How can NGOs help whistleblowers: The experience and lessons learned of the Government Accountability Project (GAP), USA** *Mr. Tom Devine, Legal Director, GAP*
11:30 – 12:00	**What Happens with Whistleblowers' Reports: Serbia Case Study** *Mr. Vladimir Radomirovic, Editor in Chief, Pistaljka*
12:00 – 13:00	**Lunch**
Coalition Member Presentations and Discussion:	
14:10 – 14:30	**Discussion of common challenges, strategies, and solutions for improving the protection of whistleblowers in SEE** Tour-de-table, Coalition members *Moderated by Mr. Mark Worth, Coalition Coordinator*
14:30 – 14:45	**Coffee Break**
14:45 – 15:45	**Presentation of achievements of Coalition members and lessons learned on whistleblower protection in SEE** Tour-de-table, Coalition members *Moderated by Mr. Mark Worth*
15:45 – 16:00	**Conclusions and Closing Remarks** *Mr. Arjan Dyrmishi* *Ms. Elmerina Ahmetaj Hrelja*

3. TRAINING MATERIALS

PAPER AND TRAINING MATERIALS

3.1. Peer-to-Peer Regional Meeting of Public Institutions, November 16

Model Provisions for Whistleblower Protection Laws

Toward ensuring the protection of witnesses in the workplace from retaliation
November 2021

In order for whistleblower protection systems to function properly – for the benefit of citizens and society – the laws that establish these systems must provide public institutions with comprehensive, loophole-free instruments to carry out the goals of whistleblower protection. Without solid legal instruments, there is a great likelihood that witnesses of crime and corruption will not be shielded from reprisals. There is high social cost for this: citizens who believe they will be protected if they report crime or corruption will suffer retaliation, with no legal recourse.

Presented here are model legislative provisions based on the "Gap Analysis of Whistleblower Protection Laws in the Western Balkans and Moldova|" that was produced in 2021 as a part of this project. These are some, but not all, of the provisions that should be included in a comprehensive whistleblower law. However, they are the most crucial in terms of providing whistleblower protection oversight agencies with sufficient tools to shield witnesses in the workplaces from reprisals. Each provision is accompanied by its rationale in real-life situations.

It is recommended that these provisions be adapted to each jurisdiction's constitutional, legal and cultural context.

Designated public institution responsible for implementation and oversight of the Act
Legislative text:
A designated public institution shall have competence for administrative remedies against retaliation; review and action on whistleblowing reports of misconduct; training; public education; oversight and transparency on the law's record. Unless exempt due to organizational size, each institution shall:

- provide advice and counselling support to witnesses in the workplace to understand rights and responsibilities in this Act;
- investigate complaints of retaliation and order corrective action;
- have the independent authority to order temporary relief pending final legal action to cease retaliation or threatened retaliation through relief available under the Act, with the employee authorized to appeal to a competent court for relief if not granted within seven days;
- have the independent authority to find illegal retaliation and order corrective action, subject to appellate review to a competent court by either party. The employee may seek relief *de novo* from a court of competent jurisdiction if not provided within 30 days. Decisions of the competent court are subject to full appellate review;
- receive and assess for credibility reports of misconduct and public health threats;

- order investigation and report on evidence and information from credible disclosures of alleged misconduct to responsible regulatory, investigative and/or prosecutorial authorities for follow-up and corrective actions; and after receiving comments from the whistleblower evaluate whether the response and corrective action are reasonable, forwarding results to executive and parliamentary competent authorities;
- preserve and protect the confidentiality or anonymity as designated by witnesses from exposure of identity or identifying information unless there is prior written consent for discretionary releases or timely advance notice for non-discretionary releases;
- working with competent offices, monitor and assess the accuracy of compliance with this law
- have a trained staff, free from personal or institutional conflicts of interest, that reports directly to the organizational head;
- be protected against retaliation for all activities necessary to carry out the designated institution's mission;
- issue annual public reports on the law's track record, covering results and impacts of whistleblower disclosures;
- assume responsibility to raise public awareness about the law's benefits to enhance societal acceptance of whistleblowing.

Rationale:
This provision establishes the rules for the key agency responsible for the law to make a difference. It is essential in order to ensure:

- an agency with sufficient knowledge, independent authority and resources for credibility and legitimacy with whistleblowers and institutions cited in reports;
- the right to seek protection without the necessity of financing an attorney and court expenses, which often is unrealistic for an unemployed or vulnerable whistleblower;
- an agency with authority to provide timely temporary relief against retaliation during lengthy investigations;
- an agency with authority to act in a timely manner for permanent relief against retaliation, rather than being limited to recommendations;
- access to court for due process if the administrative agency fails to provide timely relief;
- reliable identity protection for whistleblowers who will only make reports if they can remain confidential or anonymous;
- authority to require investigation and action on credible reports, with enfranchisement of the whistleblower as part of independent assessment whether the response was reasonable
- transparency for results of investigation; and
- cultural acceptance reinforced by knowledge of the law's track record and how it is benefiting citizens and families.

Designated office for implementation and oversight of the Act at private entities

Legislative text:
All private entities not exempted from the law also shall have a whistleblower office that assumes the same responsibilities internally to make corresponding recommendations.

Rationale:
The EU Directive requires both public and private entities to have whistleblower offices. While providing equivalent functions and services, the private offices cannot have the authority of law, but can make corrective action recommendations on retaliation and evaluate responses to whistleblowing reports.

Scope of protection
Legislative text:
Retaliation is prohibited against any legal or natural person who is perceived as associated with, about to communicate or communicating protected information, whether the report is to the designated person, to a person within the organization with authority to investigate and act on the issues, to a public institution, to the media, to the public, or to any other channel or outlet permitted under the law.

Rationale:
It takes more than the final messenger to have a responsible whistleblowing disclosure. This is to clarify that all people who participate in the process, and who prepare and communicate protected information that serves the law's objectives, are protected from retaliation. To prevent isolation, it is necessary to equally protect those who are wrongly perceived as whistleblowers. It assures that protection is not limited to communications with internal whistleblower offices, also protecting for those within normal institutional supervisory and oversight channels to detect and act on problems.

Scope of prohibition on retaliation:
Legislative text:
No legal or natural person may recommend, threaten, take or fail to take any action against any that would have a chilling effect on exercise of rights protected by this law, including but not limited to:

a) suspension, lay-off, dismissal or equivalent measures;
b) demotion or withholding of promotion;
c) transfer of duties, change of location of place of work, reduction in wages, change in working hours;
d) withholding of training;
e) a negative performance assessment or employment reference;
f) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;
g) coercion, intimidation, harassment or ostracism;
h) discrimination, disadvantageous or unfair treatment;
i) failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
j) failure to renew, or early termination of, a temporary employment contract;
k) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
l) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;

m) early termination or cancellation of a contract for goods or services;
n) cancellation of a license or permit;
o) psychiatric or medical referrals.

Rationale:
Any remedial law must clearly identify the full scope of misconduct it seeks to address. As a result, the Directive and all best practice laws specifically list the common forms of prohibited retaliation, in additional to an umbrella provision for flexibility against creative new forms of harassment that could intimidate whistleblowers into silence.

Reasonable belief threshold for protection, without good faith or motivation tests

Legislative text:
Protection shall be granted to all covered persons who make an internal or external report, or public disclosure pursuant to this law with a reasonable belief that the information is accurate at the time it is disclosed, including those who report inaccurate information in honest error. A reasonable belief requires a genuine belief in information's accuracy, but a person's motives, intentions, and good faith shall not be considered as relevant factors for protected activity. Those who make knowingly false reports or disclosures are not protected by this law, and are subject to existing liability.

Rationale:
"Good faith" tests commonly are used to deny protection and put the whistleblower's motives on trial, instead of the organization's misconduct or retaliation. All that matters for the law's objectives is whether the information is true. The law's objective is a safe channel for the message, not a positive judgment about the messenger. This standard reflects a fundamental requirement of the European Union Whistleblower Directive -- that protection is based on a genuine belief of information's accuracy, not motives why an employee blows the whistle.

Choice of audience for protected reports and disclosures

Legislative text:
Any legal or natural person covered by this law may file a whistleblowing report protected by the law internally as part of professional duties or to a designated office to internal authorities of the institution; or alternatively as an external report to the designated public agency or a competent authority for the alleged misconduct. A person who makes a public disclosure shall qualify for protection under this law if any of the following conditions are fulfilled:

a) the person first reported internally or externally, but no appropriate action was taken in response to the report within 90 days; or
b) the person has reasonable grounds to believe that:
   (i) the breach may constitute an imminent or manifest danger to the public interest, such as where there is an emergency situation or a risk of irreversible damage; or
   (ii) in the case of external reporting, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the breach or involved in the breach.

Rationale:
For initial reports of misconduct, the EU Directive permits whistleblowers freedom of choice between informal or formal institutional internal channels, and externally to competent authorities. The whistleblower may go directly to the public under the specific circumstances listed in the text.

Burden of proof for violations of the law
Legislative text:
A person filing a retaliation complaint has the burden to prove a prima facie case, which requires that he or she made a report protected by this Act and that the employer subsequently took a prejudicial action. The burden of proof then shifts to the employer to demonstrate that the action taken was not linked in any way to the protected activity.

Rationale:
This is the basic rule for what evidence each side must present to prevail and so is unsurpassed in significance for a whistleblower law's impact. It literally reflects the burdens of proof in the EU Whistleblower Directive. The Directive does not require that the employee demonstrate a causal connection between whistleblowing and alleged retaliation. Rather, once an employee shows he or she made a report and was then subject to detriment, the employer has the reverse burden of proof, which is an ultimate universal standard globally, to prove that an action had independent, innocent causes and that the stated reasons were not a pretext for retaliation.

Comprehensive relief
Legislative text:
Upon finding a violation of a person's rights under this law, the designated external public institution or a court of competent jurisdiction shall order relief to eliminate the direct and indirect effects of the retaliation, with specific authorization to provide:

- interim and injunctive relief pending final action;
- transfer or reassignment, with the employee's consent;
- compensation for any financial prejudice, and for non-financial consequences such as pain and suffering;
- attorney fees and litigation costs;
- medical and emotional treatment for the effects of retaliation;
- education, retraining and other occupational/professional support;
- any other relief the designated agency or court finds appropriate.

An employee may appeal decisions of the designated external agency on the level of relief to a court of competent authority and further appellate review.

Rationale:
This recommendation is for the right to "make whole" relief that neutralizes the direct and indirect effects of retaliation. Without comprehensive compensation, employees may still "lose by winning," which would increase the chilling effect the law seeks to overcome. However, proceedings routinely last for years, during which time an unemployed or

vulnerable whistleblower must pay an attorney. Without interim relief, any eventual victory may be too late to prevent irreparable damage.

Penalties for retaliation and for failure to comply with requirements of the law

Legislative text:

Legal or natural persons that permit, order, threaten, recommend or otherwise participate in retaliation against whistleblowers, or who fail to carry out duties required by the law, shall be subject to sanction by the designated agency or a court of competent jurisdiction. Those authorities may order any employment discipline up to termination, order corrective action and impose fines to the degree necessary to prevent recurring violations of this law. A competent court may impose criminal sanctions for repetitive or egregious violations of the law.

Rationale:

This is to ensure retaliators are held to account for their actions, and to deter individuals and organisations from retaliating against whistleblowers. The EU Directive on whist leblower protection states that criminal, civil or administrative penalties are "necessary" to ensure effective protections, and that these sanctions can "discourage" retaliation.

Training and Information

Legislative text:

All parties that must implement or comply with the law shall provide annual in-person training to their management and staff on the law's purpose, rights and responsibilities. A judicial academy (or equivalent institution) shall conduct the training. Whistleblower laws and procedures shall be posted clearly in workplaces and prominently posted on websites where their provisions apply.

Rationale:

This is to ensure personnel in whistleblower offices have adequate knowledge to implement the law, managers to obey it, and whistleblowers to be aware of their rights and responsibilities under the law. Experience repeatedly has demonstrated that training to be aware of and understand the law is an unsurpassed factor for cultural acceptance, prevention of retaliation, and enforcement of rights when needed.

Transparency of results under the Act

Legislative text:

The designated public institution responsible to implement the law annually shall prominently post on its website for the prior year the number of retaliation complaints filed, with won-loss data on outcomes; the track record for temporary and permanent relief from reprisal complaints including the length of time for decisions and the range of relief; the number of whistleblowing disclosures to the designated public institution; and public benefits from whistleblowing disclosures, with the most significant examples subject to the law's confidentiality restrictions.

Statistics on the public impact from the law shall include:

a. the number of reports received by the competent authorities,
b. the number of investigations and proceedings initiated as a result of such reports and their outcome, and
c. if ascertained, the estimated financial damage, and the amounts recovered following investigations and proceedings, related to the breaches reported.

Rationale:

It is not credible to have a transparency law without transparency about its results, which also reveal successful provisions and those that need revision to achieve the law's objectives. Agencies responsible to promote the law must educate the public on how it has made a positive difference in their lives or been effective against corruption.

Review of laws and policies

Legislative text:

Whistleblower laws and regulations shall be formally reviewed at least every three years, with findings on strengths and weaknesses from the track record and recommendations for improvement. This review shall include an opportunity for comments by key stakeholders, including employee organisations, business/employer associations, civil society organisations and academia.

Rationale:

This is to ensure the whistleblower framework is regularly updated and improved based on lessons learned. Requiring transparency and public comments will enhance social acceptance for the rights, as well as public recognition and use of the law.

3.2. Second Annual Regional Multi-Beneficiary Training on Whistleblower Protection, November 17-18

Day 1, November 17, 2021
A. Executive Summary of ECtHR Case Halet vs. Luxembourg
B. Objectively reviewing employee retaliation complaints
C. Example: Best Practices for Whistleblowers when Working with Congress
D. Example: Working with Whistleblowers Manual
E. Role-playing an interaction with a witness in the workplace
F. Paper on 'The Whistleblower Dilemma: Understanding the Nature, Legal Dimensions and Control of "Information"'

Day 2, November 18, 2021
G. Whistleblowing and public disclosure
H. Hard Wires: The Neuropsychology of Speaking Up
I. Whistleblower Protection as an Antidote for Human Instincts
J. Information Theory for EU Whistleblower Directive

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

Press Release
issued by the Registrar of the Court

ECHR 143 (2021)
11.05.2021

Conviction of a whistleblower who disclosed tax documents: no violation of the Convention

In today's **Chamber** judgment [1] in the case of Halet v. Luxembourg (application no. 21884/18) the European Court of Human Rights held, by a majority (five votes to two), that there had been:

no violation of Article 10 (freedom of expression) of the European Convention on Human Rights

The case concerned Mr Halet's criminal conviction in the "Luxleaks" case for disclosing tax documents concerning some of his employer's clients.

The Luxembourg courts did not accept whistleblowing as justification for Mr Halet's actions, taking the view that the disclosure of the documents, which were subject to professional secrecy, had caused his employer harm – resulting, in particular, from the damage to the firm's reputation and the loss of client confidence in its internal security arrangements – that outweighed the general interest. The Court of Appeal sentenced Mr Halet to a fine of 1,000 euros.

Mr Halet alleged that his conviction amounted to disproportionate interference with his freedom of expression.

In examining the case, the Court considered first of all whether Mr Halet should be regarded as a whistleblower for the purposes of the Court's case-law. Having found this to be the case in principle, it examined the criteria established by the Court's case-law in that regard.

The Court found that, in reaching the conclusion that the documents disclosed by Mr Halet had been of insufficient interest to justify acquitting him, the Court of Appeal had examined the evidence in the case carefully in the light of the criteria established by the Court's case-law.

The Court also observed that the domestic courts had taken into consideration, as a mitigating factor, the "disinterested nature of [Mr Halet's] actions" and had therefore imposed a fairly modest fine. This could reasonably be regarded as a relatively mild penalty that would not have a real chilling effect on the exercise of the applicant's freedom or that of other employees.

In view of the Contracting States' margin of appreciation in this sphere, the Court held that the domestic courts had struck a fair balance in the present case between the need to protect the rights of the applicant's employer on the one hand and the need to protect Mr Halet's freedom of expression on the other.

1. Under Articles 43 and 44 of the Convention, this Chamber judgment is not final. During the three-month period following its delivery, any party may request that the case be referred to the Grand Chamber of the Court. If such a request is made, a panel of five judges considers whether the case deserves further examination. In that event, the Grand Chamber will hear the case and deliver a final judgment. If the referral request is refused, the Chamber judgment will become final on that day.
Once a judgment becomes final, it is transmitted to the Committee of Ministers of the Council of Europe for supervision of its execution. Further information about the execution process can be found here: www.coe.int/t/dghl/monitoring/execution.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Principal facts

The applicant, Raphaël Halet, is a French national who was born in 1976 and lives in Viviers (France).

At the relevant time Mr Halet worked for the firm PricewaterhouseCoopers (PwC), which provides auditing, tax advice and business management services. Its activities include preparing tax returns on behalf of its clients and requesting advance tax rulings from the tax authorities. These rulings, also known as "advance tax agreements", concern the application of tax legislation to future transactions. Between 2012 and 2014 several hundred advance tax rulings and tax returns prepared by PwC were published by various media outlets. The documents published highlighted a practice, spanning a period from 2002 to 2012, of highly advantageous tax agreements between PwC, acting on behalf of multinational companies, and the Luxembourg tax authorities.

An in-house investigation by PwC established that in 2010, as he was about to leave the firm having resigned, an auditor, A.D., had copied 45,000 pages of confidential documents, including 20,000 pages of tax documents corresponding to 538 advance tax rulings. In the summer of 2011 he passed them on to a journalist, E.P., at the latter's request.

A second in-house investigation by PwC revealed that in May 2012, following the disclosure by the media of some of the advance tax rulings copied by A.D., Mr Halet had contacted the journalist E.P. and offered to pass on further documents. Sixteen documents (fourteen tax returns and two accompanying letters) were handed over between October and December 2012. Some of them were used by E.P. in a television programme entitled "Cash Investigation" which was broadcast in June 2013. In November 2014 the documents were also posted online by an association of journalists known as the International Consortium of Investigative Journalists.

Following a complaint by PwC criminal proceedings were instituted, which resulted in A.D. and the journalist E.P. being acquitted. Mr Halet, however, was sentenced on appeal to a criminal fine of 1,000 euros and was ordered to pay a symbolic sum of 1 euro to PwC in compensation for non-pecuniary damage. In its judgment the Court of Appeal found, in particular, that the disclosure of documents subject to professional secrecy had caused the applicant's employer harm that outweighed the general interest. Mr Halet lodged an appeal on points of law which was dismissed in January 2018.

Complaints, procedure and composition of the Court

Relying on Article 10 (freedom of expression), Mr Halet alleged that his conviction after he had disclosed sixteen documents emanating from his employer PwC to a journalist amounted to disproportionate interference with his right to freedom of expression.

The application was lodged with the European Court of Human Rights on 7 May 2018.

The association *Maison des lanceurs d'alerte* was given leave to intervene as a third party.

Judgment was given by a Chamber of seven judges, composed as follows:

Paul **Lemmens** (Belgium), *President*,
Georgios A. **Serghides** (Cyprus),
Georges **Ravarani** (Luxembourg),
María **Elósegui** (Spain),
Darian **Pavli** (Albania),
Anja **Seibert-Fohr** (Germany),
Peeter **Roosma** (Estonia),

and also Milan **Blaško**, *Section Registrar.*

Decision of the Court

Article 10 (freedom of expression)

Reiterating that Article 10 of the Convention extended to the professional sphere, including when the relationship between employer and employee was governed by private law, the Court considered that Mr Halet's conviction amounted to interference for the purposes of Article 10.

The Court also observed that it was not disputed that the interference in question had been "prescribed by law" and had pursued a "legitimate aim", as Mr Halet had been convicted of various offences laid down in the Criminal Code, and the aim in prosecuting and punishing those offences had been to prevent the disclosure of confidential information and protect the reputation of his employer, PwC.

As to whether the interference had been "necessary in a democratic society", the Court considered at the outset that its task was to assess whether this was a whistleblowing case for the purposes of the Court's case-law in which the principles established in *Guja v. Moldova* [2] and *Heinisch v. Germany*[3] were applicable. In that connection it observed, firstly, that there had been a hierarchical bond between the applicant and his employer, PwC, which entailed a duty of loyalty, reserve and discretion on his part. That duty was a particular feature of the concept of whistleblowing for the purposes of the Court's case-law. Secondly, the applicant had contacted a journalist in order to disclose confidential information which he had obtained in the context of his employment relationship. Taking the view that there were parallels between the applicant's actions and those of the applicants in the cases of *Guja* and *Heinisch*, both cited above, the Court found that the applicant should be regarded as a whistleblower for the purposes of the Court's case-law.

The Court went on to examine whether the principles established in *Guja* had been respected. It noted that only the fifth and sixth criteria established by that case-law were at issue in the present case.

Regarding the fifth criterion (the balancing of the public interest in receiving the information against the harm caused to the employer by the disclosures), the Court noted that, in the domestic courts' view, the disclosure by Mr Halet of documents that were subject to professional secrecy had caused harm to PwC – resulting, in particular, from the damage to the firm's reputation and the loss of client confidence in its internal security arrangements – that outweighed the general interest. In balancing the interests at stake, the courts had thus attributed greater weight to the harm suffered by PwC than to the interest of the disclosures made by the applicant.

In the Court's view, it could not be disputed that PwC had suffered harm owing to the very fact of the widely reported controversy arising out of the Luxleaks affair. The press coverage confirmed that the firm had "experienced a difficult year" after the affair had come to light. However – again, according to the media, and this fact had not been disputed – once this initial difficult period had passed, the firm had seen an increase in turnover coupled with a significant rise in staff numbers. Hence, it had to be ascertained whether the damage to its reputation had been real and tangible. The Court concluded that while PwC had undoubtedly suffered harm in the short term, no longer-term damage to its reputation had been established.

The Court went on to examine the reasoning of the domestic courts concerning the interest of the information disclosed by the applicant. In that connection the Court of Appeal had noted that Mr Halet's disclosures had simply related to companies' tax returns which had not revealed anything about the tax authorities' attitude towards those companies. In the Court of Appeal's view, there had been no compelling reason for Mr Halet to disclose the confidential documents in question, at a time when the practice of advance tax rulings had already been uncovered by A.D. The Court of Appeal had specified that, while the documents disclosed by Mr Halet had certainly been of interest to the journalist himself, they had not provided any essential, previously unknown information capable of rekindling or contributing to the debate on tax evasion.

In the Court's view, the Court of Appeal had given detailed reasons for its findings regarding the fifth criterion established by the *Guja* case-law. Accordingly, the Court would require strong reasons to

[2] *Guja v. Moldova* [GC], no. 14277/04, ECHR 2008.
[3] *Heinisch v. Germany*, no. 28274/08, ECHR 2011 (extracts).

substitute its own view for that of the domestic courts. That situation did not apply in the present case, for the following reasons.

The Court of Appeal had assessed the interest of Mr Halet's disclosures with care, examining in depth their content and their repercussions in terms of multinational companies' tax practices. In that context it had acknowledged that the disclosures were of general interest. It had even taken into consideration the impact of the information, accepting that it was liable to "concern and shock people". The Court of Appeal had nevertheless held that the interest of the applicant's disclosures weighed less heavily than the harm suffered by PwC, after finding that those disclosures had been of minor relevance. In reaching that conclusion it observed that the documents had not provided any information that was vital, new or previously unknown. In the Court's view, these three qualifiers – "vital, new and previously unknown" – were encompassed in the Court of Appeal's exhaustive reasoning on the fifth criterion for balancing the private and public interests at stake. In other circumstances these terms might be considered too narrow, but in the present case they had served, together with the other elements taken into account by the Court of Appeal, to found the conclusion that the applicant's disclosures had lacked sufficient interest to counterbalance the harm suffered by PwC.

The Court considered that the Court of Appeal had confined itself to examining the evidence carefully in the light of the criteria established by the Court's case-law, before concluding that the documents disclosed by Mr Halet had not been of sufficient interest to justify acquitting him. In the Court's view, the fact that A.D. had been acquitted after the same criteria based on the Court's case-law had been applied confirmed that the national authorities had carried out a detailed examination in weighing up the relevant interests.

As to the sixth criterion (the proportionality of the penalty), the Court observed that the domestic courts had taken into consideration, as a mitigating factor, the "disinterested nature of the [applicant's] actions" and had therefore imposed a fairly modest fine (1,000 euros). This could reasonably be regarded as a relatively mild penalty that would not have a real chilling effect on the exercise of the applicant's freedom or that of other employees.

In sum, regard being had to the Contracting States' margin of appreciation in this sphere, the Court found that the domestic courts had struck a fair balance in the present case between the need to protect the rights of the applicant's employer on the one hand and the need to protect Mr Halet's freedom of expression on the other. **There had therefore been no violation of Article 10 of the Convention.**

Separate opinion

Judges Lemmens and Pavli expressed a joint dissenting opinion which is annexed to the judgment.

The judgment is available only in French.

Press contacts
During the current health-crisis, journalists can continue to contact the Press unit via echrpress@echr.coe.int

Inci Ertekin
Tracey Turner-Tretz

Denis Lambert
Neil Connolly
Jane Swift

The European Court of Human Rights was set up in Strasbourg by the Council of Europe Member States in 1959 to deal with alleged violations of the 1950 European Convention on Human Rights.

'Whistleblower Disclosure and Protection in Pr actice:
Discussion of Challen ges and Solutions'

Objectively reviewing employee retaliation complaints

Indicate how you would respond if you received the following complaints from employees

(1) A hospital nurse told her manager that some of the medical equipment was not being properly cleaned and could cause hygienic problems with patients. The manager ignored the problem. When the nurse brought up the problem again with the manager, they had an argument and the nurse was fired. The manager wrote in an official document that the nurse was "difficult to manage." The nurse filed a retaliation complaint.

What should the outcome be?
___ The nurse's dismissal was legal and s hould be upheld.
___ The nurse should be reinstated and receive lost wages.

(2) A construction worker told his manager that the roof the company had just finished building at a school was not made from the proper materials and could collapse. The manager told the worker not to worry about it. The worker then told the company's board of directors, and he received a similar response. The school year was going to begin the following week. The worker gave documentation about the problem to a newspaper, which published an article. The worker was fired, and he filed a a retaliation complaint.

What should the outcome be?
___ The construction worker's dismissal was legal and should be upheld.
___ The construction worker had the right to alert the public about the roof problem. He should be reinstated and receive lost wages.

(3) A worker at a beverage company told authorities that the "secret formula" for one the company's most popular soft drinks causes cancer in laboratory animals and could endanger human health. The worker sent the entire "secret formula" to authorities. The company found out about this and fired the worker. She filed a retaliation complaint.

What should the outcome be?
___ The worker's dismissal was legal because she violated employment confidentiality and trade secrecy rules.
___ The worker had the right to tell authorities about the health risks. She should be reinstated and receive lost wages.

(4) An employee at the public tax authority learned that three wealthy people were not paying taxes. The employee told his managers, who told him to stay quiet. The employee told the public prosecutor about the problem, including the names of the wealthy people. The employee was fired, and he filed a retaliation complaint.

What should the outcome be?
___ The employee's dismissal was legal because he violated data privacy rules.
___ The employee should be reinstated and receive lost wages.

(5) A janitor at a large shopping mall told authorities that the chemicals he was using to clean the floors for three years was making people very sick. The janitor is an ex-convict who previously had served several prison sentences for violent crimes. He was fired, and he filed a retaliation complaint.

What should the outcome be?
___ The janitor's dismissal should be upheld because he is a former violent criminal and has no rights.
___ The janitor should be reinstated because he reported a problem that concerned the public interest, and his personal character is not relevant.

(6) For many years, a worker at a cheese factory knew that the company was using toxic chemicals to artificially preserve the cheese. The chemicals are widely known to cause health problems in people. For many years, she was afraid to report the problem because she is a single parent with three children, and she did not want to lose her job. Eventually she found the courage to tell authorities about the chemicals. She was fired, and she filed a retaliation complaint.

What should the outcome be?
___ The worker should not be protected from retaliation because she waited too long to report the problem.
___ The worker should be reinstated and receive lost wages.

Best Practices for Whistleblowers when Working with Congress

The right for public employees to communicate with Congress is established in the First Amendment of the U.S. Constitution. Further, various laws prohibit retaliation against public and private sector whistleblowers for providing information to Congress. However, whistleblowers still take serious risks when contacting Congress. The following best practices incorporate lessons learned from whistleblowers, advocates, attorneys, and congressional staff.

Before you proceed, are you prepared to risk retaliation to report the alleged misconduct?

Incorporate "Whistleblower Survival Tips" (available HERE) to help protect yourself during your whistleblowing process

Consult an experienced whistleblower attorney and consider partnering with whistleblower support organizations to help you safely and effectively work with Congress

Identify the best congressional committee(s) or Member office(s) to communicate your disclosure, based on jurisdiction, history or interest in the topic, track record working with whistleblowers, and a direct connection such as your District Office

Develop ground rules for your working relationship with each congressional office, including confidentiality requests and any limitations around the use of your evidence

Limit your first meeting to a succinct summary with a timeline of key events, and focus on the public consequences of your disclosures

Be clear in your congressional "asks" – whether it is investigating the underlying misconduct and/or helping to shield you from retaliation

Gather as much evidence as you legally and responsibly can, but do not provide documents in your initial outreach to Congress. To limit liability, summarize the underlying disclosure without providing documents barred from release, and make a list or "roadmap" of documents that Congress can request

Do the work of congressional staff whenever possible, such as researching and demystifying documents and ghostwriting questions or communications

Manage expectations, since congressional offices have far more work than bandwidth and they may not be able to respond quickly or pursue all the matters brought to their attention

BEST PRACTICES FOR WORKING WITH WHISTLEBLOWERS MANUAL

PREFACE

Congress plays a critical role in both learning from, and protecting, whistleblowers. Additionally, Congress' constitutionally mandated oversight work very often relies on vital disclosures from government workers and employees within the private sector. For that relationship to succeed, congressional offices need the tools to safely and constructively work with whistleblowers.

The House took an important step at the start of the 116th Congress by establishing a new Office of the Whistleblower Ombudsman. It functions as an independent, nonpartisan support office to advise House offices on best practices for working with whistleblowers from the public and private sectors. In accordance with the House Rules, Sec. 104 (e)(3), the Office has two main responsibilities: [i]

1. Promulgate best practices for whistleblower intake for offices of the House
2. Provide training for offices of the House on whistleblower intake, including establishing an effective reporting system for whistleblowers, maintaining whistleblower confidentiality, advising staff of relevant laws and policies, and protecting information provided by whistleblowers

The Office does not have the authority to receive whistleblower disclosures. However, it can provide indirect support through generic resources for whistleblowers on its public website and by guiding House offices.

This Manual will cover best practices for working with whistleblowers. It is divided into four modules:

Module 1: Managing Relationships with Whistleblowers
Module 2: Establishing an Effective Case Management System
Module 3: Protecting Whistleblower Information
Module 4: Navigating the Legal Landscape

These guidelines can be institutionalized throughout the House to establish consistent, safe, and effective practices for working with whistleblowers. They can be integrated into existing office practices or used to develop new procedures. This Manual incorporates guidance developed by the Government Accountability Office, consultation with House support offices, as well as common practices and lessons learned by congressional oversight committees, Member offices, and whistleblower rights groups.[ii]

This Manual is available at the Office's website, https://whistleblower.house.gov. Please contact the Office with related questions or for additional information on working with whistleblowers at 202.226.6638 or WhistleblowerOffice@mail.house.gov.

Warm regards,

Shanna Devine
Director

Table of Contents

Module 1: Managing Relationships with Whistleblowers

This module will explore who whistleblowers are, as well as key principles that provide the foundation for an effective working relationship, and best practices or "survival tips" for employees to consider when blowing the whistle.

Who are Whistleblowers?

In broad and nonlegal terms, a whistleblower is an individual who discloses evidence of wrongdoing that threatens the public interest. If an employee challenges an action that solely they are impacted by, it may not be considered whistleblowing. However, there are many circumstances where what is good for the individual is also good for the public. For instance, a nurse may challenge a requirement to work without proper protective equipment, due to fear of getting sick. However, he is acting in the public interest, since working under those conditions could also harm patients and the public. Notably, an individual's self-interest and motive do not disqualify them from coverage under whistleblower laws.

However, beyond generally contributing to the public interest, an individual must engage in lawful – also known as protected – whistleblowing activity to be eligible for legal protections.

The primary laws for federal employees and contractors define a whistleblower as a current employee, former employee, or applicant who discloses information that he or she reasonably believes evidences:

A violation of law, rule or regulation;
Gross mismanagement;
A gross waste of funds;
Abuse of authority; or
A substantial and specific danger to public health or safety.

Note that a whistleblower does not need to prove the wrongdoing. They merely need to provide a *reasonable belief* that the misconduct occurred. Further, contrary to popular belief, an individual who discloses evidence of wrongdoing does not need to experience retaliation to meet the legal definition of a whistleblower. Further, private sector laws apply the principle of this definition in different contexts.

Employees may disclose misconduct that does not meet the legal definition of whistleblowing, but that is still of value and in the interest of Congress. For matters of *public concern*, federal employees still have a constitutional right to communicate with Congress. However, due to a lack of clear free speech boundaries, it is more difficult for an employee to enforce their rights under the First Amendment than under most whistleblower statutes, as explored further in Module 4: Navigating the Legal Landscape.

As an alternative to the term "whistleblower," some individuals may better identify with the term "truth-teller", "watchdog", or "taxpayer protector" for instance. However, most wh istleblowers simply perceive themselves as committed employees performing their jobs. Many feel an obligation to report misconduct out of a sense of loyalty to the organizational mission. In fact, the Standards of Ethical Conduct requires executive branch employees to "disclose waste, fraud, abuse, and corruption to

appropriate authorities."[iii] Further, the Code of Ethics for Government Service requires all government employees to "[e]xpose corruption wherever discovered."[iv] As will be discussed, whistleblower laws cover employees disclosing information as part of their job duties. Still, notwithstanding legal rights, whistleblowing often comes at a significant professional and personal cost.

Whistleblowers are often trying to sort out a critical life's choice and how to make a difference by reaching out to Congress. It helps to understand the frame of mind that many whistleblowers are in by the time they contact your office. They are likely at a professional crossroad, in a vulnerable position dealing with threats and pressures that they had not anticipated. They may feel betrayed by the very institutions that they have been loyal to and are coping with significant psychological stress. Reprisal tactics frequently range from professional isolation, to blacklisting and even public smear campaigns.

Working effectively with whistleblowers is not just an altruistic undertaking, however. Congress' constitutionally mandated oversight work relies on these courageous employees. Whether a whistleblower is sounding the alarm around waste, fraud, abuse, or threats to public health and safety, helping navigate through bureaucratic mazes to find the evidentiary needle in the haystack, or calling the bluff on false answers, throughout history they have been Congress' eyes and ears to wrongdoing.

There are countless ways in which whistleblowers can be key oversight partners. To play that role, they need to believe it is worthwhile and safe to communicate with Congress.

Research has found that the primary reasons would-be whistleblowers do not come forward are

1) Fear of futility, that their whistleblowing will not make a difference
2) Fear of retaliation for engaging in whistleblowing

With the right tools, whistleblowers can be one of your most valuable resources, and you can help them to have an impact while prioritizing their protection. Once you decide to work with a whistleblower, the key to an effective partnership is earned trust.

Principles for Working with Whistleblowers

The following guiding principles provide the foundation for earned trust and a constructive working relationship. Many are applicable at the screening or intake stage, even if you do not pursue a case.

First rule of thumb: do no harm: Whistleblowers are often in a vulnerable position, and many are making the most difficult decision of their career that will have severe professional and personal consequences. While ideally a whistleblower will be better off due to contacting your office, at minimum it is important that they are not in a worse position. The subsequent principles and this Manual provide the tools to help achieve this goal.

Do not provide legal advice: While you can and should provide guidance to a whistleblower on the process of whistleblowing (including the "survival tips" discussed below), you should make clear you are not doing so as their legal counsel. Rather, the whistleblower should obtain an attorney with expertise in this area of law and consider partnering with organizations experienced in working with

whistleblowers. A broader support network will help the whistleblower to navigate the difficult road ahead more smoothly and may reinforce their ability to work safely and effectively with your office.

Establish ground rules early: From the beginning, work together to develop ground rules for the agreed terms you and the whistleblower will follow around the use of their information. Even if they do not want to remain confidential, discuss with the whistleblower how their information may be used and any boundaries that they may want to put in place. This topic is explored further in Module 3: Protecting Whistleblower Information.

Manage expectations and communicate limitations: In order to manage expectations, clearly communicate any limitations around what the office can do, including realistic timelines for follow-through, and make sure not to overpromise if you are not sure you can deliver on something. Then, when the office can provide support – at whatever level, even if simply a referral – the whistleblower is more likely to feel appreciation rather than let down.

Honor all commitments: Follow through on any commitments that you make, in a timely manner to the extent possible. This will help to engender trust and confidence in your office and will ultimately foster a more meaningful exchange.

Engage in structured active listening: As a congressional office, you need to have control of the conversation and get the record right. But remember that whistleblowers are more likely to open up if they feel heard and not rushed. Use key questions to guide the conversation, then summarize their responses to ensure you understand the facts correctly. Provide the whistleblower an opportunity to review the record for quality control before putting it to use.

Enfranchise whistleblowers in the larger context: As the experts in the issues they are bringing to your attention, whistleblowers can be indispensable oversight partners. If their facts check out and your office decides to use their information, enfranchise the whistleblower in the larger context. For instance, ask their opinion and brainstorm around policy solutions, hearing questions or other corrective actions to address the misconduct they have exposed. They can provide a roadmap for document requests, demystify obscure concepts, and help you use the correct terminology.

Network to expand the scope of witnesses: Once trust is established, network with the whistleblower to expand the scope of witnesses through their colleagues or other contacts who can corroborate their allegations. This can expand your body of evidence and increase the credibility of your source. It is far easier for an employer to discredit one or two employees than multiple witnesses who have substantiated the same concerns identified by the "pioneer" whistleblower.

Sustain the relationship: After you have obtained the initial information of interest, follow-up with the whistleblower and prioritize their protection. Check in periodically for developments, such as whether the misconduct has been resolved within their workplace and whether subsequent reprisal has occurred. This will help to sustain the flow of information and keep your office on their radar for future oversight matters. For suggested actions, refer to Appendix B: Follow-Up Checklist.

Advise whistleblower on "survival tips": Discuss with the whistleblower best practices, or "survival tips" to consider before and throughout their whistleblowing journey. If your office does nothing else, providing these valuable lessons learned will still help to ensure the whistleblower is better off for having contacted your office. Some of these tips overlap with the aforementioned principles.

Whistleblower Survival Tips

Whistleblowers can take key steps that may make the difference between a career -ending decision or protecting themselves while having an impact. The following tips were developed by attorneys and advocates who have worked with thousands of whistleblowers to provide valuable lessons learned.

Seek legal and other expert advice early: Before you make a disclosure (or early in your process before taking risks), consider consulting an attorney experienced in representing whistleblowers. This can help to protect your communications through the attorney-client privilege and help to shield you from legal liability. Also consider contacting an organization that specializes in working with whistleblowers, to help guide you through the process and provide solidarity and support. They can potentially serve as a bridge between you those who should be benefiting from your knowledge.

Consult your loved ones: Blowing the whistle may be one of your most difficult professional decisions, and it can have long-lasting personal impacts for you and your loved ones. You could become blacklisted from your industry, subjected to public smear campaigns, and undergo severe psychological trauma. It is important to have a personal support network in place. To the extent possible, discuss the decision with your family in advance, including the risks and benefits of reporting the misconduct, as well as your options for how to safely proceed. They also must live with the consequences and may well resent a *fait accompli*. Putting aside the professional and public stakes, it is an intensely personal decision.

Make a plan: Develop a well-thought-out strategy for your whistleblowing process that incorporates these survival tips, so that you remain at least one step ahead of those engaging in the misconduct. Include exactly what you plan to accomplish (your goals) and how. Consider how your employer will respond before they do, and plan accordingly (e.g. securing evidence before it is destroyed). Identify the applicable law(s) in advance to ensure you are engaging in protected whistleblowing. The plan will likely need to be adjusted throughout your journey, but it will provide a roadmap to guide you.

Carefully weigh the options of being anonymous/confidential versus public: There are risks and benefits to being anonymous, confidential or public during your whistleblowing. For instance, if you remain anonymous, the recipient of your disclosure cannot follow up to discuss how to use the information. If you remain confidential, it may be more difficult to demonstrate that your employer knew about your whistleblowing, which can help to prove retaliation. Yet, going public may expose you to professional isolation, public scrutiny, and even threats to your safety. This is a personal decision that you should discuss in advance with your attorney and support network. However, be aware that it is not possible for a congressional office or other recipients of your disclosures to guarantee confidentiality, due to legal limitations, potential surveillance, and the reality that your facts may be your signature. Always be prepared for the possibility of becoming public.

Work within your workplace for as long as possible without incurring suspicions: Working within your workplace for as long as possible without incurring suspicions will help you to maintain access to key evidence to confirm suspicious and further build your case. Moreover, it may provide an opportunity for the matter to be resolved internally before it escalates further or requires outside intervention. A few exceptions exist to this approach, such as if you have reason to believe doing so could put you or others in harm's way and/or result in the destruction of evidence.

Stick to the facts and don't embellish: Your greatest strength and ultimately key to solidarity is credibility. When making a disclosure, stick to information that you know to be sound and reliable, whether you obtained it firsthand or from a credible source. If in doubt, understate rather than risk exaggerating. Embellishing or straying from the facts will likely come back to bite you later down the road and undermine your credibility, severing trust with key allies, such as congressional offices, advocacy groups or journalists relying on your information.

Create a contemporaneous paper trail or journal: Document key facts and developments surrounding your whistleblowing through a paper trail and/or journal, in order to maintain an accurate record and timeline of events as they unfold. This will help you to share a consistent narrative with those who should be benefiting from your dissent. At the top of the notes, provide a disclaimer that "I have made these notes to refresh my recollection later," which can help prevent them from being used during the discovery process in a related legal proceeding.

Carefully secure and protect evidence before drawing suspicion: Secure and protect evidence before drawing suspicion to your whistleblowing, since the employer may take action to destroy it or block your access. However, proceed cautiously when gathering supporting evidence. Keep it in a secure location, such as with your attorney, and avoid removing original documents when possible (e.g. take a photo from your personal phone instead). Employers regularly conduct retaliatory investigations to identify the whistleblower, tracing metadata or other identifying information back to the original source. Even when you are engaging in lawful whistleblowing, employers have found methods to bypass workplace rights. They may threaten criminal prosecution for "theft" of company documents, or file SLAPP suits – defamation or breach of contract lawsuits for significant damages.

Engage in whistleblowing on your own time, with your own resources: Unless you have advance permission (e.g. via a collective bargaining agreement), engage in whistleblowing on your own time, and from your own resources (e.g. phone, computer, email). Remember that your work email and anything done through your work devices can be monitored by your employer. Due to advanced surveillance techniques, however, communication through your personal devices may also not be secure. When possible, meet in person or use secure communication platforms (e.g. Tor, SecureDrop, Signal) to engage in confidential whistleblowing. Contact an organization experienced in secure whistleblower communications for further guidance.

Test the waters with trusted colleagues: Test the waters with trusted colleagues in order to confirm your concerns and identify potential solidarity. This is a first principle both for quality control, and to test the waters for support that may be essential. However, avoid exposing yourself by engaging in strategic but casual questioning. Take note of potential allies and witnesses, since their support could help to further advance your disclosures and provide a barrier to subsequent retaliation.

Engage in self-care: Practice self-care and stress-reducing activities throughout your whistleblowing process. It is common to experience toxic forms of retaliation – from professional isolation to gaslighting (manipulating someone by psychological means into questioning their own sanity) – which can lead to post-traumatic stress disorder, depression, or even thoughts of harm. Engage in mindfulness activities, and develop a community of support through trusted peers, loved ones, and therapists. The National Suicide Prevention Lifeline offers free and confidential support for people in distress at 1-800-273-8255.

Module 2: Establishing an Effective Case Management System

This module provides four primary steps to follow when receiving, vetting, and acting on information from whistleblowers: Intake, Prioritization, Referral, and Follow-Up. Each step is organized by key practices for – 1) internal office procedures, and 2) external communications with the whistleblower. The composite of these steps is referred to as the case management system. Whether or not you decide to work with a whistleblower beyond the initial intake or screening stage, these guiding principles can have a positive impact throughout the whistleblowing process. Module 3: Protecting Whistleblower Information will expound on security measures identified in the case management process.

Intake

Intake is the initial communication with the whistleblower. It is used to – 1) gather key information for screening disclosures, and 2) create the structure for a potential working relationship.

The primary methods for receiving initial information from a whistleblower include –

Web-Based Forms: Web-based forms enable an office to have better control of what information is submitted, allowing for a more consistent initial intake process.
Email: Email can consist of a designated generic email address that is monitored daily. Unlike a web-based form, there is little control over what information is provided by email. Whistleblowers can also easily transmit supporting documents through email.
Hotline or Tipline: A hotline or tipline can consist of a designated phone number that is monitored daily. If it is answered in real-time, confirm that the whistleblower is communicating from a personal device in a secure location. If needed, schedule a separate time to conduct the intake. If the hotline includes a voicemail, it should specify how frequently the voicemail is monitored.
In-Person: Some whistleblowers may only be comfortable speaking in person, in which case identify a mutually agreeable time and location (preferably private) to conduct the intake.

Each method for intake should be accompanied by key disclaimers as applicable, including but not limited to 1) the laws that establish the right for whistleblowers to communicate with Congress, 2) your office's jurisdiction (most applicable to committees), 3) legal requirements for the disclosure of classified information, and 4) your office's practices regarding confidentiality.

Be aware that some of the most significant disclosures start with a cold call. Have guidance in place to help the front office identify whistleblower inquiries and share them with the designated staff.

See **Appendix A**: Model Intake Form, for an example form that can be incorporated into the intakes conducted through web-based forms, hotlines, or in-person. It can also be used for any follow-up to email submissions.

Whichever method a whistleblower uses initially to submit information, it will likely require additional correspondence to obtain a complete understanding. For instance, in the initial communication, a whistleblower may put out "feelers" with small amounts of information about the alleged misconduct,

in order to gauge an office's interest before providing a more complete picture of the alleged wrongdoing. Conversely, the whistleblower may provide more material than any one staffer can reasonably process.

Whether you are trying to obtain additional information or narrow it down, follow-up communication with the whistleblower by phone or in-person can help you to pin down key facts and gauge the credibility of the allegations. You can also start to build a rapport that will lead to a more meaningful working-relationship if the office decides to pursue the case. During the intake step, develop groun d rules up front for your office's use of the whistleblower's information, and provide transparency into your process, such as any jurisdictional or time limitations you may have, to help manage expectations.

A note of caution: As a rule, whistleblowers are bringing forward information that needs to be handled with caution. The first step is to get a summary of the underlying issue the whistleblower wants to disclose and how they learned about it. Ask follow-up questions to help verify their allegations, including how you can *safely* obtain supporting evidence (see Module 3: Protecting Whistleblower Information). Be aware that *providing classified documents through unauthorized channels and to unauthorized recipients could result in criminal prosecution. Only congressional staff with appropriate clearances should receive classified information.* [v] Further, due to gaps in legal rights (see Module 4: Navigating the Legal Landscape), the whistleblower could still be subjected to civil or criminal liability for sharing evidence that your office is legally authorized to receive (e.g. an employer may claim "theft" of their documents), and by association you could get swept into that legal nightmare. It is prudent for both you and the whistleblower to consult your respective counsel before sharing documentation restricted from public release. As Module 3 explores, there may be alternative, safe methods to communicate and v erify the underlying disclosure.

The following guidelines can be used to develop or inform your office's intake process:

<u>Internal Office Procedures</u>

- Develop written processes and guidelines for your office, including:
  - The office's available method(s) for receiving intakes (e.g. web-based forms, hotline)
  - Safe methods for verifying allegations (e.g. ask whistleblower for guidance around a document request, supporting witnesses, other investigations into their disclosures, secure communications)
  - Protocols to keep disclosures secure
    - Designate staff to work with whistleblowers trained in best practices
    - Ensure personally identifiable information (PII) is handled appropriately[vi]
    - Ensure sensitive or classified information is handled lawfully[vii]
    - Require use of a secure tracking system
- Develop a secure tracking system for whistleblower communications[viii]
  - House it in a secure environment within the office
  - Limit access to designated staff, and on need-to-know basis
  - Document whistleblower inquires in a secure tracking sheet or form

After initial intake, create a separate case file for each whistleblower with key information that can be updated as needed to reflect the case status, referrals, follow-up, and other relevant notes

- Routinely evaluate trends and risks to ensure you are using the most up to date and secure technology available to the House and have adequate safeguards[ix]

External Communications with the Whistleblower

- Apply "Principles to Working with Whistleblowers" to protect the office and build a good rapport (e.g. don't provide legal advice, structured active listening)
- Explain the office's entire process to provide transparency and manage expectations
  - How office decides whether to pursue a disclosure (e.g. jurisdiction, systemic impact)
  - Information office can/cannot receive (e.g. classified), and how it may be used
  - Abilities of office to provide support, without overpromising (e.g. "Due to limited bandwidth we may not be able to pursue your case, but we may be able to provide referrals and inform you of relevant laws")
  - Timelines and potential outcomes
- Ask whistleblower key questions to develop the intake record (see Appendix A for full list):
  - Do you have lawyer, and do you prefer we communicate through your lawyer?
  - What is your employment status and position, and who is your employer?
  - Describe the issue you want to disclose and your goals in working with Congress?
  - How did you obtain this information, and are there legal limitations around its release?
  - Have you filed your disclosure elsewhere? If so, where, and what is the status of any related investigation?
  - Are you a constituent of this Member; have you contacted other offices?
- Establish ground rules for use of whistleblower's information (see Module 3 for full list)
  - Discuss whether whistleblower wants to be a confidential or public source
  - Share the office's confidentiality practices, but be transparent about limitations
  - Discuss boundaries around use of information, and obtain consent before sharing
  - Before acting on information, have whistleblower review for accuracy and to screen for identifiable information

Prioritization

The office can develop guidelines and procedures to help determine whether it will pursue a whistleblower disclosure. It likely will not have the capacity or jurisdiction to work on all the whistleblower intakes it receives. It will also need to distinguish between whistleblowing matters and non-whistleblowing matters. For instance, an employee may use the office's intake process to report an individual benefits issue that is unrelated to retaliation for reporting misconduct. Whatever the determination, be transparent with the intake about how the decision was made and in as timely a manner as practical, so that they are not left in the dark.

If you decide not to pursue a case, it is still important to conclude on good terms when possible, both for the whistleblower's morale and the interest of the office. For instance, later developments may cause you to want to reopen or reprioritize a case. Further, the whistleblower is more likely to refer subsequent supporting whistleblowers to you if they feel they have been treated with respect. Even if your relationship ends after the initial intake stage, there are simple but significant measures you can take to ensure the whistleblower is better off for having contacted your office. The final two steps, Referral and Follow-Up, provide related guidance.

The following guidelines can be used to develop or inform your office's prioritization process:

Internal Office Procedures

- Develop written guidelines on the office's priorities, to help determine if a disclosure will be handled in the office and/or referred
    - Is it a whistleblowing matter, or was the reprisal action triggered by whistleblowing?
    - Is it a matter within office's jurisdiction and/or priorities?
    - Is it an urgent issue, such as national security threat or danger to public health?
    - Does it concern systemic breakdowns within the public or private sectors?
    - Is the whistleblower a constituent?
- Document the prioritization determination within the office's secure tracking system

External Communication with the Whistleblower

- Clearly communicate with the whistleblower about the types of disclosures the office will pursue, and explain how the office cannot pursue all disclosures
- Discuss updated timelines for follow-up, as applicable
- Even if the office does not pursue the disclosure, try to end on good terms (e.g. share referral options, "survival tips")

Referral

Whistleblower cases are often complex and can be difficult to navigate. They can also be time-consuming and require a multifaceted approach to achieve the desired results for the office and the whistleblower. The saying, "it takes a village" can be aptly applied when working with whistleblowers. While congressional partnerships provide a vital lifeline for whistleblowers, you are not expected to be their sole outlet or source of support. Taking on that responsibility can be overwhelming and unrealistic, potentially leading to unreasonable expectations for your office and the whistleblower. Further, making a referral does not mean that your working relationship needs to end, although it can provide helpful closure if that is what is desired.

Referrals provide an opportunity to matchmake the whistleblower with additional sources who should be – 1) benefiting from their knowledge and/or 2) in a position to assist them further during their whistleblowing process.

During the referral process, you can suggest different options for the whistleblower to consider. They can range from internal referrals (e.g. congressional committees of jurisdiction, or personal offices, including district offices) to external referrals (e.g. federal whistleblower agencies, advocacy groups).

In addition to Congress, key government entities are authorized to receive whistleblower disclosures and/or address retaliation. Common referral options are provided in this section, with a focus on resources for executive branch whistleblowers.

See **Appendix B**: Referral Tip-Sheet for a more complete list of the available government entities and their jurisdiction.

Further, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and the federal whistleblower agency Office of Special Counsel have developed an interactive online tool to ensure that whistleblowers are informed of the avenues available to them to report wrongdoing, and also the correct venue to file a complaint to address any retaliation that may occur after reporting wrongdoing.[x]

Note that these are not exhaustive referral lists, and several internal agency whistleblower offices exist, such as the Department of Veterans Affairs' Office of Accountability and Whistlebl ower Protection or the Federal Aviation Administration's Office of Audit and Evaluation. However, congressional hearings and related oversight demonstrate how internal offices have often been the source of conflict or have poor track records in handling whistleblower disclosures. While it is important to be aware of available options, be on guard that some may be higher risk for the whistleblower.

Report Waste, Fraud, Abuse or other Misconduct

Supervisors and Management: Under most public and private sector whistleblower laws, employees are protected against retaliation when they make an internal disclosure to supervisors and management. In fact, studies have found that most employees first report their concerns through internal channels. However, whistleblowers may, rightfully so, be hesitant of this option due to fears of an adverse employment action in response to their disclosure.

Offices of Inspectors General (OIG): OIGs are independent offices within executive branch agencies that can investigate potential waste, fraud, abuse, and other misconduct in their agencies, reported by federal employees or contractors. A limitation is OIGs can only issue recommendations to agency heads for corrective action. The Inspector General Act of 1978 (IG Act) requires Inspectors General (IGs) and their staff maintain whistleblower confidentiality "unless otherwise unavoidable." However, the confidentiality provision is not defined a nd there is no statutory remedy for enforcement. Further, only OIGs are bound to the IG Act's confidentiality requirement, and there have been instances when OIGs have, intentionally or unintentionally, unlawfully disclosed the identity of confidential witnesses.

Office of Special Counsel (OSC): OSC is an independent agency that provides a secure channel for disclosing and resolving wrongdoing in federal agencies. Under the Whistleblower Protection Act, the primary whistleblower law for most federal employees, OSC is required to maintain confidentiality if requested by the employee, unless it is necessary to disclose the identity because of an "imminent danger to public health or safety or imminent violation of any criminal

law." OSC will screen the whistleblower disclosure, and if it determines a "substantial likelihood" that alleged wrongdoing occurred, it can order and oversee an agency investigation into the misconduct. OSC shares the final agency report and recommendations, along with the whistleblower's comments and its own evaluation, with leadership of the congressional committees of jurisdiction and the President. It also publicly posts those results on its website. In addition to its whistleblower-related mandates, OSC enforces the Hatch Act provisions on political activity by government employees, and it helps to enforce the Uniformed Services Employment and Reemployment Rights Act (USERRA).

Report Retaliation

Offices of Inspectors General: The OIG will investigate alleged retaliation or refer it to a relevant agency, such as OSC. In addition, various OIGs are responsible for enforcing whistleblower protections for employees in the Intelligence Community, FBI, Military Services, as well as government contractors, subcontractors and grantees. They also investigate security clearance reprisals. Akin to findings of agency misconduct, OIGs can issue recommendations to agency heads for corrective action if they find retaliation. Most IGs are required to designate a Whistleblower Protection Coordinator to educate agency employees about whistleblower protections for protected activity. These individuals are potential contacts for your office if you want to identify a designated agency whistleblower contact.

Office of Special Counsel: OSC has jurisdiction to investigate claims of retaliation by most federal employees – including current federal employees, applicants, and former employees. If OSC finds that an agency engaged in reprisal, it can seek a "stay" or temporary hold on the retaliatory action, corrective action, and disciplinary action for the retaliator. OSC also provides a highly effective mediation option to resolve disputes.

Merit Systems Protection Board (MSPB): The MSPB is an independent federal agency that considers certain allegations from federal employees who believe they have experienced retaliation for engaging in protected whistleblowing. If OSC does not pursue an employee's retaliation claim after 120 days, the individual can request an Individual Right of Action hearing with the MSPB. An employee who has experienced severe retaliation, such as demotion or termination, can bypass the OSC process and go directly to the MSPB to exercise its administrative due process rights. MSPB cases receive a hearing before an administrative judge, and a written decision that can be appealed to the full Board and to the relevant U.S. Court of Appeals. However, since 2017 the full Board has been without a quorum and is unable to take final administrative action on appeals.

Department of Labor's Whistleblower Protection Program: The Department of Labor's Whistleblower Protection Program, housed within the Occupational Safety and Health Administration, enforces most private-sector whistleblower retaliation claims. The 23 laws under its jurisdiction protect employees who report violations of workplace health and safety, transportation, consumer product, environmental, financial reform, food safety, health insurance reform, motor vehicle safety, nuclear, pipeline, public transportation agency, railroad, maritime, and securities laws. Some of the environmental laws under its jurisdiction also cover federal, state, and local employees.

The following guidelines can be used to develop or inform your office's referral process:

Internal Office Procedures

- Develop a "tip sheet" that provides easily accessible information for the office on the different options for whistleblowers, including the relevance, advantages, and implications of each option (see Appendix B)
- Document where and when a disclosure was referred and/or an action was taken within the office's secure tracking system

External Communication with the Whistleblower

- Consider additional questions at this stage to inform the referral process, including any developments since the initial intake (e.g. have goals changed, subsequent retaliation, contacted other offices?)
- Share relevant referral options with the whistleblower, including actions the office is considering, and discuss potential risks and benefits
- Incorporate ground rules for use of information
  - Request permission before sharing the disclosure outside of your office
  - Provide the whistleblower the opportunity to discuss and/or review potential communications around their information so that they can ensure it is accurate and maintains their confidentiality to the extent desired

Follow-Up

It is useful to develop a follow-up strategy to sustain the flow of information between you and the whistleblower. This includes keeping the whistleblower informed of the status of their disclosure within your office, including any actions you have taken or are considering. Likewise, the whistleblower can keep you current on case developments, including new evidence or retaliatory actions, and apply their expertise to support your office's oversight and investigative work. The follow-up process can also help to manage expectations, by communicating realistic timelines that you can deliver on, and any opportunities or limitations to pursuing their case further.

See **Appendix C**: Follow-Up Checklist for a list of suggested follow-up actions.

See **Appendix D**: Sample Letter for Employer for guidance on sending a retaliation "warning" letter. [xi]

The following guidelines can be used to develop or inform your office's follow-up process:

Internal Office Procedures

- Develop written procedures with clear expectations for follow-up practices
  - Designated contact or other form of internal accountability to ensure follow-up
  - Appropriate timelines for completing follow-up
  - Checklist of potential follow-up actions
  - Document actions taken within office's secure tracking mechanism

External Communication with the Whistleblower

- Communicate when the whistleblower should expect to hear follow-up and ensure the communication occurs, even if the office chooses not to act on the disclosure

- Check-in as appropriate to share respective developments, actions taken and responses
  - Was the disclosure referred?
  - Was the issue resolved by their employer?
  - Have they experienced delayed retaliation?
- Ask for whistleblower's expertise in the larger context
  - Provide roadmap for document requests
  - Demystify obscure concepts and identify correct terminology
  - Matchmake you with additional witnesses to expand investigative record
  - Brainstorm around policy solutions and hearing questions
- Discuss additional actions to support whistleblower and advance oversight work (see Appendix C for full list)
  - Send "warning letter" that it is illegal to retaliate against a congressional witness[xii]
  - Open or request investigation into alleged wrongdoing
  - Explore legislative solutions to address systemic threats exposed by disclosure

Module 3: Protecting Whistleblower Information

This module will explore key practices to maintain confidentiality and guidelines around information security. These measures are intended to protect the whistleblower's information, as well as the security of Congress' investigative and oversight work.

Confidentiality

When a whistleblower contacts your office, discuss the level of anonymity they want to keep. This can range from sharing information on background for your informational awareness, to establishing boundaries for use of their evidence and remaining a confidential source, to not placing any restrictions around the use of their information and working with you as a public witness. Check-in with your source periodically about their desired level of confidentiality; developments with their whistleblowing may cause them to want to tighten or loosen restrictions around the use of their information.

To the extent the whistleblower wants to remain confidential, inform them of your office's commitment to protect their identify to the extent possible and the measures that you will take to do so. At the same time, be careful not to overpromise the level of confidentiality that you can guarantee and manage expectations around what is and is not within your control, as this section will explore further. For instance, once their information leaves your office, without obtaining advance commitments you can no longer place safeguards around its use.

If a whistleblower contacts your office anonymously and without any method to respond, you should still exercise extreme caution when working with their information through the applicable practices outlined in this module.

This section will identify key factors to consider when maintaining a whistleblower's confidentiality, including risks and benefits to being confidential verses public, common pitfalls made by congressional offices, and ground rules around the use of the whistleblower's information.

Confidential versus Public

The whistleblower's decision to work with your office in a confidential or public capacity is a personal choice, largely based on how much risk they are willing to take. They will ideal ly make the determination through talks with their lawyer and loved ones. Key factors they may consider are summarized below.

Confidential

- **Benefit**: The longer a whistleblower remains confidential, the more likely they are to have access to key evidence and to sustain the flow of information to your office.
- **Benefit and Risk**: Federal whistleblowers are entitled under certain laws to remain confidential, including the IG Act and the Whistleblower Protection Act. However, application is limited to OIGs and the Office of Special Counsel. Further, they do not have legal remedies to enforce confidentiality under those and other witness protection laws.
- **Benefit and Risk**: Due to technological advances, whistleblowers are more at risk of surveillance or having their evidence traced back to them. The flip side of technology is that it can also help to secure communications between the whistleblower and your office.

Public

- **Benefit**: In some circumstances, in may be safer for the whistleblower to go public. When a whistleblower is in the "grey area" – meaning their employer may already suspect they are making a disclosure – going public can provide an additional layer of protection. It provides an opportunity for solidarity from everyone who should be benefiting from the whistleblower's dissent (e.g. public, media) and who may be able to help shield the whistleblower from retaliation. Further, under whistleblower protection laws, in o rder to establish that a personnel action is retaliatory, the employee must demonstrate that the employer had *knowledge* ("knew of should have known") of their whistleblowing activity. While public whistleblowing is not necessary to prove knowledge, it is easier to do so.
- **Risk:** If the whistleblower becomes public, willingly or unwillingly, they should be prepared for a public smear campaign by their employer in an attempt discredit them and distract from the misconduct they are bringing to light. To undermine the whistleblower's credibility, the retaliator may make false accusations or expose skeletons in their closet. The act of being public could result in blacklisting and other forms of professional and social isolation. The whistleblower will need to have thick skin and may even need to take security precautions to protect their and their family's safety.
- **Risk:** Due to gaps in whistleblower rights, a known whistleblower could become the target of criminal or civil retaliation (e.g. criminal investigation, defamation suit) for providing information to Congress, even if the individual is engaging in lawful whistleblowing for which employment retaliation would be illegal.

Common "Pitfalls"

Remember that whistleblowers' facts are often their signature. An office must be careful not to reveal them through the information it uses. Common "pitfalls" that can lead to inadvertently disclosing the identity of a confidential source include:

Receiving documents that include identifying information or are sent through an unsecured system and can be traced back to the whistleblower
Sending a whistleblower's complaint back to the agency with related questions (e.g. to confirm credibility of disclosure, to investigate further), without removing PII or information that only the whistleblower or a small number of people have access to
Sharing a whistleblower's case without any limitations with another congressional office, which may use the information in a manner that discloses their identity
Discussing the whistleblower's evidence in a congressional hearing or publicizing it without first working with the whistleblower to prevent exposure of any identifying information
Storing a whistleblower's information in an unsecure location and without adequate safeguards

Develop Ground Rules

During the intake process, establish ground rules with the whistleblower around the use of their information. The ground rules can be revised to address developments, such as a whistleblower becoming public. Best practices for intake ground rules include:

Establish if the whistleblower wants to be confidential or public, and honor their choice
Establish the extent to which the whistleblower is comfortable having their disclosure shared, and any boundaries around its use
Obtain the whistleblower's consent before sharing their information internally (e.g. to another congressional office or in a closed-door hearing) or externally (e.g. the whistleblower's employer, a nonprofit organization, or publicly)
Work with the whistleblower to screen information for PII and metadata (e.g. track changes, photo location) before it is shared
Communicate through a whistleblower's attorney whenever possible instead of the whistleblower, to invoke the client-attorney privilege
Identity alternative channels to obtain a whistleblower's evidence (e.g. direct requests to the employer for documentation – while being careful not to provide a level of specificity that could be traced back to the whistleblower), and consider working through a nonprofit organization or other trusted entity that can serve as a buffer and reduce paper trails
Keep the whistleblower's information in a secure location
Alert the whistleblower to applicable survival tips
- Carefully secure and protect evidence before drawing suspicion
- Engage in whistleblowing on own time, with own resources
- Communicate through secure methods[xiii]

Information Security

Take concrete measures to secure the whistleblower's information, and as discussed in the previous section, enfranchise the whistleblower in the decision-making process to share it. The House already operates within a secure environment, and it is exploring additional measures to enhance information security. Due to technological advances, whistleblowers are at increased risk of surveillance, but there are also more tools available to protect their communications. Always confirm that encryption or other security software is approved by the House before you use it to communicate with a confidential source.[xiv] In the meantime, there are basic preventative measures and controls that your office can put in place to help safeguard whistleblower communications. These practices should be used in conjunction with any ground rules established in the previous section.

This section will provide guidance for protocols to keep disclosures secure and the development of a secure tracking system.

Protocols to Keep Disclosures Secure

Develop written processes and guidelines to keep disclosures secure. Any relevant existing office policies, such as around the handling of classified or other sensitive information, should be incorporated into your office's procedures for this section. Best practices include:

- Designate one or more staff to handle whistleblower correspondence, who are trained in best practices for working with whistleblowers and keeping their disclosures secure, and limit access to whistleblower files on a need-to-know basis
- Ensure Personally Identifiable Information (PII) is handled appropriately[xv]
- Ensure sensitive or classified information is handled lawfully[xvi]
- Use a House authorized email address (<u>not</u> a personal email address) for email communications
- Use a secure tracking system to store whistleblower files

Secure Tracking System

Develop a secure tracking system located within your office's secure environment to store and update all whistleblower-related documentation.[xvii] Key practices include:

- Limit access to authorized staff or on a need-to-know basis
- Document initial inquires in a tracking sheet or form filed within the secure tracking system
- After initial receipt, create a separate case file for each whistleblower with key information that can be updated to reflect status/prioritization, referrals, follow-up, and designated staff contact
- Evaluate trends and risks within your office, Congress, and throughout the federal government to ensure that you are using the most secure technology available to the House and have adequate safeguards in place[xviii]

Module 4: Navigating the Legal Landscape

This module will provide an overview of protected whistleblowing, the primary federal whistleblower laws within the public and private sectors, the lawful disclosure of classified information, and gaps in legal protections.

Whistleblower law is notoriously complex and can be difficult to navigate. Fortunately, your job is not to provide legal advice to the whistleblower. That said, to help limit liability for your office and your sources, it is important to understand a whistleblower's legal protections – or lack thereof.

There exists a patchwork of federal, state and local laws, as well as First Amendment rights, that comprise the legal whistleblower landscape. Each law has different remedies, procedural steps, and paths for enforcement. However, nearly all modern whistleblower statutes reflect strong workplace rights and have passed either unanimously or with bipartisan support.

Protected Whistleblowing

Primary laws for the executive branch and contractors define a whistleblower as a current employee, former employee, or applicant who discloses information that he or she reasonably believes evidences:

A violation of law, rule or regulation;
Gross mismanagement;
A gross waste of funds;
Abuse of authority; or
A substantial and specific danger to public health or safety.

The Whistleblower Protection Act, the primary law for most executive branch employees, also protects:

Disclosures of policy decisions if the employee reasonably believes that the *consequences* would result in one of the protected categories (e.g. gross waste of funds, substantial and specific danger to public health or safety)
Censorship of peer-reviewed research, analysis, or technical information

Retaliation against an executive branch employee for engaging in protected whistleblowing is considered a prohibited personnel practice and is explicitly banned.

Specifically, under the Whistleblower Protection Act, employers are prohibited from *taking, failing to take, or threatening to take*, personnel actions against an employee for engaging in protected whistleblowing. Prohibited personnel actions include:

Failure to promote
Certain forms of disciplinary or corrective action
Detail, transfer or reassignment

Poor performance evaluation
Change in compensation, benefits or awards
Decision regarding education or training that would otherwise result in a positive personnel action such as an appointment or promotion
Change in duties, responsibilities, or working conditions
Ordering a psychiatric exam
Use of non-disclosure agreements that do not include an exception for legal whistleblowing

Executive branch employees are also protected from retaliation if they:

Refuse to obey an order that would require the employee to violate a law, rule, or regulation
File a complaint, grievance or appeal
Testify or help another person with exercising their rights
Cooperate with or disclose information to Congress, an OIG, or the Office of Special Counsel

Under whistleblower protection laws, there are four key questions to determine if retaliation occurred, including:

Did the whistleblower engage in protected activity?
Did the whistleblower face an adverse employment action?
Did the employer have knowledge of the protected activity?
Did the protected activity prompt the adverse employment action?

However, if the employer can show it would have taken the same employment action in the absence of the protected activity, the whistleblower may not be able to prove retaliation.

Notably, the Whistleblower Protection Act includes an employee-friendly burden of proof – the level of evidence required to win a case. The employee must demonstrate that the protected activity was a *contributing factor*. In other words, they must show that their whistleblowing impacted the personnel action in any way, which is basically a relevance standard or a low bar. The employer then must prove by *clear and convincing evidence* that it would have taken the same personnel action regardless of the whistleblower activity, which is a much higher bar.

For employees engaging in "Duty Speech" – making a disclosure related to their job duties – they have a slightly higher burden under the Whistleblower Protection Act. Specifically, rather than a mere causal connection, they must prove retaliation and demonstrate that their employer had animus (intent to harm) as a result of their whistleblowing.

Under public and private-sector whistleblower laws, several factors are used to evaluate an employee's options for reporting wrongdoing, including:

Who is making the disclosure?
What is the nature of the information being disclosed?
To whom, how, and where was the disclosure made?

Executive Branch and Contractors

The right for executive branch employees to communicate with Congress was originally established in the constitution and the Lloyd La-Follette Act of 1912. However, the Whistleblower Protection Act codified rights against retaliation for making a protected disclosure to Congress. Public employees are also protected from retaliation under the First Amendment when exposing matters of *public concern*. However, the constitutional rights are difficult to enforce. They are governed by far more difficult burden of proof and depend on a balancing test that the *public benefits of the communication outweigh any disruption to the government.* In effect, an employee may not know if their activity is protected under the First Amendment until the case is over. Conversely, most whistleblower protection laws include clear free speech boundaries to operate within.

The Whistleblower Protection Act covers most federal executive branch civilian employees. Separate whistleblower protection laws and policies exist for intelligence, military, law enforcement, public health service, and contractor employees, as well as employees who hold a security clearance.

There are several primary statutes that protect whistleblower communications with Congress, including:

Lloyd-La Follette Act of 1912:[xix] Right of executive branch employees to communicate with Congress
First Amendment of the U.S. Constitution: Right to free speech for all U.S. citizens, including communications with Congress, but limitations on enforcement of anti-retaliation rights
"Anti-Gag" Protections:[xx] Requires every U.S. Government and contractor nondisclosure agreement, policy or form to notify employees that their rights under laws for whistleblower protection and congressional communications supersede any restrictions. Comparable rights exist in most modern private sector whistleblower laws
Whistleblower Protection Act, as amended by Whistleblower Protection Enhancement Act of 2012:[xxi] Provides whistleblower protections for most executive branch employees who make authorized disclosures, including to Congress
Intelligence Community Whistleblower Protections:[xxii] Presidential Policy Directive-19, the Intelligence Authorization Act (IAA) FY2010, IAA FY2014, and Foreign Intelligence Surveillance Reauthorization Act of 2017 establish protections for Intelligence Community whistleblowers who make authorized disclosures, including to congressional intelligence committees, through designated processes
Military Whistleblower Protection Act:[xxiii] Provides whistleblower protections for Members of the Military Service who make authorized disclosures, including to Congress
Federal Contractor, Subcontractor, Grantee, Subgrantee, & Personal Service Contractor Whistleblower Protections:[xxiv] Provides whistleblower protections for federal contractors, subcontractors, grantees, subgrantees and personal service contractors who make protected disclosures to Congress and other recipients

Under certain statutes, penalties also exist for individuals who engage in retaliation or try to interfere with whistleblower communications to Congress, including protections for federal witnesses:

Salary Cutoff for Interfering with Congressional Communications:[xxv] Prohibits funds from being used to pay the salary of a federal officer or employee who interferes with or retaliates against a federal employee for communicating with Congress

Dr. Chris Kirkpatrick Whistleblower Act of 2017:[xxvi] The Office of Special Counsel can propose disciplinary penalties for supervisors who engage in whistleblower retaliation, including a suspension and potential reduction in grade or pay for the first offense and proposed removal for the second offense

Protections for Witnesses in Federal Investigations

- 18 U.S.C. § 1505: Prohibits obstruction of proceedings before Congress, agencies and departments. Penalty is a fine and imprisonment up to 5 years
- 18 U.S.C. § 1513(e): Prohibits retaliation against a witness, victim, or informant for law enforcement. Penalty is a fine or imprisonment up to 10 years
- 18 U.S.C. § 1512: Prohibits tampering with a witness, victim, or an informant. Penalty is a fine or imprisonment up to 20 years

Legislative Branch

The Congressional Accountability Act (CAA) provides legislative branch employees with protections under 13 laws, ranging from rights against discrimination and harassment to job protection under the family and medical leave provisions. Section 207 prohibits retaliation against employees who exercise their rights under the CAA.[xxvii] However, it does not provide anti-retaliation rights for disclosing waste, fraud, corruption, and other misconduct outside the scope of the CAA.

The CAA is enforced by the Office of Congressional Workplace Rights (OCWR), formerly the Office of Compliance. For matters within the scope of the CAA, legislative branch staff can arrange a meeting with the OCWR Confidential Advisor, who can provide legal advice, on a confidential and privileged basis, including assistance in drafting a claim that can be filed in the OCWR. House employees can also seek legal advice and representation confidentially from the Office of Employee Advocacy. House managers can seek confidential legal advice and representation from Office of House Employment Counsel.

To report misconduct, including matters outside the jurisdiction of the CAA, House staff can arrange a confidential consultation and submit an allegation with the House Committee on Ethics, submit an allegation with the Office of Congressional Ethics, or contact the House Office of Inspector General.

Private Sector

The Department of Labor's Whistleblower Protection Program, housed within the Occupational Safety and Health Administration, enforces most private-sector whistleblower retaliation claims. The 23 laws under its jurisdiction protect employees who report violations of workplace health and safety, transportation, consumer product, environmental, financial reform, food safety, health insurance reform, motor vehicle safety, nuclear, pipeline, public transportation agency, railroad, maritime, and

securities laws. Some of the environmental laws under its jurisdiction also cover federal, state, and local employees. Many of the laws explicitly protect communications with Congress.[xxviii]

Some private-sector whistleblower protection laws also include monetary award programs, which allow a whistleblower to receive a percentage of the recoveries resulting from their disclosure. Those programs are largely administered by the Securities and Exchange Commission Office of the Whistleblower, the Commodity Futures Trading Commission Whistleblower Program, and the Internal Revenue Service Whistleblower Office.

The False Claims Act, the pioneer whistleblower award law, is widely considered the federal government's most effective tool in combating fraud in federal spending. Under that law's qui tam provision, whistleblowers have helped the Department of Justice to recover nearly $45 billion dollars in taxpayer fraud since 1986. However, be aware that a whistleblower may be precluded from the benefits of the False Claims Act if they first disclose their information to Congress or other public entities.

Disclosing Classified Information

Whistleblower disclosures that involve information marked classified or other information barred from public release are permitted only if made through appropriate, lawful channels. *Providing classified documents to unauthorized recipients could result in criminal prosecution. Only congressional staff with appropriate clearances should receive classified information.* [xxix]

Under the Intelligence Identities Protection Act, classified information must be marked or designated. [xxx] That requirement is enforced through the anti-gag protections included within the annual federal budget. [xxxi] However, some Intelligence Community (IC) elements do not universally recognize that boundary and their regulations may prohibit the release of unmarked but classified information. When in doubt about what information you are authorized to receive, it is advisable to consult House counsel or the Office of House Security.

Employees and contractors working in the IC elements should follow the processes established within the Intelligence Community Whistleblower Protection Act (ICWPA) to ensure they are making a protected disclosure to the House Permanent Select Committee on Intelligence or the Senate Select Committee on Intelligence. The IC OIG has developed a website with guidance for lawful disclosures.[xxxii]

Under the ICWPA, an IC employee or contractor who intends to report to Congress a complaint or information with respect to an "urgent concern" must report to their respective IG. Within 14 days of receiving the complaint, the IG must report all complaints that the IG deems credible to the head of the IC element. Within seven days, the agency head is required to report the complaint to the congressional intelligence committees. However, if the agency head determines that the complaint would create a conflict of interest, then that individual would return the complaint to the IG to forward to the Director of National Intelligence (or Defense Secretary for the DoD intelligence agencies) to forward to Congress.

If the event the IG does not report the complaint, does not find it credible, or reports it inaccurately, the whistleblower has the right to submit the complaint directly to the congressional intelligence

committees. However, the whistleblower must first inform the agency head, through the IG, of the intent to contact the congressional intelligence committees directly. Further, the whistleblower must follow the head of the IC element's guidance on protection of classified information.[xxxiii]

Executive branch employees or applicants that are covered under the Whistleblower Protection Act and have authorized access to classified information can also make protected classified disclosures to Congress, *if the information was classified by the heads of non-IC elements and if the disclosure does not reveal sources and methods*.[xxxiv] E.g. a State Department employee lawfully discloses to the House Foreign Affairs Committee a classified memorandum about a security threat to a U.S. embassy overseas.

There are also some limitations on protection for the public disclosure of certain unclassified information. For instance, a public disclosure is not protected under the Whistleblower Protection Act if – 1) disclosing the information is prohibited by law, or 2) under an executive order the information is required to be kept secret in the interest of national defense or the conduct of foreign affairs.

Gaps in Legal Protections

There are significant gaps in whistleblower laws that leave certain sectors of the labor force uncovered. Specifically, the Whistleblower Protection Act does not cover executive branch political appointees, the legislative branch, or the judicial branch. Further, many industries, such as agriculture and meat packing, do not have sector whistleblower rights. However, many private sector employees within those uncovered industries are still swept in under broader whistleblower statutes, such as the Sarbanes O xley Act, which provides protections to employees of publicly traded companies.

For those whistleblowers covered under the law, the strength of their rights varies significantly. This is most obvious in terms of the basic legal fundamentals, including:

Burden of Proof: The amount of evidence that is required to prove retaliation and win a case can range from a low bar for the employee (e.g. Whistleblower Protection Act) to a much higher burden (e.g. Military Whistleblower Protection Act).

- **Statute of Limitations**: The amount of time an employee must file a retaliation claim can range from a mere 30 days (e.g. Clean Water Act) to three years (e.g. False Claims Act).
- **Due Process**: Some laws do not even include the right to an administrative hearing or to appeal an informal agency investigation that may take years to complete (e.g. Occupational Safety and Health Act), whereas other laws provide employees with full appeal rights and access to a jury trial to challenge retaliation (e.g. federal contractor whistleblower rights).
- **Covered Categories**: Under all but one U.S. federal whistleblower law (Defend Trade Secrets Act), legal rights are limited to workplace retaliation, such as being demoted or fired. The laws do not provide protection against civil and criminal retaliation. In effect, even when the whistleblower is engaging in legally protected activity, they can become the targets of expensive defamation suits or criminal investigations and prosecutions. Conversely, most modern international whistleblower laws shield against civil and criminal liability when engaging in lawful whistleblowing.

[i] H. Res. 6, Sec. 104 (e)(3)
[ii] U.S. Government Accountability Office, "Whistleblowers: Key Practices for Congress to Consider When Receiving and Referring Information," GAO-19-432 (2019), *available at* https://www.gao.gov/assets/700/698940.pdf; Project On Government Oversight, Government Accountability Project, Public Employees for Environmental Responsibility, "Caught Between Conscience and Career: Expose Abuse Without Exposing Your Identity," (2019), *available at* https://s3.amazonaws.com/docs.pogo.org/publication/Caught_Between_Conscience_and_Career.pdf.
[iii] 5 CFR § 2635.101
[iv] Public Law 96-303
[v] Classified conversations should be coordinated with the Office of House Security, *available at* http://sgtatarms.house.gov/ohs.
[vi] Personally Identifiable Information (PII) includes any information that can be used to determine an individual's identity, including name, date of birth, Social Security number, or other types of information that can be traced to an individual, such as employment, medical, financial, and educational information. The House Office of the Sergeant of Arms provides additional guidance for the handling of PII, *available at* http://saa.house.gov/ohs/personally-identifiable-information-pii.shtml.
[vii] Classified conversations should be coordinated with the Office of House Security, *available at* http://sgtatarms.house.gov/ohs/. Further, the House has developed standards for the electronic and physical protection of sensitive information, "HISPOL 010.0, Protection of Sensitive Information," *available at* https://go.usa.gov/xveDA.
[viii] The House has developed standards for the electronic and physical protection of sensitive information. These standards can be applied to your office's development of a secure tracking mechanism for whistleblower communications, "HISPOL 010.0, Protection of Sensitive Information," *available at* https://go.usa.gov/xveDA. House Information Resources can assist your office in developing a separate secure OneDrive that can only be accessed by designated individuals.
[ix] Review House IT Security Policies or contact House Information Resources for the most current information, *available at* https://go.usa.gov/xveDA.
[x] Oversight.gov, "Report Waste, Fraud, Abuse, or Retaliation," *available at* https://oversight.gov/whistleblowers.
[xi] A warning letter is a useful tool to help deter retaliation against a congressional witness. However, it is important to weigh the specific circumstances involved in each case and manage expectations around your office's involvement. For instance, a congressional office may be willing to send a support letter but not willing to serve as a witness in subsequent litigation. Conversely, an office may not place limitations around support for their witnesses. Consult your office's counsel before making any commitments that you may not be able to honor.
[xii] Ibid.
[xiii] Whistleblower-specific guidance on how to protect their communications can be found in the following resource developed by the Project On Government Oversight, Government Accountability Project, and Public Employees for Environmental Responsibility, "Caught Between Conscience and Career: Expose Abuse Without Exposing Your Identity," (2019), *available at* https://s3.amazonaws.com/docs.pogo.org/publication/Caught_Between_Conscience_and_Career.pdf.
[xiv] Offices may utilize platforms compliant with the House encryption requirements. Encryption requirements are explicitly outlined for mobile devices in "HISPOL 008.1, Information Security of Enterprise Mobile and Portable Devices," *available at* https://go.usa.gov/xveDA.
[xv] Personally Identifiable Information (PII) includes any information that can be used to determine an individu al's identity, including name, date of birth, Social Security number, or other types of information that can be traced to an individual, such as employment, medical, financial, and educational information. The House Office of the Sergeant of Arms provides additional guidance for the handling of PII, *available at* http://saa.house.gov/ohs/personally-identifiable-information-pii.shtml.
[xvi] Classified conversations should be coordinated with the Office of House Security, *available at* http://sgtatarms.house.gov/ohs/. Further, the House has developed standards for the electronic and physical protection of sensitive information, "HISPOL 010.0, Protection of Sensitive Information," *available at* https://go.usa.gov/xveDA.

[xvii] The House has developed standards for the electronic and physical protection of sensitive information. These standards can be applied to your office's development of a secure tracking mechanism for whistleblower communications, "HISPOL 010.0, Protection of Sensitive Information," *available at* https://go.usa.gov/xveDA. House Information Resources can assist your office in developing a separate secure OneDrive that can only be accessed by designated individuals.
[xviii] Review House IT Security Policies or contact House Information Resources for the most current information, *available at* https://go.usa.gov/xveDA.
[xix] 5 U.S.C. § 7211
[xx] 5 U.S.C. § 2302(b)(13) and Sec. 743 of Public Law 116-93 require that any non-disclosure policy include the following language: "These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling."
[xxi] 5 U.S.C. § 2302(b)(8)
[xxii] Michael E. DeVine, "Intelligence Community Whistleblower Protections," Congressional Research Service, R45345 (2019), *available at* https://fas.org/sgp/crs/intel/R45345.pdf.
[xxiii] 10 U.S.C. § 1034
[xxiv] 41 U.S.C. § 4712 and 10 U.S.C. § 2409
[xxv] Sec. 713 of Public Law 116-93
[xxvi] 5 U.S.C. § 7515
[xxvii] 2 U.S.C. § 1317
[xxviii] Occupational Safety and Health Administration, U.S. Department of Labor, "The Whistleblower Protection Program," *available at* https://www.whistleblowers.gov/.
[xxix] Classified conversations should be coordinated with the Office of House Security, *available at* http://sgtatarms.house.gov/ohs.
[xxx] 50 U.S.C. § 3126
[xxxi] Sec. 743 of Public Law 116-93
[xxxii] Office of the Director of National Intelligence, "IC Whistleblowing," *available at* https://www.dni.gov/ICIG-Whistleblower/index.html.
[xxxiii] Michael E. DeVine, "Intelligence Community Whistleblower Protections," Congressional Research Service, R45345 (2019), *available at* https://fas.org/sgp/crs/intel/R45345.pdf.
[xxxiv] 5 U.S.C. 2302(b)(8)(C)(ii)

'Whistleblower Disclosure and Protection in Pr actice:
Discussion of Challenges and Solutions'

Role-playing an interaction with a witness in the workplace

Scenario 1

A construction worker is telling his/her manager that the roof that the company had just finished installing at a school was not made from the proper materials, and it could collapse. The school year is going to begin the following week, and the worker is worried about teachers and students being hurt or killed.

Employee: sincere, helpful, loyal, concerned about the well-being of the company, dedicated, has detailed facts about the misconduct, apprehensive about coming forward:
• "I think this problem is serious and needs to be fixed."
• "I felt a duty to tell you about this."

Manager: open, curious, protective, discreet, thankful, supportive, compassionate:
• "I will fix the problem, and I will help you. I will protect your name and your job."
• "Thank you for coming forward. We need more employees like you."

Scenario 2

A construction worker is telling his/her manager that the roof that the company had just finished installing at a school was not made from the proper materials, and it could collapse. The school year is going to begin the following week, and the worker is worried about teachers and students being hurt or killed.

Employee: sincere, helpful, loyal, concerned about the well-being of the company, dedicated, has detailed facts about the misconduct, apprehensive about coming forward:
• "I think this problem is serious and needs to be fixed."
• "I felt a duty to tell you about this."

Manager: skeptical, threatening, hostile, suspicious, paranoid, close-minded, disinterested:
• "Why are you getting involved with this? Who do you think you are? It is not your concern."
• "Do you want to keep working here? Be quiet or else."

Scenario 3

A bank employee is showing to his/her manager documents that show unexplained transfers of large amounts of money into the bank accounts of local politicians. The documents do not prove that crimes have been committed, but they suggest a potential problem.

Employee: sincere, helpful, loyal, concerned about the well-being of the company, dedicated, has detailed facts about the misconduct, apprehensive about coming forward:
• "I think this problem is serious and needs to be fixed."
• "I felt a duty to tell you about this."

Manager: open, curious, protective, discreet, thankful, supportive, compassionate:
• "I will fix the problem, and I will help you. I will protect your name and your job."
• "Thank you for coming forward. We need more employees like you."

Scenario 4

A bank employee is showing to his/her manager documents that show unexplained transfers of large amounts of money into the bank accounts of local politicians. The documents do not prove that crimes have been committed, but they suggest a potential problem.

Employee: sincere, helpful, loyal, concerned about the well-being of the company, dedicated, has detailed facts about the misconduct, apprehensive about coming forward:
• "I think this problem is serious and needs to be fixed."
• "I felt a duty to tell you about this."

Manager: skeptical, threatening, hostile, suspicious, paranoid, close-minded, disinterested:
• "Why are you getting involved with this? Who do you think you are? It is not your concern."
• "Do you want to keep working here? Be quiet or else."

'Whistleblower Disclosure and Protection in Pr actice:
Discussion of Challe nges and Solutions'

Whistleblowing and Public Disclosure

*Which of these situations would justify **bypassing workplace and regulatory reporting channels** and making a report to the public or the media directly?*

(1) The construction company where I work installed a sidewalk that is 1 meter too wide.
Yes ___ / No ___

(2) My company spilled large amounts of toxic chemicals into a river that serves as a drinking water supply, and the managers are trying to cover up the incident.
Yes ___ / No ___

(3) The construction company where I work knowingly used large amounts of substandard concrete to build a school that is 10 stories tall, and the company is doing nothing to fix the problem.
Yes ___ / No ___

(4) Some of my coworkers harass me because of my religious affili ation.
Yes ___ / No ___

(5) More than 300 of my coworkers were threatened with immediate physical violence by my managers because of their religious affiliation.
Yes ___ / No ___

(6) I am an IT worker, and my company gave me an outdated software training manual.
Yes ___ / No ___

(7) The freshness date on the milk being served with the coffee in our office has expired.
Yes ___ / No ___

(8) The head of my ministry embezzled millions of lei in public funds and has destroyed all of the evidence of his crime and threatened people not to report him.
Yes ___ / No ___

Hard Wires: The Neuropsychology of Speaking Up[1]

Now that whistleblowing has become an everyday happening, more attention is turning to figuring out why only some people speak up while most others don't.

Amherst College psychology Professor Catherine Sanderson began delving into the question after a tragedy that occurred at her son's university. For nearly 20 hours, a group of students stood over a drunken student who had fallen and hit his head. By the time someone called for help, it was too late. Why did this group of people remain idle and watch their friend die?

Sanderson says part of the answer lies in the physical processes that naturally govern how our brain works. In her recent book *The Bystander Effect: Understanding the Psychology of Courage and Inaction*, Sanderson explains that human physiology itself is at least partly to blame.

In an interview with Amelia Tait of *The Guardian*, Sanderson says that interacting with other people reduces our feeling of control. Remarkably, as the number of people involved with a situation increases, the parts of our brain that help us respond to events actually start to shut down. "Many of the processes that drive inaction occur not through a careful deliberative process, but at an automatic level in the brain," she said.

Our neurological systems are so firmly biased against whistleblower-type behavior, says Sanderson, that taking action can cause feelings of rejection so intense that they can feel like physical pain. This is especially strong among people who are particularly worried about fitting in and fear being ostracized.

It is little wonder that individual employees – especially those who work in large companies or organizations – say nothing when they witness crime or corruption. Sanderson estimates only 5-10 percent of people have the capacity to overcome social pressures and be "moral rebels": people who have a high level of self-esteem and a strong belief that their actions will make a difference in the world.

Sanderson's findings also help explain the retaliation and rejection that whistleblowers experience in a vast majority of cases. Their behavior simply doesn't compute, and even family members and close friends cannot comprehend doing the same thing. They cannot understand why someone would blow the whistle because their brains tell them it's not normal.

Through her research, Sanderson found that people often believe they would take swift action when presented with the opportunity. In their private thoughts, people may tell themselves they would stand up and do the right thing. When a real-life opportunity actually arrives, however, most people remain bystanders because of a phenomenon called "deindividuation."

Tait asked Sanderson whether people can be "re-individualized" so we can do what we consciously think is right for us – even if it means going against our own instincts. Encouragingly, Sanderson answers affirmatively: "My hope is that reading this book will help people understand that they have a choice. Neuroscience lets us be aware of our pre-existing unconscious biases. It gives us the power to say: 'This is normal and it's natural, but I still have some agency and I can act.'"

[1] Worth, Mark, *Whistleblower Network News*, May 13, 2021; https://whistleblowersblog.org/features/hard-wires-the-neuropsychology-of-speaking-up/

Whistleblower Protection as an Antidote for Human Instincts[1]

There's a lot more to writing an effective whistleblower protection law than including the correct legal phrasing. Words matter, but so does the meaning behind the words. The process is always different, usually depending on the officials' previous knowledge of the issue. Typically, the level of awareness is inversely proportional to the officials' hesitance to grant strong whistleblower rights.

Over the years, we've learned a great deal about this reluctance. What we've seen is that officials' arguments against whistleblower rights correspond directly to the very reasons we need whistleblower protection laws in the first place.

Most of the resistance to protecting whistleblowers – and the reasons people usually are denied protection in real-life cases – stem from these questions:

- Was the person acting in good faith?
- What was the person's motivation?
- Was the person's evidence accurate or complete?
- Did the evidence lead to an investigation or prosecution?
- Did the person make the report to the right office and in the proper way?
- Did the person prove he or she was fired because of making a disclosure?

These are the natural, almost instinctual reactions to a whistleblower: the person must have had an ulterior motive, the person didn't actually prove misconduct occurred, the person should have told someone else or in a different way, and the person couldn't prove they were fired because they made a report.

This is why international standards for whistleblower laws don't include a good faith or motivation test, do not require the person to prove anything, do not require an investigation to result from the report, give people options on how to make a report, and require employers to prove why they fired a whistleblower.

A lot of work needs to be done before officials themselves overcome these natural reactions to a whistleblower. Officials do not have to like the person, agree with the person, or think the report was important. Officials should not judge the person's behavior or put themselves in the shoes of the whistleblower and contemplate what they would do in the same situation. In fact, whistleblower laws do not give officials the authority or the discretion to do this. Their opinions are irrelevant. But these opinions reflect the very real instinctual reactions to a person who steps up and reveals hidden evidence of a crime.

In our work with policy-makers, we always talk about the spirit of the law: how can the law – however imperfect it may be – achieve its goals of protecting employees from reprisals and ensuring the evidence they report is fully investigated. Officials need to understand that the law is not a detached bureaucratic exercise. It is an active, living tool that is there to negate and overcome the skepticism of whistleblowers.

[1] Worth, Mark, *Whistleblower Network News*, March 11, 2021; https://whistleblowersblog.org/global-whistleblowers/opinion-whistleblower-protection-as-an-antidote-for-human-instincts/

If the officials themselves act upon this skepticism and allow their own opinions and instincts to cloud their judgment and interfere with their official duties, then there is very little chance of these laws working in practice. Promotional campaigns from public agencies encouraging people to make reports and promising protections will be empty and disingenuous. Employees will not be protected. Their careers and personal well-being will be destroyed. The crimes they report will not be investigated. Criminals will continue to break the law with impunity.

Adaptation of Information Theory to

DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
Adopted 23 October 2019

On the Protection of Persons Who Report Breaches of Union Law

Breaking the Silence:
Enhancing Whistleblowing Policies and Culture
in Western Balkans and Moldova

Regional Anti-Corruption Initiative (RAI)
(http://www.rai-see.org/)

Sarajevo November 16 -19, 2021

Thad M. Guyer
Government Accountability Project and
T.M. Guyer and Ayers & Friends, PC
Washington, DC
thad@guyerayers.com

TABLE OF CONTENTS

INFORMATION THEORY AS A TOOL FOR ANALYZING WHISTLEBLOWER INFORMATION REGIMES

Summary: Whistleblowers and governmental and corporate whistleblower protection programs can benefit from more sophisticated conceptual understandings of the cognitive process whistleblowers use to source, collect, and transmit "information" as that term is used in the EU Whistleblower Directive. Notwithstanding how fundamental "information" is to every whistleblower protection regime, and to the law generally, the conceptual dimensions and legal parameters of the term "information", "provided information" or "disclosed information" are seldom discussed beyond the context of "protected" or "unprotected" disclosures of information.

Objectives: By adapting "Information Theory" to whistleblower information transmission regimes, we hope to impart a deliberate conceptual grasp to whistleblower advocates on the sources and role of whistleblower "information". Doing so could foster enhanced appreciation of the strengths, weaknesses and potential impacts of whistleblowing in addressing corruption.

Information Theory: Information Theory is the scientific study of the quantification, transmission, communication and storage of information launched by Claude Shannon's 1948 paper. Although Shannon intended his audience to be radio and television communication engineers, his concepts and methodology of thinking moved into the popular domain. In 1953, Fortune magazine described the theory as more crucial to 'man's progress in peace, and security in war' than Einstein's physics. The theory is now used beyond digital applications, including legal applications. (See Appendix). Key components of information theory include:

> ***Channel Capacity*** Every communication channel had a speed limit, and it is impossible to get error free communication above the limit. No channel can go faster than the limit without losing information. This limitation is mitigated by separating the design of the information source from the design of the communication channels.
>
> ***Efficiency of Transmission Through Source Coding:*** Source coding is a process to format information to make it suitable for transmission through a selected communications channel. The basic objective of source coding is to remove redundancy and "noise" in the information to make the message smaller.
>
> ***Entropy and Information Content:*** Content of the information is irrelevant to its suitability for transmission. The problem is that as the number of recipients or uses increases, the capacity of channels degrades. The solution is to either reduce demand on available n channels or increase the number of channel available.

See Diagram on the next page.

Formal Architecture of Communication Systems

The following diagram illustrates the formal architecture Shannon offered as a schematic for a general communication system. Flip open to the beginning of any random textbook on communications, or even a paper or a monograph, and you will find this diagram.

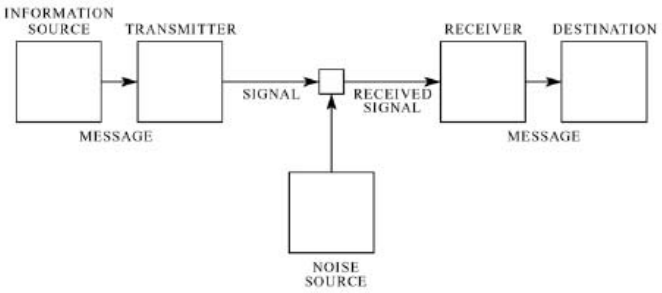


Figure 1. From Shannon's "A Mathematical Theory of Communication", page 3.

This figure represents one of the great contributions of A Mathematical Theory of Communication: the architecture and design of communication systems. It demonstrates that any

6.933 Project History, Massachusetts Institute of Technology
SNAPES@MIT.EDU

THE RADIOACTIVITY METAPHOR OF WHISTLEBLOWER INFORMATION

Uranium: A heavy metal which in raw ore is weakly radioactive. Uranium has been used as an abundant source of concentrated energy for over 60 years. Until *processed*, normal exposure is not considered hazardous.

> **Whistleblower Metaphor**: the basic data that employee may associate with possible corruption is like uranium, in and of itself it is not dangerous. But when these data are aggregated and *processed* into information and messages for disclosure, possessing it presents little danger so long as safe handling and storage practices are used.

Beta radiation: A small particle ejected from a radioactive atom. It has a moderate penetrating power and will penetrate only a fraction of an inch of skin tissue.

> **Whistleblower Metaphor:** Until a whistleblower places the corruption information into a communications channel, its beta radiation will present low level danger so long as it diligently secured from inadvertent discovery or audit, or revealed by missteps in exfiltrating the information from the workplace.

Gamma radiation: Radiation of high energy with high penetration of skin, tissues and organs.

> **Whistleblower Metaphor:** Once the corruption information is shared or transmitted through an information channel, it becomes gamma radioactive and dangerous to the whistleblower and to recipients or potential recipients of corruption message, including the whistleblower's financial dependents, supportive coworkers, the targeted corrupt officials, and even the whistleblower program receiving the information and charged with processing it. Whistleblower information can lead to financial catastrophe, psychiatric illness, suicide or murder.

Curie: A unit of measure of radioactivity. Depending upon the quality and grade of the uranium ore, large amount of uranium can have a small amount of radioactivity, and a small amount of uranium can have a lot of radioactivity.

> **Whistleblower Metaphor**: There is no link between the volume of information a whistleblower transmits and its potency. Unlike prosecutors, police and criminal investigators who have developed innate measures of corruption information danger, whistleblowers have no Geiger–Müller counters to assess the curie level of the corruption information they have transmitted. They tend to overrate the potency of their information and underestimate its danger.

Controlled Radiation area: An area where entry, activities, and exit are controlled by regulation to help ensure radiation protection and prevent the spread of contamination.

> **Whistleblower Metaphor:** The containment of a whistleblower's radioactive corruption information is mandated by the Directive, which regards such information as extremely dangerous.

Radioactive Waste and Storage: Radioactive waste by-products are stored to avoid radiation exposure to people. While those radioactive materials can no longer meet their beneficial purposes of lighting cities, treating cancer, and propelling submarines, their wastes are highly radioactive. Because radioactivity decays with time, high-level waste is stored in barrel or tanks for approximately 50 years before deep geological disposal. This has resulted in radiation "events" by movement, corrosion, ruptures and leaks of such barrels and tanks.

Whistleblower Metaphor: The Directive mandates long term storage of whistleblower and corruption information due to its potential valuable to future investigations perhaps years away. Like radioactive waste vessels, that information is subject to hack, inadvertent release, theft, and failure of cyber or cloud storage.

I. NORMATIVE RULES ESTABLISHING MESSAGE PARAMETERS

Legal and Social Norms Governing Whistleblower Information

1. Definitions of Whistleblower

Article 5 Definition: (7) '*reporting person'* means a natural person who reports or publicly discloses information on breaches acquired in the context of his or her work-related activities;

2. Charter and Fundamental Freedoms to Receive and Impart Information

(a) Consideration (31) Persons who report information about threats or harm to the public interest obtained in the context of their work-related activities make use of their *right to freedom of expression*. The right to freedom of expression and information, enshrined in *Article 11 of the Charter and in Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms*, encompasses the right to receive and impart information as well as the freedom and pluralism of the media.

(b) Consideration (31) [The] Directive draws upon the case law of the European Court of Human Rights (ECHR) on the right to freedom of expression, and the principles developed on this basis by the Council of Europe in its *Recommendation on the Protection of Whistleblower*s adopted by its Committee of Ministers on 30 April 2014.

(c) Consideration (45) Protection against retaliation as a means of safeguarding freedom of expression and the *freedom and pluralism of the media* should be provided both to persons who report information about acts or omissions within an organisation ('internal reporting') or to an outside authority ('external reporting') and to persons who make such information available in the public domain, for instance, directly to the public through online platforms or social media, or to the media, elected officials, civil society organisations, trade unions, or professional and business organisations.

(d) Consideration (109) *** Accordingly, it is essential that this Directive be implemented in accordance with those rights and principles by ensuring full respect for, inter alia, freedom of expression and information,

3. Goals: detection, investigation and prosecution of breaches

Consideration (2) [Whistleblowers] feed national and Union enforcement systems with information, leading to effective detection, investigation and prosecution of breaches of Union law, thus enhancing transparency and accountability.

II. INFORMATION AND MESSAGE SOURCES

The Exclusive Focus on Work-Related Information

1. Work Related Context

Article 5 Definition: (9) 'work-related context' means current or past work activities in the public or private sector through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information;

Consideration (36) Persons need specific legal protection where they acquire the information they report through their work related activities and therefore run the risk of work-related retaliation, for instance, for breaching the duty of confidentiality or loyalty.

2. Information from Present, Past or Future Employees

Article 4. Personal scope 1-3. This Directive shall apply to reporting persons working in the private or public sector who acquired information on breaches in a work-related context; including in a work-based relationship which has since ended; and to persons whose work-based relationship is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.

Consideration (39) Protection should also be granted to persons whose work-based relationship has ended, and to candidates for employment or persons seeking to provide services to an organisation, who acquire information on breaches during the recruitment process or another pre-contractual negotiation stage, and who could suffer retaliation, for instance in the form of negative employment references, blacklisting or business boycotting.

3. Information About Past Present or Future Breaches

Consideration (43) Effective prevention of breaches of Union law requires that protection is granted to persons who provide information necessary to reveal breaches which have already taken place, breaches which have not yet materialised, but are very likely to take place, acts or omissions which the reporting person has reasonable grounds to consider as breaches, as well as attempts to conceal breaches.

III. SOURCE CODING FOR TRANSMISSION

Special Rules for Protecting Certain Information

1. Inaccurate Information

Article 6-1. Reporting persons shall qualify for protection under this Directive provided that: (a) they had reasonable grounds to believe that the information on breaches reported was true.

Consideration (32) Protection is not lost where the reporting person reported inaccurate information on breaches by honest mistake.

2. Information About Potential and Future Breaches

Article 5 Definition: (2) 'information on breaches' means information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the organisation in which the reporting person works or has worked or in another organisation with which the reporting person is or was in contact through his or her work, and about attempts to conceal such breaches;

3. Privileged Access to Information

Consideration (37) Effective enforcement of Union law requires that protection should be granted to the broadest possible range of categories of persons, who have privileged access to information on breaches that it would be in the public interest to report and who may suffer retaliation if they report them.

4. Immunity for Exfiltrating Employer Information

Consideration (92) Where reporting persons lawfully acquire or obtain access to the information on breaches reported or the documents containing that information, they should enjoy immunity from liability. This should apply both in cases where reporting persons reveal the content of documents to which they have lawful access *as well as in cases where they make copies of such documents or remove them from the premises of the organisation* where they are employed, *in breach of contractual or other clauses* stipulating that the relevant documents are the property of the organisation.

5. Confidential Information

Article 21-2. [Reporting persons] shall not be considered to have breached any restriction on disclosure of information and shall not incur liability of any kind in respect of such a report or public disclosure provided that they had reasonable grounds to believe that the reporting or public disclosure of such information was necessary for revealing a breach pursuant to this Directive.

6. Professional Information

Consideration (27) Members of professions other than lawyers and health care providers should be able to qualify for protection under this Directive when they report information protected by the applicable professional rules, provided that reporting that information is necessary for the purposes of revealing a breach falling within the scope of this Directive.

7. Exemptions for Disclosures of InformationViolating Loyalty, Confidentiality, Trademark and NDA Rules

(a) **Article 21-7**. Where a person discloses information on breaches that includes trade secrets, such reporting or public disclosure shall be considered lawful under the conditions of Article 3(2) of the Directive (EU) 2016/943.

(b) **Consideration (97)** In actions taken against reporting persons outside the work-related context, through proceedings, for defamation, breach of copyright, trade secrets, confidentiality and personal data protection, they should be able to rely on this Directive as a defence, provided that the information reported or publicly disclosed was necessary to reveal the breach.

(c) **Consideration (91)** It should not be possible to rely on individuals' legal or contractual obligations, such as loyalty clauses in contracts or confidentiality or non-disclosure agreements, so as to preclude reporting, to deny protection or to penalise reporting persons for having reported information on breaches or made a public disclosure where providing the information is necessary for revealing the breach.

IV. INFORMATION MESSAGE TRANSMISSION

Information Processing Modalities: Internal, External and Public Domain

1. Internally Reported Information

(a) **Article 5 Definition: (4)** 'internal reporting' means the oral or written communication of information on breaches within a legal entity in the private or public sector;

(b) **Article 9-1**. The procedures for internal reporting and for follow-up as referred to in Article 8 shall include the following: (c) the designation of an impartial person or department competent for following-up on the reports, asking for further information and providing feedback to the reporting person; and (g) provision of clear and easily accessible information regarding the procedures *for reporting externally to competent authorities*.

(c) **Consideration (55)** Internal reporting procedures should enable legal entities in the private sector to receive and investigate in full confidentiality reports by the workers of the entity and of its subsidiaries or affiliates ('the group'), but also, to any extent possible, by any of the group's agents and suppliers and by any persons who acquire information through their work-related activities with the entity and the group.

(d) **Article 7-1**. As a general principle information on breaches may be reported through the internal reporting channels and procedures provided for in this Chapter.

(e) **Consideration (33**) Internal reporting is the best way to get information to the persons who can contribute to the early and effective resolution of risks to the public interest.

2. Externally Reported Information to Authorities

Article 5 Definition: (5) 'external reporting' means the oral or written communication of information on breaches to the competent authorities;

Article 10. [R]eporting persons shall report information on breaches using the channels and procedures referred to in Articles 11 and 12, after having first reported through internal reporting channels, *or by directly reporting through external reporting channels*.

3. Information to Public Domain

Article 5 Definition: (6) 'public disclosure' or 'to publicly disclose' means the making of information on breaches available in the public domain;

Article 15-1(b)(ii). A person who makes *a public disclosure* shall qualify for protection under this Directive if the person has reasonable grounds to believe external reporting [presents] a risk of retaliation or low prospect of the breach being effectively addressed; or where evidence may be concealed or destroyed; or where an authority may be in collusion with the perpetrator of the breach or involved in the breach.

V. NOISE AND INFORMATION ENTROPHY

Special Disqualifications for Certain Information

1. Classified Information

Article 3.3(a). This Directive shall not affect the application of Union or national law relating to the protection of classified information;

Consideration (25) This Directive should also be without prejudice to the protection of classified information which Union law or the laws, regulations or administrative provisions in force in the Member State concerned require, for security reasons, to be protected from unauthorised access.

2. False or Malicious Information

(a) **Article 23-2**. Member States shall provide for effective, proportionate and dissuasive penalties applicable in respect of reporting persons where it is established that they *knowingly reported or publicly disclosed false information*.

(b) **Consideration (32)** reporting persons should believe the matters reported by them are true. That requirement is an essential safeguard against malicious and frivolous or abusive reports.

(c) **Consideration (102)** Penalties against persons who report or publicly disclose information on breaches which is demonstrated to be knowingly false are also necessary to deter further malicious reporting and preserve the credibility of the system.

3. Superfluous and Publicly Known Information

(a) **Article 11-4**. Member States may provide that competent authorities can decide to close procedures regarding *repetitive reports* which do not contain any *meaningful new information.*

(b) **Consideration (70)** Competent authorities can close repetitive reports which do not contain any meaningful new information *adding to a past report* in respect of which the relevant procedures were concluded.

(c) **Consideration (91)** [P]rotection should not extend to *superfluous information*.

(d) **Consideration (43)** [P]protection should not apply to persons who report information which is *already fully available in the public domain* or *unsubstantiated rumo*urs and *hearsay*.

VI. INFORMATION RECEIVER CHANNELS

Member State Information Processing Obligations

1. Competent Authorities to Receive Information

(a) **Article 5 Definition (14)** 'competent authority' means any national authority designated to receive reports in accordance with Chapter III and give feedback to the reporting person, and/or designated to carry out the duties provided for in this Directive, in particular as regards follow-up.

(b) **Consideration (64)** Such competent authorities could be *judicial* authorities, *regulatory* or supervisory bodies competent in the specific areas concerned, or authorities of a more general competence at a *central level* within a Member State, *law enforcement* agencies, *anticorruption* bodies or *ombudsmen*.

(c) **Consideration (64)** It should be for the Member States to designate the authorities competent to receive information on breaches falling within the scope of this Directive and give appropriate follow-up to the reports.

2. Information Channel Requirements

(a) **Article 11-2(a).** Member States shall ensure that the competent authorities establish *independent and autonomous* external reporting channels, for receiving and handling information on breaches;

(b) **Consideration (73)** In order to enable effective communication with staff members who are responsible for handling reports, it is necessary to have channels that are user-friendly, secure, ensure confidentiality.

(c) **Article 20-1(c).** Member States shall ensure access to legal aid in criminal and in cross-border civil proceedings and, in accordance with national law, legal aid in further proceedings and legal counselling or other legal assistance.

3. Confidentiality Control Areas and Protocols

(a) **Article 12-1(a)** External reporting channels shall be designed, established and operated in a manner that ensures the completeness, integrity and confidentiality of the information and *prevents access thereto by non-authorised staff members* of the competent authority.

(b) **Article 16.1**. Member States shall ensure that the identity of the reporting person is not disclosed to anyone beyond the authorised staff, including information from which the identity of the reporting person may be directly or indirectly deduced.

(c) **Article 16.2.** [T] he identity of the reporting person may be disclosed only where necessary and proportionate to an obligation imposed by Union or national law in the context of investigations by national authorities or judicial proceedings.

VII. COMPETENT AUTHORITY TRANSMITTERS OF INFORMATION

1. Required Information Feedback Loop

Article 5 Definition: (13) 'feedback' means the provision to the reporting person of information on the action envisaged or taken as followup and on the grounds for such follow-up.

Article 12-4. Member States shall ensure that competent authorities designate staff members responsible for handling reports, and in particular for: (a) providing any interested person with information on the procedures for reporting; and (c) maintaining contact with the reporting person for the purpose of providing feedback and requesting further information where necessary.

2. Advice on Risks and Protected Status of Information Disclosure

Article 20-1(a). Member States shall ensure access to support measures, in particular comprehensive and independent *information and advice.*

Consideration (89) Individual, impartial and confidential advice, free of charge, should be available on:

> (i) whether the information in question is covered by the applicable rules on whistleblower protection;
>
> (ii) which reporting channel might best be used; and
>
> (iii) which alternative procedures are available in the event that the information is not covered by the applicable rules, so-called 'signposting'.

3. Clarifying and Supplemental Information Requirements

Article 13(c). Member States shall ensure that competent authorities publish on their websites the procedures for competent authority to request the reporting person to *clarify the information* reported or to provide additional information.

Consideration (57) It should be possible to ask the reporting person to provide *further information*, during the course of the investigation, albeit without there being an obligation to provide such information.

4. Required Information Storage

Article 12-1(b). External reporting channels shall enable the durable storage of information in accordance with Article 18 to allow further investigations to be carried out.

Consideration (86) Member States should ensure that there is adequate record-keeping as regards all reports of breaches, *that every report is retrievable* and that information received through reports *can be used as evidence* in enforcement actions where appropriate.

VIII. RE-TRANSMISSION OF INFORMATION TO SUBSEQUENT DESTINATIONS

Agencies Receiving Whistleblower Information from Competent Authorities

1. Referral of Information within the Member State

Article 11-2(f) Competent authorities must transmit in due time the information contained in the report to competent institutions, bodies, offices or agencies of the Union, as appropriate, for further investigation, where provided for under Union or national law.

Consideration (64) Such competent institutions within the Member State include:

(1) Authorities at a central level within a Member State
(2) Regulatory bodies in the specific areas concerned
(3) Judicial authorities
(4) Law enforcement agencies
(5) Anticorruption bodies
(6) Ombudsmen.

2. Referral of Cases and Information by Competent Authorities to the EU

Consideration (71) Where provided for under Union or national law, the competent authorities should refer cases or relevant information on breaches to:

(i) Institutions, bodies, offices or agencies of the Union

(ii) European Anti-Fraud Office (OLAF)

(iii) European Public Prosecutor Office (EPPO)

3. Cross-Border Information Shared by Member States

Consideration (72) In many policy areas falling within the material scope of this Directive, there are cooperation mechanisms through which national competent authorities exchange information and carry out follow-up activities in relation to breaches of Union rules with a cross-border dimension.

IX. CONCLUSION

Acquiring a theoretical understanding of the complex information channels required by the Directive will enhance the practitioner's effectiveness as a participant in regional and continental anticorruption initiatives. In particular, an information management approach will allow whistleblower programs to achieve the following in addition to supporting (a) normative values of informational freedom, (b) societal benefits in waging anticorruption battles regardless of outcome, and (c) the humanistic value of protecting workers:

1. Implementation of the primary operational objective of the Directive: Information collection and storage to fuel present and future corruption investigations.

2. Compliance with informational mandates and considerations of the Directive in designing, maintaining and evolving whistleblower protection programs with maximum information utilization and responsiveness.

3. Shielding whistleblower protection programs from unfair criticism of results by showcasing demonstrable and measurable operational excellence.

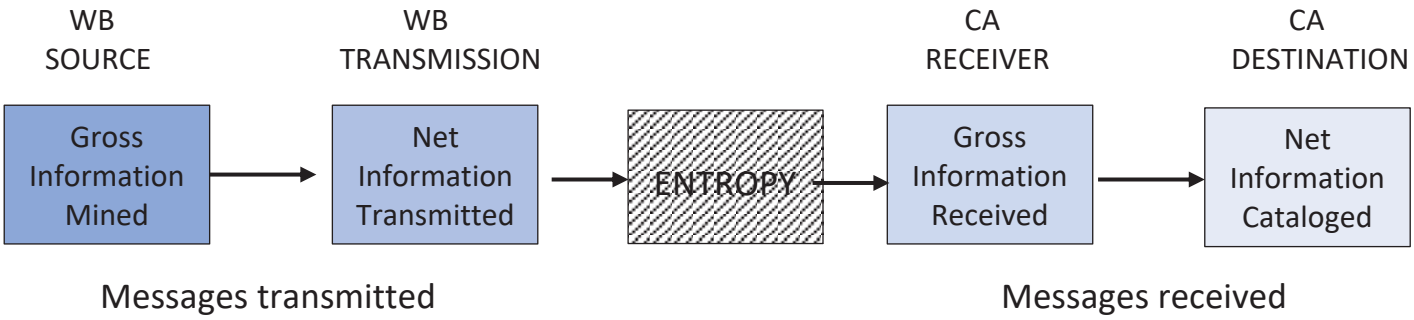
Belgrade, November 12, 2021

APPENDICES

X. APPENDIX 1. INFORMATION THEORY: SHANNON CHANNEL DIAGRAMS

A. INFORMATION THEORY FOR IMPLEMENTING EU DIRECTIVE GOALS AND OBJECTIVES

"Information theory" posits a universal communication ***channel design schematic*** of ***five information stations***, (2) transmission, (2) receipt and (1) channel connecting the four. ***Inefficiency*** of any station will ***degrade message transmission*** and/or ***receipt***



The *value* of the following normative and operational goals and objectives are ***not dependent on favorable outcomes***

1. EU Directive primary ***normative goals*** of:

   (a) "***informational freedom"*** of citizens and journalists

   (b) promoting ***anti-corruption programs*** by ***encouraging whistleblowers*** to provide information of corruption

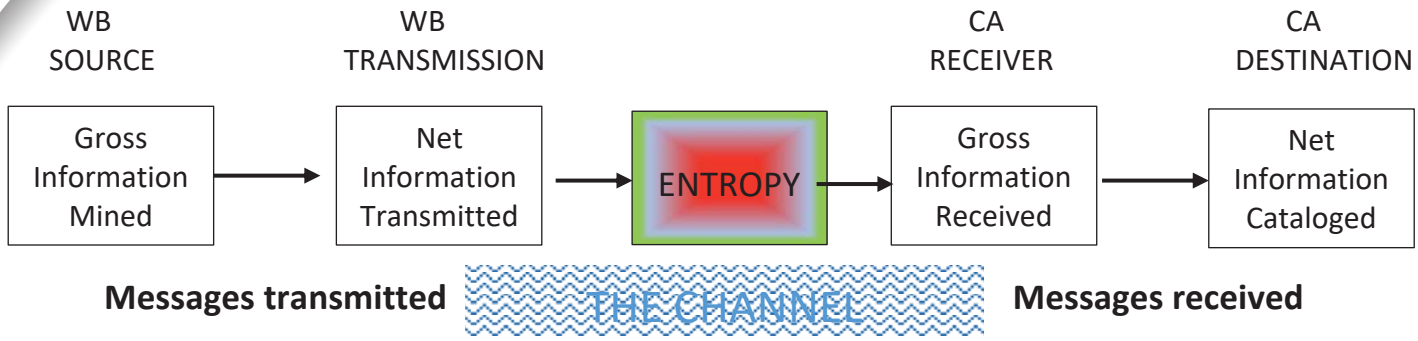
(2) EU Directive primary ***operational objectives***:

   (a) ***collection and storage*** of ***evidence*** to support present and future investigations

   (b) ***collaborating with EU*** anti-corruption agencies by ***sharing corruption evidence*** within and outside country

EU Directive enabling of ***information channels*** is a ***landmark institutionalization*** of ***whistleblowing and informational freedom***

B. EU OPERATIONS PRIME DIRECTIVE: CREATING INFORMATION "CHANNELS"



Core challenges in designing and managing channel flow:

The How-to

(+) MAXIMIZE CHANNEL EFFICIENCY
(-) MINIMIZE CHANNEL ENTROPY
"Entropy" = channel inefficiency, obstruction or "noise"

The Directive addresses channel efficiency

Article 12

Design of external reporting channels *must ensure*:

(a) ***Completeness***, ***integrity*** and ***confidentiality*** of information

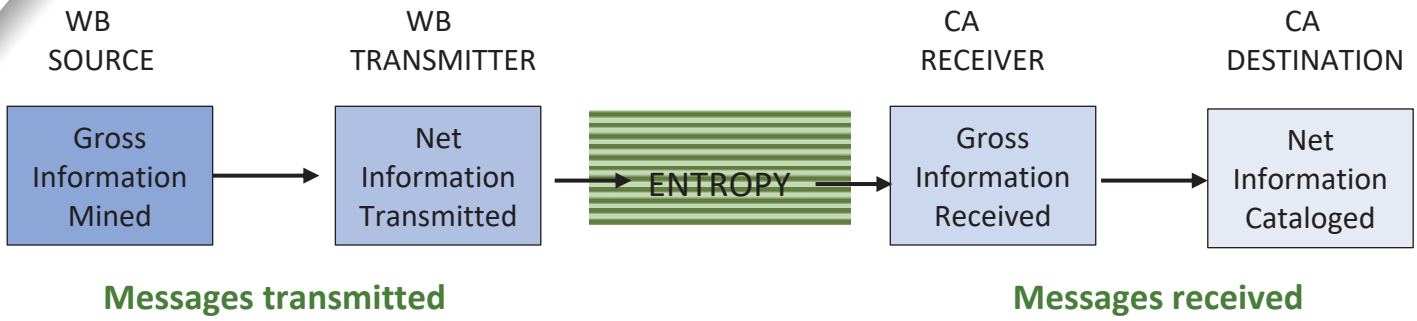
(b) ***Follow-up reporting*** by ***continuing contact*** and ***further information***

Article 13

Websites *must explain*:

(a) ***Confidentiality*** protections for WB
(b) ***Authorization to breach*** target confidentiality
(c) Availability of ***confidential advice***

C. DEFINITION OF OPERATIONAL SUCCESS: CREATION OF A HIGH EFFICIENCY INFORMATION CHANNEL



"Success" is *design of channels* maximizing *collection*, *storing* and *sharing* of corruption information

Article 11

Member States shall establish "external reporting channels"

- "to ***receive***, ***give feedback*** and ***follow up*** on reports"; and
- "***transmit*** *** the information" to "agencies of the Union"

Article 12

External reporting channels shall *** "enable ***the durable storage of information*** to allow further investigations"

Article 18

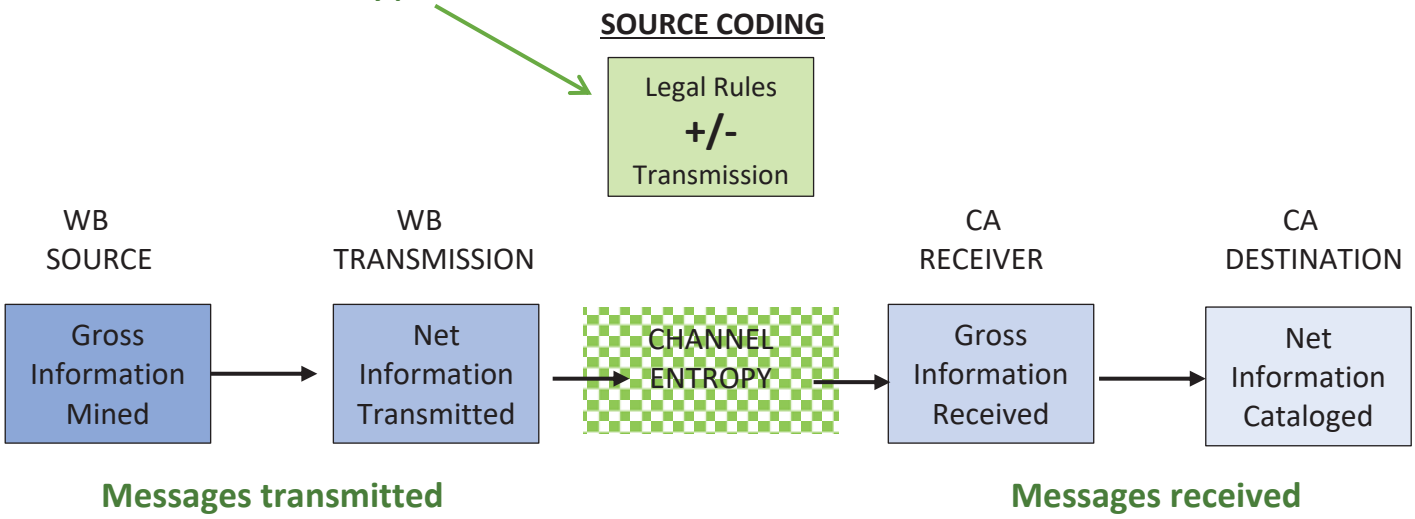
Member States shall ensure ***private and public*** sector authorities keep ***records of every report received***

D. POSITIVE SOURCE CODING TO REDUCE CHANNEL ENTROPY

"Channel coding"= Application of Rules Affecting Information Flow Positively or Negatively

(+) ***From EU Directive Information Rules***

- **WB Privilege to report**
- **Proprietary info not prohibited**
- **Inaccurate info is protected**
- **WB confidentiality protection**



Article 6 Conditions for protection of reporting persons

Reporting persons are protected if "they had reasonable grounds to believe that the ***information on breaches*** reported was ***true***" and "within the scope of this Directive"

Article 21 Measures for protection against retaliation

Reporting persons "shall not incur ***liability of any kind*** *** provided they had ***reasonable grounds to believe*** that the reporting *** of such ***information*** was necessary for revealing a breach"; and

"***shall not incur liability*** in respect of the acquisition of or ***access to the information*** *** provided that such acquisition or access did not constitute a self-standing criminal offence"

As to "information includ[ing] trade secrets, reporting or public disclosure shall be considered lawful"

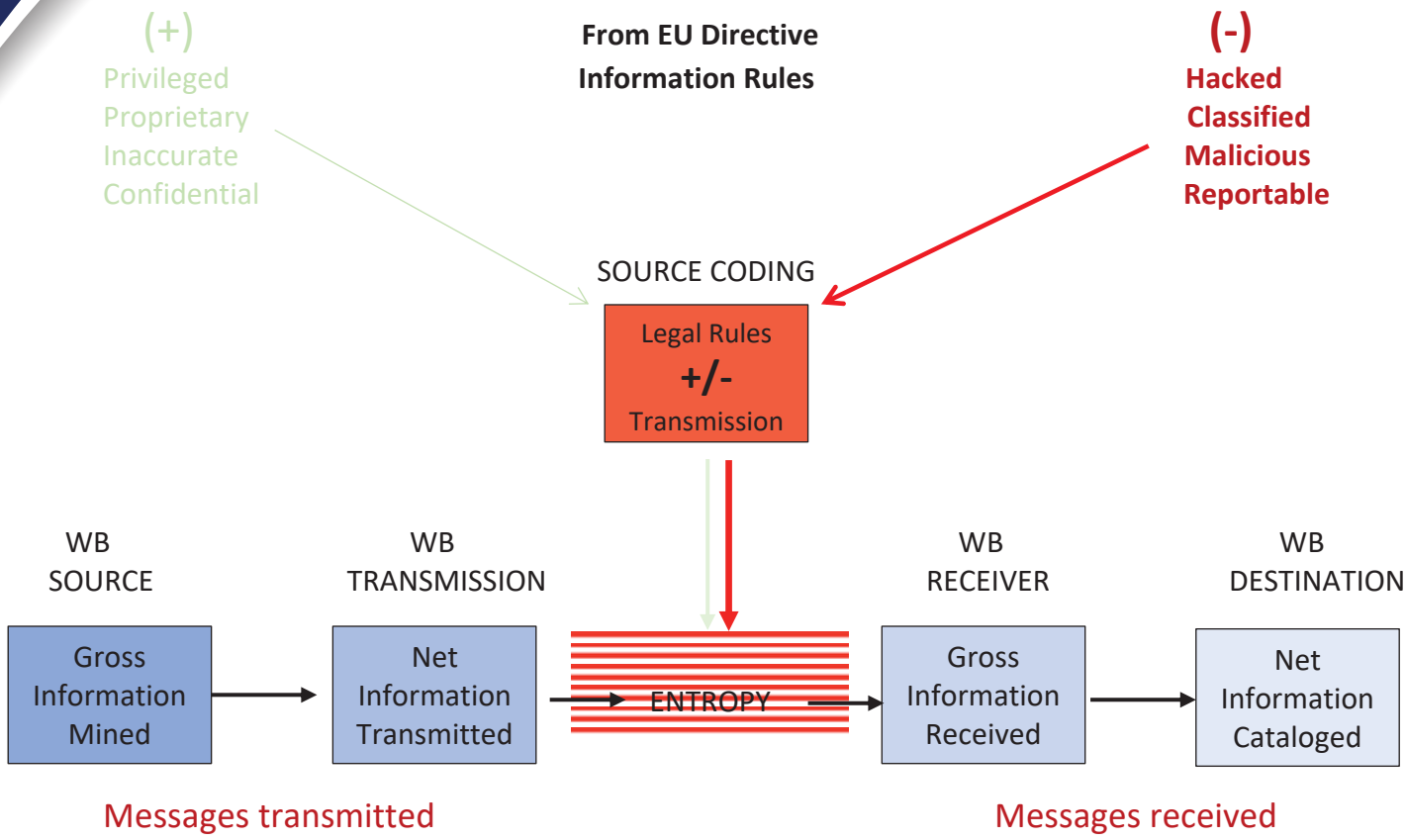
Article 16 Duty of confidentiality

"***The identity of the reporting person*** [shall not be] disclosed to anyone beyond the authorised staff members ", nor information from which identity "***may be deduced***"

Consideration (32)

"Protection is not lost where the reporting person reported ***inaccurate information*** on breaches by honest mistake, and "***motives*** of the reporting persons in reporting should be irrelevant"

E. NEGATIVE SOURCE CODING TO INCREASE CHANNEL ENTROPY



Article 3

This Directive shall not affect Union or national law of ***classified information***

Article 21

Information if acquisition or access constituted "***a self-standing criminal offence***"

Article 23

Member States shall provide for penalties for ***publicly disclosed false information***

Article 11

Member States can close ***repetitive reports*** lacking *meaningful new information*

Consideration (32)

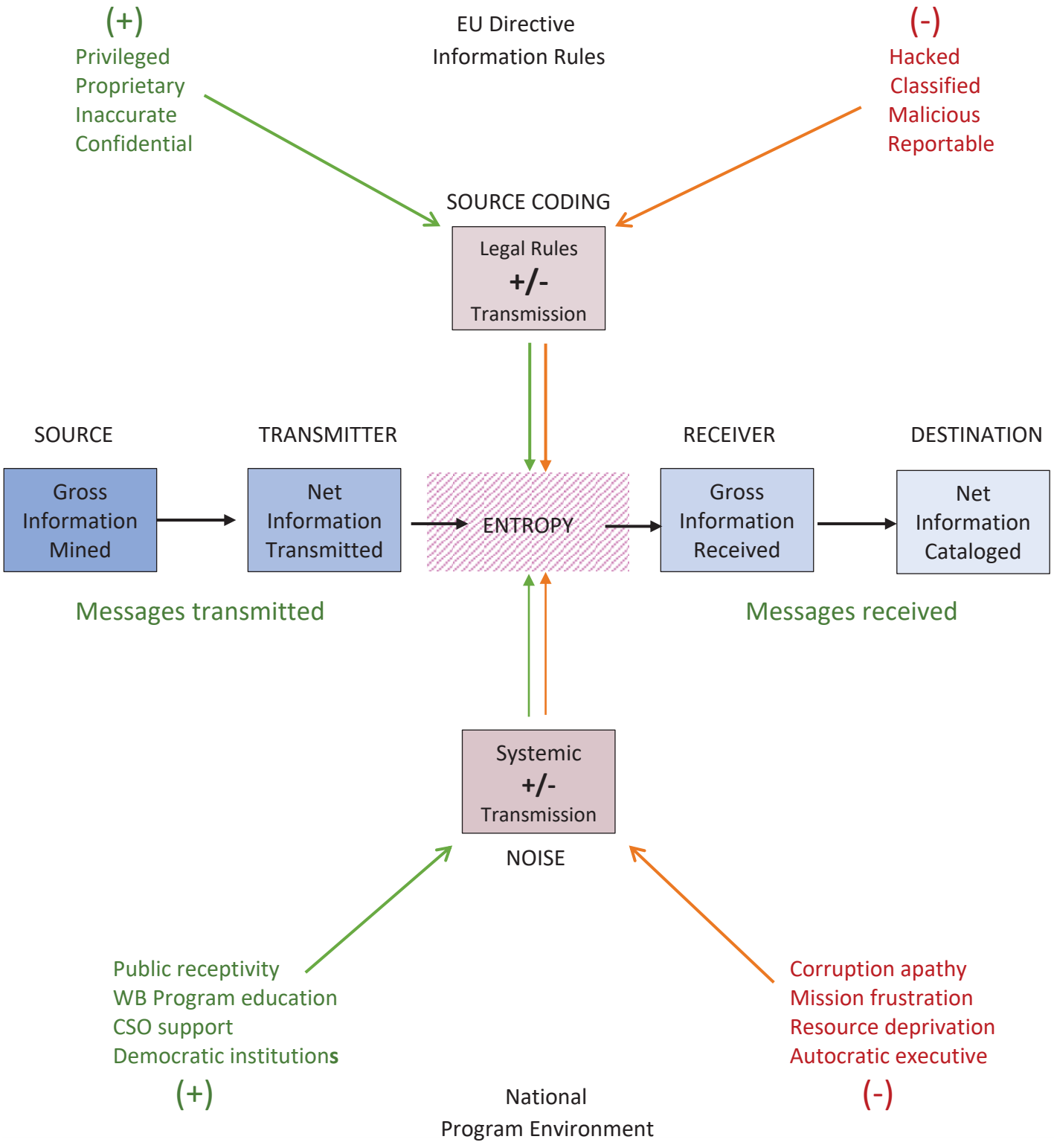
Need "safeguard against ***malicious and frivolous or abusive*** reports"

Article 16

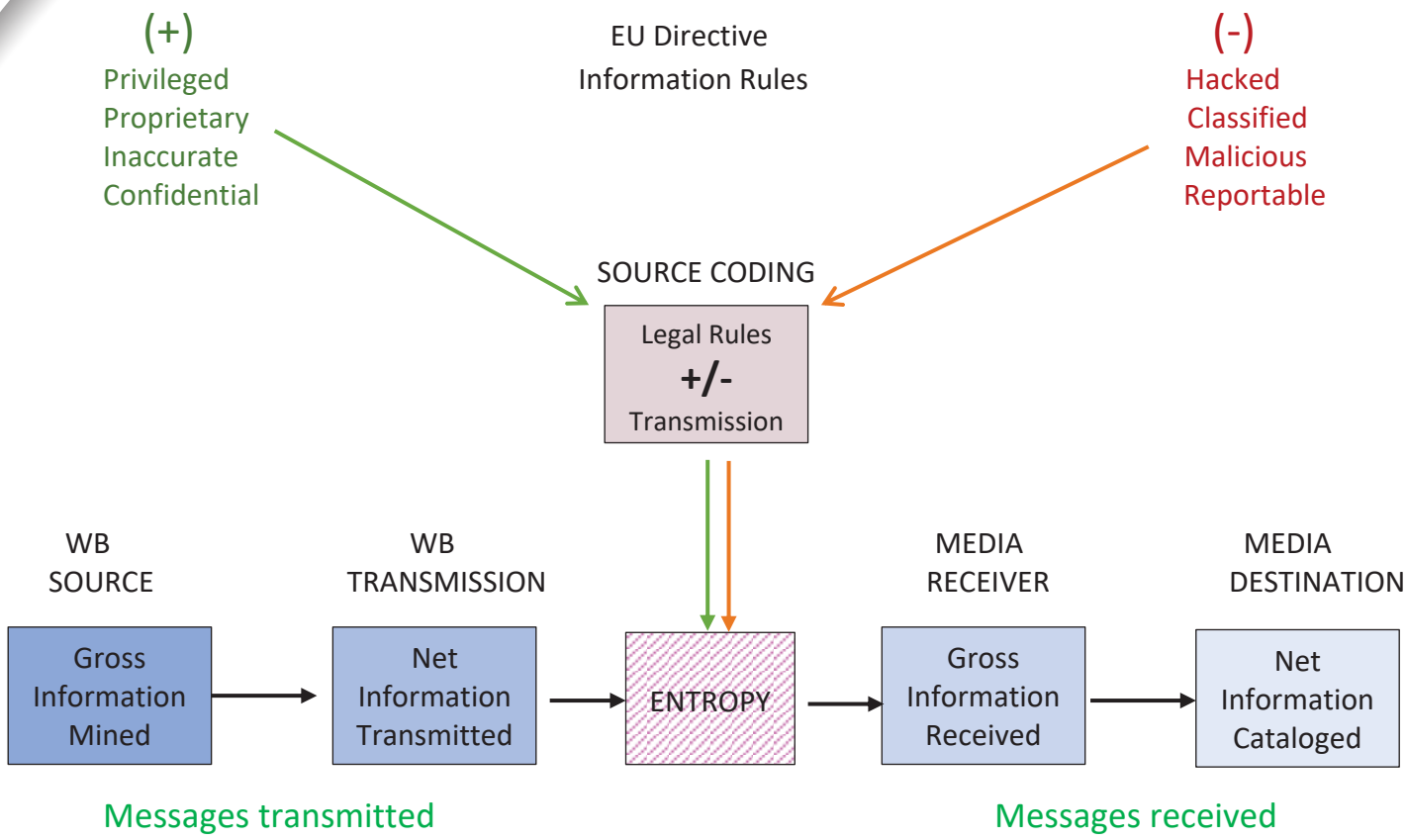
Identity disclosed for "Union or national law *** of investigations *** or judicial proceedings

F. POSITIVE AND NEGATIVE SYSTEMIC NOISE IN THE INFORMATION CHANNEL

"Noise" = non-coding background conditions affecting channel efficiency



G. INFORMATION THEORY PUBLIC CHANNELS AND THE MEDIA



Article 5 Definition

'Public disclosure' or 'to publicly disclose' means the ***making information available in the public domain***

Article 15

A *public disclosure* protected if "reasonable grounds to believe external reporting presents a ***risk of***: **(a)** retaliation **(b)** low prospect of being effectively addressed; (c) evidence may be concealed or destroyed; or (d) authority may be in collusion with the perpetrator

Consideration (31)

The ***right to freedom of expression and information*** in *the Convention for the Protection of Human Rights and Fundamental Freedoms*, encompasses the ***right to receive and impart*** information under freedom and ***pluralism of the media***.

XI. Appendix 1. Adapting Information Theory to the Management of Legal Information

Frontiers in Physics: Social Physics
(21 June 2021)

Quantifying Legal Entropy

Ted Sichelman

School of Law, University of San Diego, San Diego, CA, United States

(Reprinted excerpts with permission of the author and publication)

Many scholars have employed the term "entropy" in the context of law and legal systems to roughly refer to the amount of "uncertainty" present in a given law, doctrine, or legal system. Just a few of these scholars have attempted to formulate a quantitative definition of legal entropy, and none have provided a precise formula usable across a variety of legal contexts. Here, relying upon Claude Shannon's definition of entropy in the context of information theory, I provide a quantitative formalization of entropy in delineating, interpreting, and applying the law. In addition to offering a precise quantification of uncertainty and the information content of the law, the approach offered here provides other benefits. For example, it offers a more comprehensive account of the uses and limits of "modularity" in the law—namely, using the terminology of Henry Smith, the use of legal "boundaries" (be they spatial or intangible) that "economize on information costs" by "hiding" classes of information "behind" those boundaries. In general, much of the "work" performed by the legal system is to reduce legal entropy by delineating, interpreting, and applying the law, a process that can in principle be quantified.

Introduction

It goes without saying that the law and legal systems are uncertain to a significant degree. Several scholars (e.g., Katz and Bommarito [1]; Friedrich et al. [2]) have attempted to determine the uncertainty (and related complexity) of legal systems by formulating measures of the "entropy" of words in legal texts, including statutes and other legal authorities. Although measuring the ambiguity of words in texts can be valuable in many situations, it does not provide a comprehensive measure of the uncertainty in interpreting legal rules, much less a "system-wide" measure of the uncertainty of the law and legal system and subsystems more generally. Other scholars (e.g., Dworkin [3], Parisi [4, 5], Ruhl and Ruhl [6]) have focused their efforts on more general notions of legal entropy and related concepts, but have done little to nothing to formalize those notions in mathematical terms.

This article provides several important contributions to the literature by formalizing the notion of legal entropy. First, it offers a conceptual framework to quantify the entropy of legal systems that extends beyond legal text to capture how the law actually functions in real-world situations, including not only legal interpretation, but also the entropy and related information costs in formulating and applying the law. Second, although some previous works have foreshadowed the possibility of a quantitative description of legal entropy (e.g., D'Amato [7]), the formalization offered here provides a fully mathematical formulation as it applies to legal systems and disputes. Third, the mathematical model proposed here offers a potential template for how legal AI systems can measure and store information about the uncertainty of legal systems. Fourth, the model helps to explain more fully the nature and function of important concepts in the law, including the so-called "modularization" of the law and legal concepts, as proposed in the seminal works on the topic by Smith [8–10] and follow-on works by others (e.g., Newman [11]), as a well as the Coase Theorem [12] and the indeterminacy of legal rules [13].

The article proceeds as follows. Part 2 provides a brief background of the notion of entropy in physics and information theory, particularly Shannon's [14] formulation of information entropy. Part 3 describes previous attempts to describe legal entropy, including descriptive notions of legal entropy and measures of the word entropy found in legal texts. It explains the limitations inherent in these previous treatments. In Part 4, relying on Shannon [14] and the theoretical work of Hohfeld [15], it introduces a formal mathematical description of legal entropy, as it applies to a particular legal issues and disputes

as well as across legal systems and subsystems. Specifically, Part 4 proposes models for quantifying entropy in formulating and interpreting the law, as well as applying the law to a set of facts. In Part 5, the article applies its formal model to important theoretical and practical issues in the law, including legal indeterminacy, modularity, and the Coase Theorem. In so doing, it discusses practical problems in "measuring" legal entropy. Finally, the article concludes with some suggestions for further research.

Entropy in Physics and Information Theory

The concept of entropy in physics traces to the work of Clausius [16] in the mid-nineteenth century to describe a property of the transfer of heat, ΔQ, from a heat source at a certain temperature, T, to an idealized engine in a so-called reversible process.[1] In this situation, according to Clausius, the entropy of the system increases by ΔQ/T. Similarly, entropy decreases by such an amount when an idealized engine loses heat ΔQ to a heat sink at temperature T. In other words, as heat enters a thermodynamic system, entropy increases—particularly, if the system is cold, less if the system is already hot.

In the 1870s, Boltzmann [17] offered a molecular (i.e., microscopic) description of Clausius's notion of entropy. Specifically, Boltzmann [17] postulated that Clausius's macroscopic description of entropy could be explained in relation to microscopic states. Because heat at a macroscopic level is essentially a "disordered" collection of microscopic particles, the exact behavior or which is unknown at the macroscopic level, the entropy of the system can be viewed roughly as a measure of macroscopic disorder. As a cold system becomes hotter, its ordered, stable microscopic state of particles in fixed positions yields to a frenzy of quickly moving particles. Although in a classical system, the position and momentum of microscopic particles is measurable in principle, merely measuring the temperature and other macroscopic properties of a system would be insufficient to determine the precise position and momentum of each and every particle. As more heat enters a system, the more difficult it becomes to use macroscopic measures to determine the position and momentum of each particle that the system comprises. This increasing uncertainty results because the microscopic particles could be in a greater number of potential states (i.e., of position and momentum) in an increasingly hotter system than an increasingly colder system, where particles are relatively motionless. If a system is already hot, introducing a bit more heat increases the uncertainty of the microscopic states much less than if the system begins cold.

***

The Gibbs entropy is in effect a special case of a more general phenomena in which some "macroscopic" state of a generalized system, call it M, may be instantiated by W different "microscopic" states of the generalized system (Jaynes [20]). For instance, the "macroscopic" state of having 10 cents in one's hand can be instantiated by four "microscopic" states: (1) 10 pennies; (2) a nickel and 5 pennies; (3) two nickels; or (4) one dime. In other words, knowing the "macroscopic" state (here, the total monetary value) generally will be insufficient to specify the "microscopic" state (here, the precise coins used to achieve the total monetary value).
The greater the uncertainty in microscopic configuration, the greater the entropy.
***

Previous Treatments of Entropy in Legal Systems

Many scholars have applied the concept of entropy to legal systems. All of these treatments can be classified into two categories: (1) metaphorical uses of the concept of entropy; and (2) uses of formal mathematical and physical definitions to measure the "entropy" of legal texts.

Although the first category of scholarship (metaphor) can often be useful in thinking about the disorder, complexity, and uncertainty present in legal systems, it fails to offer any formal quantification of legal entropy. For instance, in a well-known article, Parisi [4] contends that real property is subject to a fundamental law of entropy that leads to increasing fragmentation of property interests, but fails to quantify the notion. Lewis [22] applies thermodynamic principles, including entropy, to the explain corporate reorganizations but, like other treatments, does not extend his notions beyond the level of metaphor. Ferrara and Gagliotti [23] purport to develop a conceptual "mathematical" approach to the law, including a notion that has "somewhat to do with the concept" of entropy in information theory, but their scheme is devoid of formal definition and thus reduces to metaphor. Ultimately, all previous treatments of the broad of concept of legal entropy (see also Berg [24], Edgar [25], Fromer [26], King [27], Moran [28], Stephan [29], as examples) fail to quantify the notion.[4]

Perhaps the treatment that comes closest to any quantification of legal entropy is that of D'Amato [7], who recognizes that entropy is at a maximum when the outcome of a legal dispute is equally likely for each part, further remarking that "[i]n order to use entropy in law directly, the legal scientist would have to embed the collection of predictions we call law into an abstract space that exhibited the variations in the level of uncertainty of the predictions." Yet, immediately following this insight, D'Amato [7] states that "Since law cannot be completely transcribed into words, it cannot be transcribed into symbols and spaces either." D'Amato's [7] statement is deficient in two important respects. First, to the extent one is concerned about the probabilities of outcomes in legal disputes, as is D'Amato [7], although it may be practically difficult to "transcribe" disputes into probability spaces, it is not impossible. Indeed, attorneys regularly the estimates the odds of winning and losing cases. Moreover, recent developments in legal artificial intelligence have vastly expanded the promise of more automated approaches to predicting legal outcomes (e.g., Katz et al. [32]; Branting et al. [33]). Second, aside from practical interest, it may be theoretically illuminating to devise mathematical models of the operation of the law. In this regard, such theoretical modeling is in turn arguably critical to practical advances in legal artificial intelligence.

The second category of articles relies on measures of entropy from computational linguistics and related fields, typically derived from Shannon [14, 34], to measure the uncertainty or ambiguity that is present in the text of statutes, regulations, and legal documents. For instance, Katz and Bommarito [1] measure legal complexity based on linguistic entropy present in U.S. federal statutes. In a similar vein, Friedrich et al. [2] examine the word and document entropy of opinions from the U.S. Supreme Court and the German Bundegerichtshof in order to measure and compare the textual ambiguity present in the courts' opinions.[5]

Although these text-based endeavors are important contributions to the literature, especially by formalizing previous metaphorical treatments, they are limited to what I term the "interpretive entropy" of legal systems—namely, the entropy and associated information costs involved in interpreting the law prior to its application to a particular set of facts. Moreover, because this scholarship tends to focus on the language of statutes and regulations, it measures only a portion of the interpretive entropy, because interpretation also involves the consultation of authoritative legal opinions, administrative interpretations, legislative and regulatory history, the text of other statutes and regulations, and not infrequently, general facts about the world (e.g., social norms, scientific facts, etc.).[6]

The present article adds to the literature by formalizing the metaphorical treatments in the first category. Like the articles examining the entropy of legal texts, it relies on formal mathematical and physical definitions, but it extends beyond the mere words of laws to provide more general, quantitative definitions of legal entropy.[7]

Formalizing Legal Entropy

This section relies on the work of Shannon [14], Hohfeld [15], and others to introduce a basic mathematical formalization of the entropy involved in the formulation, interpretation, and application of a law to a given set of facts involving a single legal actor, as well as system-wide entropy across multiple laws and facts concerning many legal actors. In so doing, it begins to overcome the theoretical limitations of the prior literature described earlier.

The Entropy of Legal Systems

As noted, although formal measures of the ambiguity of words in legal documents through measures of word entropy is useful to analyze and parse legal texts, it does not measure the entire extent of interpretive entropy, much less the entropy of legal systems more generally. Rather, one would like to quantify the ambiguity across the entire range of the formulation, interpretation, and application of particular laws to particular behavior.

For instance, the tax laws are notorious for being uncertain in delineation, interpretation, and application (Osofsky [37]). Regarding application, just small variations in the underlying facts relating to a particular tax provision can lead to large changes in the likelihood that the applicable legal actor is obligated to pay taxes or not. Similarly, patent infringement disputes are often difficult to predict, and like tax issues, are sensitive to small variations in the underlying law and facts (Sichelman [38]). Moreover, even if one can quantify the "entropy" of a particular application of law to facts involving a single legal actor, is it possible to quantify the entropy of a legal system and its subsystems encompassing many laws and many legal actors?

Thus, it becomes incumbent to conceptualize the different domains of entropy that arise in legal systems. *Delineative entropy* involves the ambiguity and related information costs in formulating the law in the first instance, typically into

written symbols, in a constitution, statutes, regulations, judicial decisions, and the like. As noted earlier, *interpretive entropy* concerns the ambiguity in interpreting the written symbols in legal documents, including not only constitutions, statutes, and regulations, but also judicial decisions. Such an endeavor is not merely textual in nature, but will often involve relying upon institutional and social norms, which themselves can be uncertain. Finally, *applicative entropy* is roughly the uncertainty involved in applying an interpreted law to a given set of facts.[8] Each type of legal entropy is considered in turn, along with a proposed formal quantification of each.[9]

***

Conclusion

Numerous legal scholars have discussed the notion of legal entropy, but few have attempted to quantify it. Those attempts to quantify the notion have been limited to analyzing the ambiguity of legal texts by measuring the entropy of words. Although certainly useful, these approaches fail to capture the multifaceted nature of legal entropy. In this article, relying upon the work of Shannon [14, 31] and Hohfeld [15], I have proposed the beginnings of a mathematical framework to quantify legal entropy more broadly. The model proposed offers several useful benefits. First, it offers a potential template for how legal AI systems can measure and store information about the uncertainty of legal systems. Second, the model helps to explain more fully the nature and function of so-called legal indeterminacy as well as the "modularization" of the law and Coasean notions of how transaction costs affect the allocation of legal entitlements. To be certain, the model fails to address important practical details concerning how to assess the underlying probabilities necessary to calculate legal entropy, but hopefully increasing advances in legal AI will lead to the wide-scale realization of such a model in the near future.

Footnotes

1. ^The discussion in this section is designed to offer a concise and simplified qualitative background of the notion of entropy in physics and information theory in order to set the stage for the following discussion of legal entropy, and thus should not be viewed as a precise technical account.

2. ^Because the log (AB) = log A + log B, by defining the entropy in terms of a logarithm (such as the natural logarithm), it becomes simpler to calculate entropy as the number of microstates increases, particularly when two systems are combined.

3. ^Another way to conceptualize Shannon entropy is in terms of "surprise," which typically is defined as the unlikelihood of an event occurring, i.e., 1/p [21]. Since the log (1/p) = –log *p*, we can rewrite Shannon entropy as proportional to the sum over states of $p_i \log_2(1/p_i)$. Thus, information entropy is driven by a combination of the logarithm of the level of surprise (i.e., improbability) of a given microstate and the probability of the microstate occurring, summed across all microstates.

4. ^Loevinger [30] cites Shannon and Weaver [31] and offers an "equation," which is best characterized as tongue-and-cheek. Namely, Loevinger [30] states: "The second law of sociodynamics is the law of the conservation of entropy. Entropy, in social as in physical phenomena, is a measure of disorder, uncertainty or confusion. The law of the conservation of entropy in sociodynamics states that the amount of entropy concerning any social problem remains constant regardless of the number of agencies or entities to which it is referred while the time required for decision or action on the problem increases in geometrical proportion to the number of agencies or entities whose concurrence is required. This law can be expressed as $T = NC^2$, where "W" is the time required for decision or action and 'NC' is the number of agencies or entities whose concurrence is required."

5. ^Other studies use legal documents as inputs and measure entropy unrelated to legal entropy. For instance, Zhang et al. [35] extend the application of Shannon entropy from text to patent indicators, including citation counts, number of patent families, and similar indicators, to measure the importance of particular patents in technological innovation. Although such approaches may be useful for determining the economic "information" content and, hence, the economic importance signified by a particular legal document, they do not measure legal entropy, that is, the uncertainty or ambiguity of a legal document or broader legal relation within the legal system.

6. ^As D'Amato [7] insightfully remarks, “For example, a statute that seemed to mean one thing may be construed by a court to mean something different. Although the court will usually say that it is clarifying the statute, it does not always do so. It may create an exception, an exemption, a privilege; it might construe the rule narrowly to avoid constitutional problems, or broadly to give effect to an unnoticed legislative intent buried in the legislative history. The court's decision becomes a part of the meaning of the rule, so that the rule now becomes more complex—it is a statute plus a judicial decision. The more complex rule may invite further adjudication and more inventive subsequent constructions by courts.”

7. ^Lee et al. [36] propose a statistical mechanics-based model of voting within groups using a maximum entropy model, applying it to the U.S. Supreme Court. This approach is more in the vein of political science than law per se and, as such, is somewhat orthogonal to the discussion here, but it could be useful in quantifying applicative entropy for disputes to be resolved by a group of adjudicators (e.g., on appeal).

8. ^In this regard, contracts also may be considered as a form of “private lawmaking” [39], subject to delineative, interpretative, and applicative entropy. In other instances, law may be formulated in unwritten ways, such as through oral tradition or even social symbols (e.g., Weyrach and Bell [40]), again, subject to all forms of legal entropy.

9. ^Another type of legal entropy is enforcement entropy, which stems from the uncertainty in the enforcement of a given law. I abstract away from enforcement entropy in this treatment for simplicity, but the same types of approaches discussed herein would apply to enforcement entropy (see generally Lederman and Sichelman [41]).

4. Powerpoint presentations

EPA OIG Whistleblower Training

Tom Devine, Legal Director
Government Accountability Project

I. WHAT IS THE GOVERNMENT ACCOUNTABILITY PROJECT?

- A tax-exempt, non-profit, non-partisan public interest organization that serves whistleblowers by providing them with legal representation against retaliation, legal representation to help make a difference through their disclosures, advocacy for stronger whistleblower protection rights, and training and education in those rights.

II. WHO ARE "WHISTLEBLOWERS"?

- Legally, they are employees or applicants who disclose information that they reasonably believe evidences illegality, gross waste, gross mismanagement, abuse of authority or a substantial and specific danger to public health or safety.

- In non-legalese, these are employees who exercise free speech rights to challenge abuses of power that betray the public trust.

III. HOW WHISTLEBLOWERS CAN HELP OFFICES OF INSPECTOR GENERAL

From GAP's experience, examples include –

- Bearing witness through testimony
- Identifying witnesses to question, and relevant documents or other evidence to seek
- Navigating where to find the evidence
- Making backup copies of key evidence, to produce when a target asserts it doesn't exist.
- Serving as a human dictionary and encyclopedia to analyze technical evidence and demystify agency or professional jargon
- Explaining the value of evidence whose significance may be camouflaged without understanding of circumstances or consequences.

III. HOW WHISTLEBLOWERS CAN HELP OFFICES OF INSPECTOR GENERAL (Cont.)

- Finding the evidentiary needle in the haystack when a target floods the investigation with irrelevant information.
- Intelligence gathering for law enforcement to stay a step ahead of the target, by attending and reporting on agency meetings.
- Flushing out previews of potential bad faith alibis by raising pre-identified issues at agency meetings.
- Helping to develop questions of agency witnesses, through personal and professional knowledge
- Matchmaking with other whistleblowers to sustain and increase the flow of evidence
- Monitoring follow up corrective action commitments

IV. RELATIONSHIPS: THE NORTHWEST PASAGE BETWEEN WHISTLEBLOWERS' POTENTIAL AND REALITY

- If you earn their trust, they will open up.
- Start by opening up yourself, sharing your background, history of successful cases, and why this one matters to you. Consider these lessons learned from GAP's experience:

IV. REL TIONSHIPS (Cont.)

1. Honor all commitments, from scheduling to substantive, or provide advance notice if they must be adjusted.
2. Be clear about confidentiality from the beginning, from witness rights to their limits.
3. Be clear about what protection you can provide, and what you cannot to prevent later charges of betrayal.
4. Proactively shield witnesses with advance warnings to employer of zero tolerance for retaliation, which will create a presumption of misconduct on associated charges.
5. Make their protection a visible priority for whistleblowers so they feel the relationship is a two way street, rather than being mere "evidence objects" who will be abandoned after no longer needed.

IV. REL TIONSHIPS (Cont.)

6. Provide a safe environment for interviews and communications. Interviews in an agency office can be viewed as bad faith.
7. Engage in active listening during interview. Feeling heard is significant to open up further.
8. Engage in visible quality control. Even if there will not be an affidavit, have the whistleblower read and confirm that the report of interview is accurate. They must agree that they said what you say they did.
9. Enfranchise the whistleblowers in the larger context by asking their opinions and brainstorming with them. They may have more to offer than expected/ previously realized.

IV. RELATIONSHIPS (Cont.)

10. If trust with the pioneer has been established, network to expand the scope of witnesses. Sometimes a community will form around support for the investigation, which means you almost certainly will crack the case.

11. Sustain the relationship. Following through can earn a steady stream of new issues and updated evidence.

12. Set an example at the OIG. Restore climates of respect for whistleblowing and zero tolerance within OIG's, where incidents of internal retaliation cases have been too common. Credibly implement the Whistleblower Ombudsman requirement of the Whistleblower Protection Enhancement Act.

Use us!

- GAP is a resource for informal or volunteer assistance in formal or informal training to help work more effectively with whistleblowers, particularly through implementing WPEA Ombudsman requirements.

- For more information, contact Shanna Devine, shannad@whistleblower.org, 202-457-0034, ext. 132; or Tom Devine, tomd@whistleblower.org, 202-457-0034, ext. 124.

This project is funded by the European Union

REGIONAL ANTI-CORRUPTION INITIATIVE

Breaking the Silence:

Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

Lifecycle of a Whistleblower Case: From Report to Resolution

This project is funded by the European Union

Breaking the Silence:

Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

Report of workplace retaliation

- The most important things:
  - anticipated risks vs. rewards
  - anticipated costs vs. benefits
- Is the person an employee?
  - if yes, what is the person's position and status?

This project is funded by the European Union

Breaking the Silence:

Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

Report of workplace retaliation

- Advice on reducing / eliminating risks
- Has retaliation already happened?
- Legal options?
- Is mediation possible? / confront employer

This project is funded by the European Union

Breaking the Silence:

Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

Report of workplace retaliation

- Take the burden off
- Basic emotional support (not therapy)
- Help the person to move on
  - don't become an investigator or crusader

This project is funded by the European Union

Breaking the Silence:

Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

'Proving Retaliation': Timing + Knowledge

- What was the timing of the action against the employee?
- Who had knowledge of the action against the employee?

This project is funded by the European Union

Breaking the Silence:

Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

Circumstantial evidence

- workplace / public humiliation
- silencing the employee
- mobbing / colleagues ganging up on the employee

This project is funded by the European Union

Breaking the Silence:

Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

Circumstantial evidence

- cover up the wrongdoing via conflict-of-interest – are criminals doing the investigation?
- discriminatory treatment – whistleblower vs. other employees
- disparate treatment – pre-whistleblowing vs. post-whistleblowing

This project is funded by the European Union

Breaking the Silence:

Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

Circumstantial evidence

- ignoring the whistleblower's concerns
- investigate employee as a distraction / find ammunition to dismiss the person ('witch-hunt')
- motive to retaliate – is the whistleblower a threat to managers and/or the organization?

This project is funded by the European Union

Breaking the Silence:

Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

Hard Truths

- Almost always some type of retaliation – unless whistleblower is anonymous
- Almost no cases are simple – is much more of an art than a science
- Very few public agencies can order reinstatement and compensation

This project is funded by the European Union

Breaking the Silence:

Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

Hard Truths

- Conflicts of interest / ineffectiveness of 'internal reporting channels'
- Court battles – long, expensive, uncertain
- Too many legitimate whistleblower disclosures are not investigated and prosecuted

This project is funded by the European Union

Breaking the Silence:

Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

Hard Truths

- Media exploitation, oversimplification, lack of foll0w-up
- Biggest barriers:
  - instinctual bias / bystander effect
  - conflicts of interest / political & business elites

This project is funded by the European Union

Breaking the Silence:

Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

Hardest Truths

- Almost never can you change the world
- Usually you have to take what you can get
- There is almost always some damage
- ‘Whistleblower Identity Syndrome’

Breaking the Silence: Enhancing Whistleblowing Policies and Culture in the Western Balkans and Moldova

Activity Status

Annual Meeting of the SEE Coalition on Whistleblower Protection
19 November, 2021, Sarajevo, Bosnia and Herzegovina

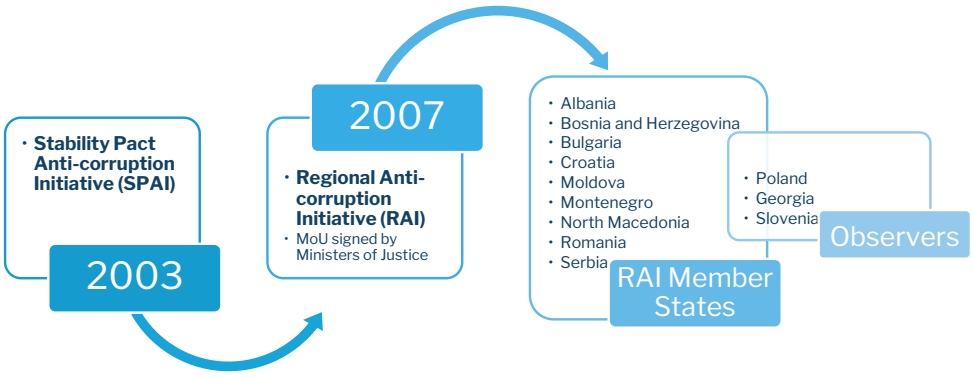
This project is funded by the European Union

Breaking the Silence:

Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

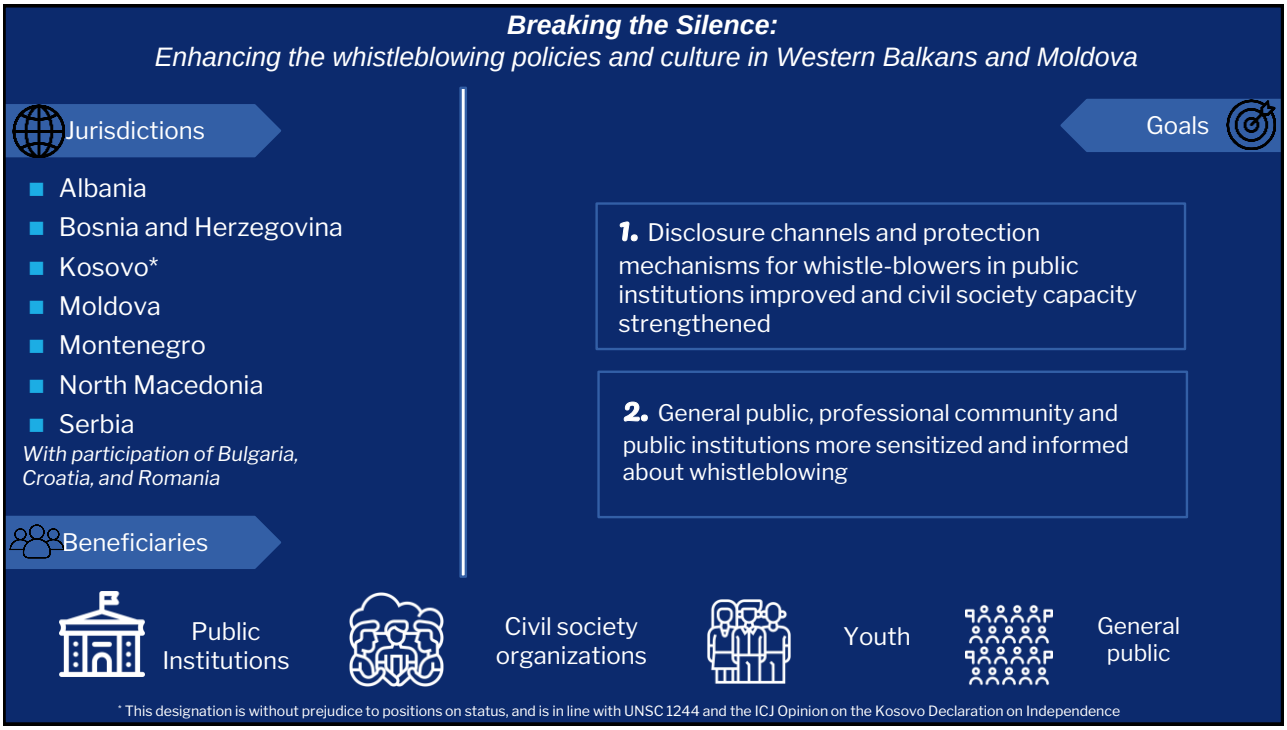
REGIONAL ANTI-CORRUPTION INITIATIVE (RAI)

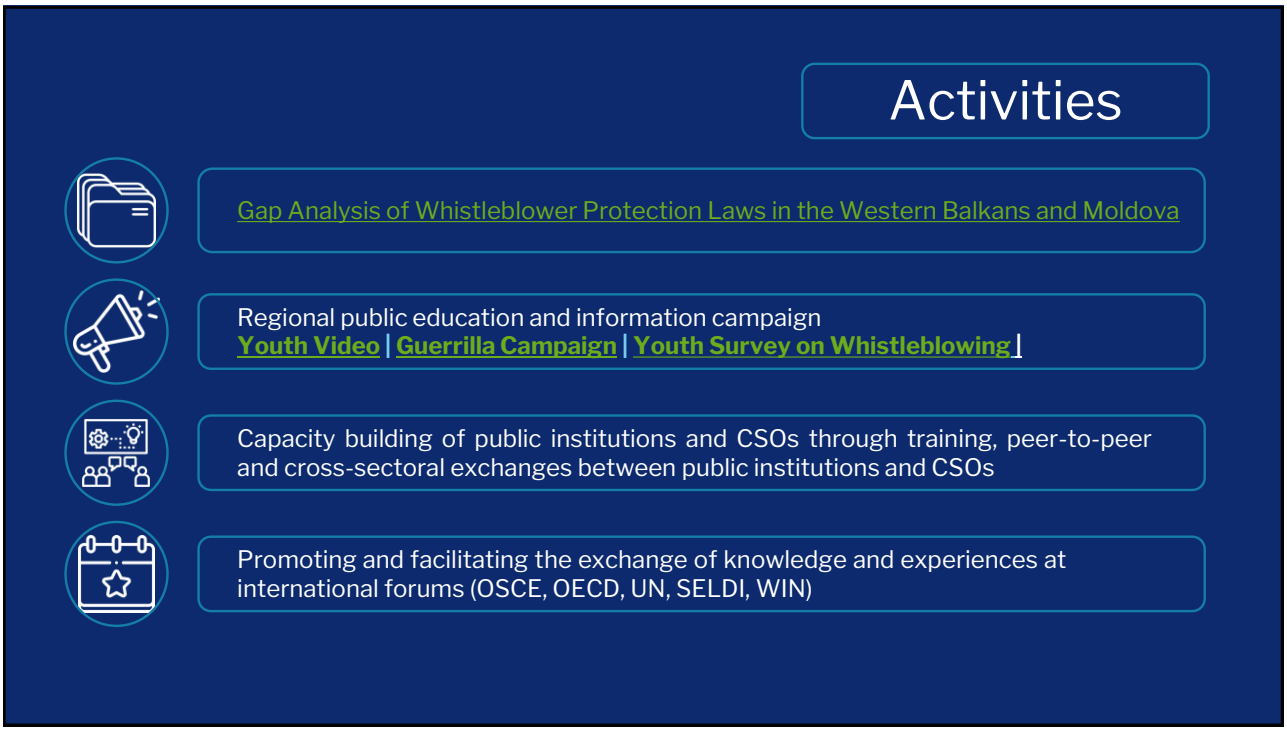


RAI MISSION

Enhance regional cooperation in the fight against corruption

Support and strengthen the capacity of countries in anti-corruption efforts


Breaking the Silence:
Enhancing the whistleblowing policies and culture in Western Balkans and Moldova
Jurisdictions
Albania
Bosnia and Herzegovina
Kosovo*
Moldova
Montenegro
North Macedonia
Serbia
With participation of Bulgaria, Croatia, and Romania
Goals
1. Disclosure channels and protection mechanisms for whistle-blowers in public institutions improved and civil society capacity strengthened
2. General public, professional community and public institutions more sensitized and informed about whistleblowing
Beneficiaries
Public Institutions
Civil society organizations
Youth
General public
* This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration on Independence


Activities
Gap Analysis of Whistleblower Protection Laws in the Western Balkans and Moldova
Regional public education and information campaign
Youth Video | Guerrilla Campaign | Youth Survey on Whistleblowing
Capacity building of public institutions and CSOs through training, peer-to-peer and cross-sectoral exchanges between public institutions and CSOs
Promoting and facilitating the exchange of knowledge and experiences at international forums (OSCE, OECD, UN, SELDI, WIN)

GAP ANALYSIS METHODOLOGY

- assesses to what extent each of 21 key standards, extracted from the CoE Recommendation and the EU Directive, are incorporated in the whistleblower protection laws of the Western Balkans and Moldova
- highly consultative development process, with valuable inputs provided by representatives of public institutions (anticorruption agencies, ministries of justice)
- gaps in statutory provisions were identified and recommendations for improvement developed for each jurisdiction
- foundation for follow-up advocacy, capacity building and public awareness activities toward improving whistleblower policies and systems

This project is funded by the European Union

Breaking the Silence:
Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

GAP ANALYSIS FINDINGS
Legislative and Institutional Framework Strengths

1. Most of the whistleblower protection laws in the Western Balkans and Moldova adequately incorporate the following key whistleblower protection international standards:
- the applicability of the whistleblower protection law to both public and private sector corruption;
- designated reporting channels;
- designated reporting persons/government institutions for whistleblower reporting and protection;
- a broad statement of whistleblower rights;
- broad scope of protection from all forms of harassment;
- guarantee of whistleblower confidentiality.

2. More recent laws better incorporate the developing international standards on whistleblower protection:
substantial compliance with the EU Directive – the laws of Kosovo*, and Serbia;
partial compliance with the EU Directive - the laws of Albania, Montenegro, North Macedonia, and the BiH entity of Republika Srpska.
inadequate compliance - the state law of BiH, the law of Brcko District of BiH, and the law of Moldova.

3. There is some practical experience and insight into which legislative solutions work and which don't work in practice.

This project is funded by the European Union

Breaking the Silence:
Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

GAP ANALYSIS FINDINGS
Legislative and Institutional Framework Weaknesses

The following key international standards are inadequately incorporated in the laws:

1) types of misconduct that may be reported under the law;
2) the scope of protection for all potential whistleblowers with significant evidence;
3) the "reasonable grounds to believe that the reported matter is true" standard for whistleblower disclosures (vs. good faith/motive test);
4) the protection of whistleblower disclosures made to the public;
5) clarity and accessibility for anti-retaliation protection;
6) relief through legal remedies;
7) reverse burden of proof on employers to show actions taken against employees are not linked to whistleblowing;
8) penalties for retaliation and other actions;
9) the protection of whistleblower against civil and criminal liability;
10) credible reporting channels that enfranchise whistleblowers to follow up on reports; and
11) transparency of the law's results, in terms of impact from whistleblowing reports and effectiveness against retaliation.

This project is funded by the European Union

Breaking the Silence:
Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

This project is funded by the European Union

Breaking the Silence:

Enhancing whistleblowing policies and culture in the Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

FINDINGS/CHALLENGES

Institutional Capacity

1. Resources:

- anticorruption agencies, as external whistleblower reporting mechanisms, lack sufficient human and other resources (case management system, specialized training) and struggle to effectively collaborate with bodies in charge of the investigation into the reported wrongdoing.

- other public institutions (health and education sector) which play a role in whistleblowing enforcement received ad hoc specialized training on whistleblowing, following the adoption of whistleblower protection law. There is a need for educational material and continuous training to persons who handle WB reports, but also employees on whistleblower reporting procedures (internal and external) and whistleblower rights.

2. **professional qualifications** of staff handling whistleblower reports and retaliation cases are insufficient.

3. several of the public agencies reported that they **do not have designated staff to focus solely on whistleblower reports and retaliation complaints**. In some agencies, any number of people may be in the position to take a case or handle a report (risk from inconsistency)

This project is funded by the European Union

Breaking the Silence:

Enhancing whistleblowing policies and culture in the Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

FINDINGS/CHALLENGES

Institutional Capacity

No jurisdiction includes complete and adequate information on whistleblower cases in their annual reports. Without complete public information, citizens will not have full confidence that the system is working on their behalf, and they will continue to be reluctant to make a report.

1. **Albania:** 14 WB cases before HIDAACI (2019)
2. **BiH:** 24 WB cases before APIK (2014-2020)
3. **Kosovo*:** 5 WB cases before ACA, 142 WBer reports filed through internal channels (2020)
4. **North Macedonia:** 19 WB cases before SCPC (2018-2020), 59 WBer reports filed through internal channels (January-June 2019)
5. **Moldova:** 0 WB cases before NAC (2020)
6. **Serbia:** 117 WB protection cases before all courts (2020)
7. **Montenegro:** 75 cases before ACA (2020).

This project is funded by the European Union

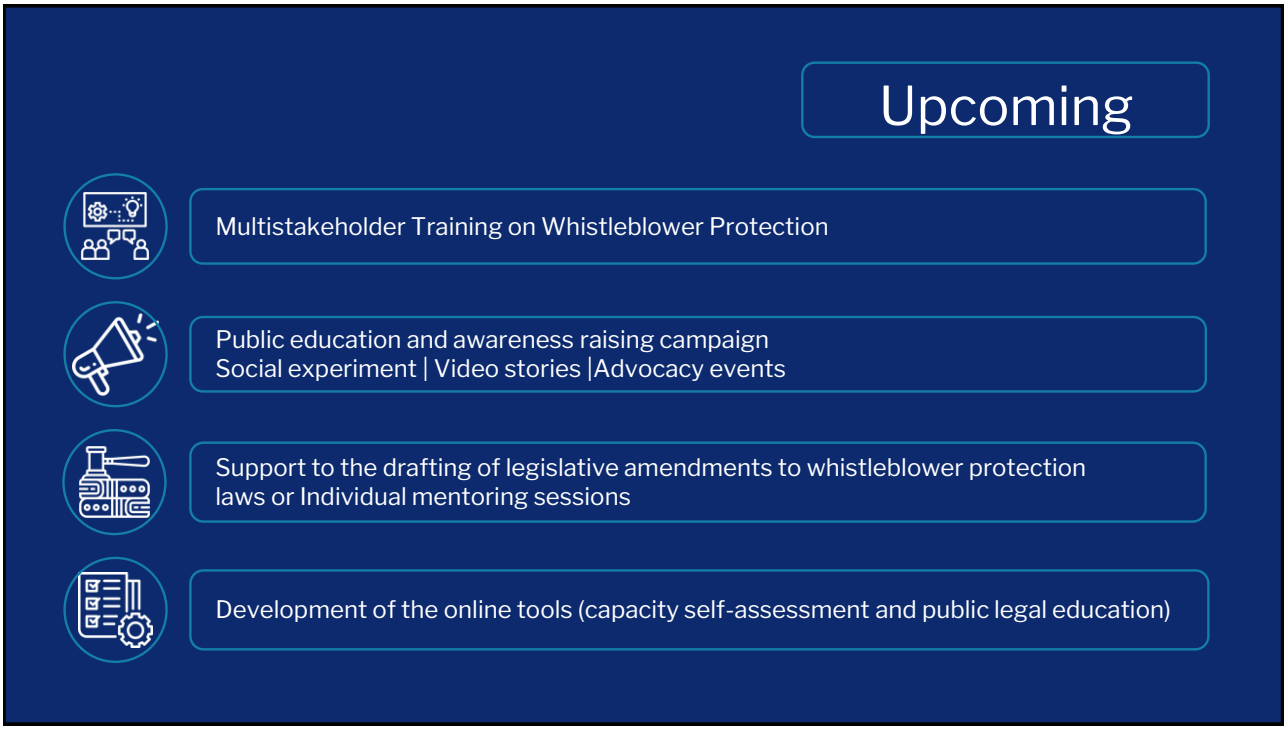
Breaking the Silence:

Enhancing whistleblowing policies and culture in the Western Balkans and Moldova

REGIONAL ANTI-CORRUPTION INITIATIVE

CSO Activity

- RAI Project Team identified 41 NGOs, which have been involved in whistleblower protection in the beneficiary jurisdictions.
- The number of participating CSOs in the project events varied from 18 in the Annual Meeting of the SEE Coalition on Whistleblower Protection (November 2020) to 22 in the First and Second Annual Multi-Beneficiary Training on Whistleblower Protection (February and November 2021).
- NGOs involved in whistleblower protection reported following activity: advocacy for legislative improvements, the monitoring of the implementation of laws, provision of alternative whistleblower reporting channels, whistleblower support and legal aid, as well as training for public institutions.


Upcoming
Multistakeholder Training on Whistleblower Protection
Public education and awareness raising campaign
Social experiment | Video stories |Advocacy events
Support to the drafting of legislative amendments to whistleblower protection laws or Individual mentoring sessions
Development of the online tools (capacity self-assessment and public legal education)

pištaljka.rs

What Happens with Whistleblowers' Reports: Serbia Case Study

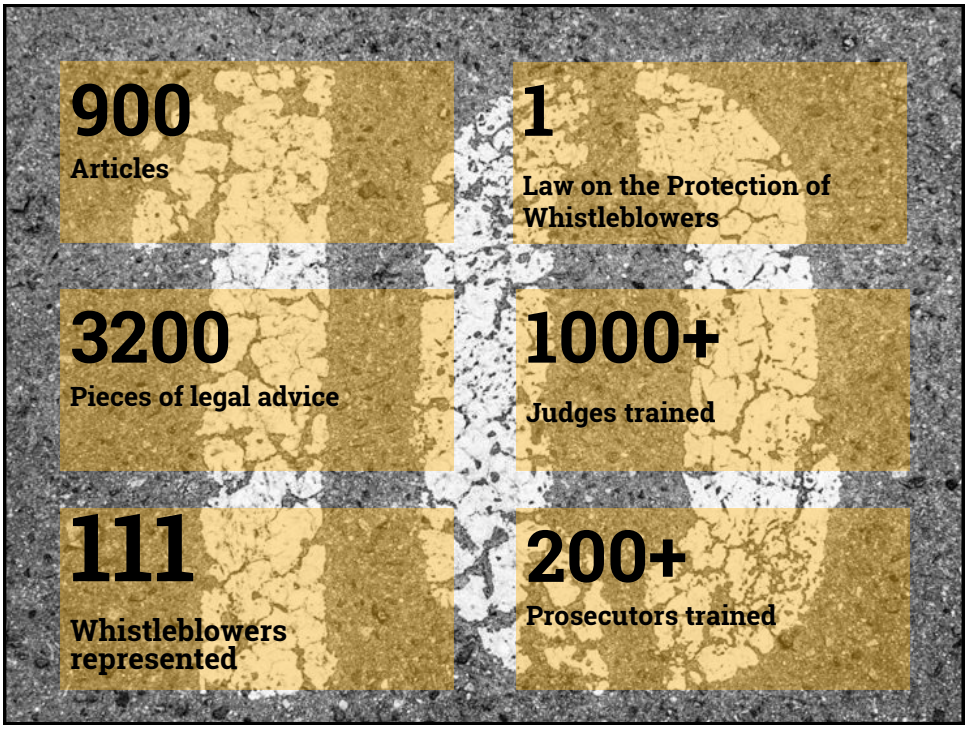
Vladimir Radomirović
editor-in-chief
Pištaljka

This project is funded by the European Union

Breaking the Silence:
Enhancing the whistleblowing policies and culture in Western Balkans and Moldova

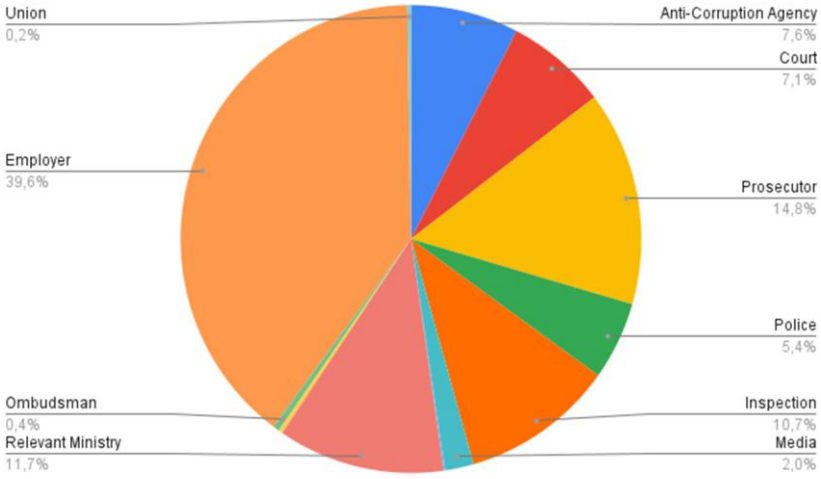
REGIONAL ANTI-CORRUPTION INITIATIVE

About Pištaljka


900
Articles
1
Law on the Protection of Whistleblowers
3200
Pieces of legal advice
1000+
Judges trained
111
Whistleblowers represented
200+
Prosecutors trained


Legal Advice Service
pištaljka.rs

Who whistleblowers go to



What would you do?


Tomislav Veljković
Reported corruption and waste of public funds in the town of Rača


Mika's Investigation
September, 2021

What would you do?

Darko Nenadić

Reported toxic water in the town of Požarevac

Prosecutors have launched an investigation (finally)

What would you do?


Divna
Sakradžija
Reported head of local administration over falsified CV


What would you do?

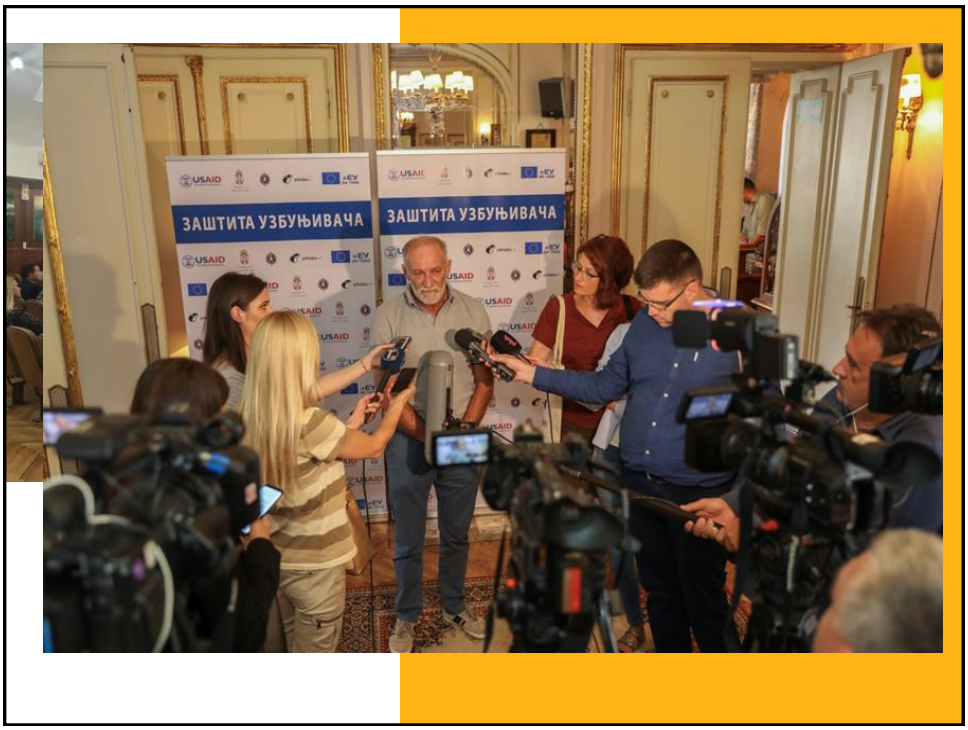
Borko Josifovski

Reported that medical teams were taking bribes from funeral homes

What would you do?

Milenko Jovanović

Reported manipulation of air pollution data



Thank you

pištaljka.rs

5. READING MATERIALS FOR FUTURE REFERENCE

Second Annual Regional Multi-Beneficiary Training on Whistleblower Protection

Day 1, November 17, 2021

1. *Study 'Are whistleblowing laws working?': https://www.ibanet.org/MediaHandler?id=49c9b08d-4328-4797-a2f7-1e0a71d0da55*
2. *EU Directive: https://eur-lex.europa.eu/eli/dir/2019/1937/oj*
3. *ECtHR Case Halet vs. Luxembourg. a whistleblower who disclosed tax documents: no violation of the Convention*
4. *Case Whitmore v. Department of Labor, the key U.S. decision on assessing whether an employer's reasons are pretext or truly independent justifications, the issue for reverse burden of proof: https://scholar.google.com/scholar_case?case=26595367592208816&hl=en&as_sdt=6&as_vis=1&oi=scholarr*

Day 2, November 18, 2021

5. *'The Red Flags', Excerpts from Whistleblower's Survival Guide on Retaliation Tactics*
6. *Case Department of Homeland Security v. MacLean, in which the U.S. Supreme Court clarified and upheld the standards for public freedom of expression: https://www.supremecourt.gov/opinions/14pdf/13-894_e2qg.pdf*

5.1 CASE OF HALET v. LUXEMBOURG (Application no 21884_18) JUDGMENT Art 10

THIRD SECTION

CASE OF HALET v. LUXEMBOURG

(Application No. o 21884/18)

STOP

Art 10 • Freedom of expression • 1000 EUR of criminal fine for having leaked confidential documents from his private employer to the media ("Luxleaks"), without sufficient public interest to weigh the damage caused • *A priori* whistleblower within the meaning of the Court's case-law • Proportionality of the sanction • Fair balance struck between the interests involved by a detailed analysis of the domestic courts

STRASBOURG

May 11, 2021

Referral to the Grand Chamber

09/06/2021

This judgment will become final under the conditions defined in Article 44 § 2 of the Convention. It can undergo retouching.

HALET v. LUXEMBOURG

In the case of Halet v. Luxembourg,

The European Court of Human Rights (third section), sitting in a Chamber composed of:

Paul Lemmens, *president,*
Georgios A. Serghides,
Georges Ravarani,
María Elósegui,
Darian Pavli,
Anja Seibert-Fohr,
Peeter Roosma, *judges,*

and Milan Blaško, *Section Registrar* ,

Seen :

the application (no ₀ 21884/18) against the Grand Duchy of Luxembourg and of which a French national, Mr. Raphaël Halet ("the applicant") seized the Court under Article 34 of the Convention for the Protection of Human Rights man and fundamental freedoms ("the Convention") on May 7, 2018,

the decision to inform the Luxembourg government ("The Government") the complaint concerning Article 10 of the Convention and to declare the remainder of the complaint inadmissible,

the observations communicated by the respondent government and those communicated in reply by the applicant,

the comments received from the association "House of whistleblowers", that the president of the section to which the case had originally been assigned had authorized to act as a third party intervenor,

Noting that the French government, invited to present if it so wished, had having regard to the applicant's nationality, written observations (Articles 36 § 1 of the Convention and 44 of the Rules), indicated that he did not intend to take advantage of their right to intervene,

After deliberating in the council chamber on March 30, 2021,

Delivers the following judgment, adopted on that date:

INTRODUCTION

1. The application concerns, under Article 10 of the Convention, the criminal conviction of the applicant in the so-called case *"Luxleaks* ", by refusing him the justification of the whistleblower.

IN FACT

2. The applicant was born in 1976 and lives in Viviers. He was represented by M e C. Meyer, lawyer practicing in Strasbourg.

3. The Luxembourg government ("the Government") has been represented successively by an *ad hoc* appointed agent , Mr. Christophe Schiltz, Head of the Legal Department of the General Secretariat

to the Ministry of Foreign Affairs, then by its agent, Mr. David Weis, of the Permanent Representation of Luxembourg to the Council of Europe.

I. THE CONTEXT OF THE CASE

4. The complainant was employed by *PricewaterhouseCoopers.* ("PwC"), which provides auditing, tax advisory and advisory services in business management.

PwC's activity consists in particular of preparing tax returns in the name and on behalf of its clients and to request from the tax administration of advance tax rulings. These decisions, which concern the application of the tax law to future transactions, are called " *Advance Tax Agreements* " (abbreviated as " *ATAs* ") or " *rulings*

tax ”or even“ tax rulings ”. They will be referred to below as tax rulings.

5. The complainant states that, while employed by PwC, he coordinated a team of five and did not occupy a minor position but, on the contrary, a position at the heart of PwC's activity which consisted of obtain, for its customers, the best possible treatment by the administration Luxembourg tax. This description is questioned by the Government which, based on the observation that the judges of the merits in the case indicates that, at the material time, the applicant was administrative agent functions which consisted in collecting, centralizing, scan, save and send the declarations to the customers concerned tax.

6. Between 2012 and 2014, several hundred tax rulings and PwC tax returns were published in various media. These publications highlighted a practice, over a period extending from 2002 to 2012, very advantageous tax agreements concluded between PwC on behalf of multinational companies and tax authorities Luxembourgish.

7. An internal investigation conducted by PwC established that an auditor, AD, had copied, on October 13, 2010, the day before his departure from PwC following his resignation, 45,000 pages of confidential documents, including 20,000 pages of tax documents corresponding in particular to 538 tax rulings, which he had submitted in summer 2011 to a journalist, EP, at the latter's request.

8. A second internal investigation carried out by PwC identified the applicant. The latter had, following the revelation by the media of some of the tax rulings copied by AD, contacted EP in May 2012 in with a view to proposing the delivery of other documents. This discount, finally accepted by the journalist, took place between October and December 2012 and brought on sixteen documents, comprising fourteen tax declarations and two

accompanying letters. Some of the documents were used by the journalist as part of a second TV show " *Cash Investigation* ”broadcast on June 10, 2013, one year after the broadcast of the first. On November 5 and 6, 2014, the sixteen documents were also

posted online by an association of journalists called " *International Consortium of Investigative Journalists* " (" *ICIJ* "). This publication was qualified by its authors of " *Luxleaks* ". It appears from articles press that the *Luxleaks* affair generated "a difficult year" for PwC, but that, after this year, the firm experienced a growth in its turnover business that went hand in hand with a significant increase in its workforce.

II. PENAL PROCEDURES INITIATED

9. Upon complaint from PwC, AD, the applicant and EP were indicted by a investigating judge and sent back by the investigating court to the Luxembourg district court.

A. The first instance judgment

10. On June 29, 2016, the Luxembourg district court, ruling in correctional matters, sentenced AD and the applicant for theft domestic, fraudulent access to a processing or transmission system automated data, breach of trade secret, breach of confidentiality professional and money laundering-detention.

11. AD was sentenced to imprisonment for twelve months, with full stay, and a fine of 1,500 euros (EUR). the the applicant was sentenced to nine months' imprisonment, with full stay, and a fine of EUR 1,000. They were in in addition ordered to pay to PwC, as civil compensation for the damage moral, the amount of a symbolic euro, to which this civil party had limited its demand.

12. EP was acquitted on the ground that he had not participated within the meaning of the law, as a co-perpetrator or accomplice, to the violation by the applicant of the secrecy business and professional secrecy.

B. The judgment of the Court of Appeal

13. AD and the applicant appealed in criminal and civil proceedings against this judgement. The public prosecutor lodged a criminal appeal against AD, the applicant and EP

14. On March 15, 2017, the Court of Appeal of the Grand Duchy of Luxembourg halted.

15. Prior to its analysis of the merits of the case, the Court of Appeal had the opportunity to note that "[t] he public denunciation [on the part of the

applicant], by the communication of tax returns [of companies multinationals], falls within the framework of the tax practice of tax rulings favorable to multinationals, initially denounced by [AD] ". In this same context, it also stated that "the legality or the illegality of the disclosed act or conduct is not, depending on the case law of the European Court of Human Rights, not a criterion application of the status of the whistleblower, the information disclosed may even relate to a *dysfunction* or *questionable practices* (...) ".

16. As to the merits, the Court of Appeal decided that, for various reasons drawn from internal criminal law, there was no reason to hold against AD or the requesting the offense of violation of trade secrets and, to this extent, the money laundering-holding, nor the laundering-holding of the fraud proceeds computer science.

17. It considered that, from the point of view of internal criminal law alone, it was right title that the first judges had held that AD and the applicant had committed the offenses of domestic theft, fraudulent access or maintenance in an automated data processing or transmission system, violation of professional secrecy and money laundering - possession of the proceeds of domestic flight. She considered that, contrary to the conclusion of the first judges, EP should be considered an accomplice in the breach of secrecy professional commission committed by the applicant and the money laundering-holding of proceeds of domestic theft committed by the latter.

18. The Court of Appeal then examined whether these offenses, noted and to be retained in principle, were likely or not to be justified on the basis of Article 10 of the Convention. She explained that the admission of the fact proof of the whistleblower, deduced from Article 10 of the Convention, had in Luxembourg law for the effect of neutralizing the illegality of the violation of the law. She clarified that this was the legal element of the offense - necessarily committed by disclosing, in good faith, in a manner measured and adequate, information of general interest - which was thus neutralized and carried the acquittal of the accused.

19. As regards EP, it considered that it was appropriate to recognize him the benefit of the cause of justification of the responsible journalist, deduced by the Court of Article 10 of the Convention. Therefore, she confirmed, for this reason, the full acquittal of the person concerned.

20. As regards AD and the applicant, it applied the case law of the Court relating to the protection of whistleblowers (see, in particular, *Guja vs. Moldova* [GC], n o 14277/04, ECHR 2008). She recalled that this jurisprudence subordinated the protection of the whistleblower to the respect of six conditions, which she explained. His reasoning can be summarized as follows.

1. Analysis of the first four criteria of the Guja case law

21. The Court of Appeal found, in application of this case law, that the disclosures were in the public interest (criterion 1), in that they had "allowed in Europe and Luxembourg, the public debate on the taxation (...) of multinational companies, on tax transparency, practice of tax rulings and tax justice in general ". She added that the European Commission presented, following the revelations *Luxleaks,* a package of measures against tax evasion and an action plan for fair and efficient corporate taxation in the Union European.

22. The Court of Appeal also stated that the disclosures were authentic (criterion 2).

23. As to criterion (3), based on the fact that disclosure to the public is not considered only as a last resort in the event of manifest impossibility to act otherwise, it considered that, having regard to the circumstances of the case, informing the public through a media was "the only realistic alternative for raise the alert ".

24. She admitted that the criterion of good faith (criterion 4) was met. concerning the applicant.

For AD, it considered that this criterion had been met in the summer of 2011, time of handing over to the EP journalist the documents he had appropriate in October 2010. It considered, on the other hand, that this criterion had not been respected by AD at the time of the appropriation of documents, given that he did not yet intend to to make them public.

2. Analysis of the fifth criterion of the Guja case law

25. The Court of Appeal then analyzed the test of the balancing of the public interest in obtaining the information with the damage that the disclosure caused to the employer (criterion 5).

26. Insofar as the applicant contested any prejudice in respect of of the company PwC, pointing out that it had even announced a increase in turnover and staff, the Court of Appeal - after having reviewed the various judgments of the Court on the matter -

recalled this:

> "(...) the European Court does not specifically analyze the damage suffered, but considers that the damage caused to the employer may result from a violation of his image, loss of confidence, and, in general, the impact that denunciation may have have on the public. Plus the case and therefore the information that the employer had wanted keep secret, knows a strong impact, the more the confidence of the public is shaken. "

She also specified this:

> 'There is therefore no need to verify whether, owing to the disclosures of [AD] and [of the applicant], PwC's turnover has decreased or if customers have complained, have brought civil liability actions or have left PwC.
>
> The Court of Appeal held that the fact of disclosing documents covered by secrecy business and professional secrecy undoubtedly prejudices PwC, in particular non-pecuniary damage in his capacity as a victim of criminal offenses, resulting from the damage to its reputation and [from] the loss of confidence of its customers in to the security system within this company. "

In addition, and more particularly in the context of information provided concerning the applicant, it recalled that:

> "In this case, PwC is associated with a practice of tax evasion, if not with a tax optimization described as unacceptable. She was the victim of offenses criminal law and has necessarily suffered prejudice. "

27. Then weighing the public interest on the one hand and the interest of PwC on the other hand, it considered, in the case of AD, that the public interest largely outweighed any damage that PwC and its clients. It therefore concludes that this criterion was met with regard to AD

28. On the other hand, in the applicant's case, it considered that the disclosure documents had caused PwC harm greater than the general interest, so that the fifth criterion was not met. She concludes that the cause of justification constituted by the quality of whistleblower could not not be accepted by the applicant for the following reasons:

> "The documents provided by [the applicant] to the journalist did not (...) nor contribute to th

public debate on the Luxembourg practice of [fiscal rulings] nor triggered [a] debate on tax evasion or provided essential, new and unknown until then. "

29. In reaching this conclusion, it relied on the considerations following.

30. Documents chosen by the applicant, unlike those having were disclosed by AD, did not constitute administrative decisions and did not illustrate the application of tax rulings either. It was about simple tax declarations - therefore unilateral assertions of taxpayers regarding their patrimonial or financial situation - which did not illustrate the attitude of the administration tax on them. These documents therefore brought no revelation on the technique of tax optimization and were only relevant limited.

31. Nor had they been selected by the applicant for the purposes of to complete the tax rulings already in the possession of the EP journalist, by example to illustrate how these tax rulings translated in tax returns. Their selection was made only on the basis of the criterion of the notoriety of the taxpayer concerned.

32. At the time of the appropriation of the documents by the applicant and their transmission by him to the journalist EP, the practice of tax rulings had already been disclosed through the documents sent by AD, which had been broadcast on the occasion of the first program " *Cash Investigation* ", a circumstance of which the applicant was aware.

33. Thus, there was no compelling reason for the applicant to proceed to a new violation of the law to appropriate and disclose confidential documents.

34. The documents had been used by the journalist EP to prepare, in the part of the second " *Cash Investigation* " program, a topic on tax evasion and devoted to the "billions that are missing", and not on the practice of tax rulings. The documents had been used to illustrate the tax evasion of two groups of multinational companies, A. and AM, which were the subject of the report.

I n the case of company A., the tax declarations had, according to the EP journalist, allowed to illustrate that this group had declared to Luxembourg a considerable turnover without however exerting a commercial activity corresponding to it.

Regarding the company AM, the journalist criticized the process following. He reported that this group had transferred to its legal subsidiary Luxembourg the sum of 173 million euros (EUR) to reimburse the interest on a loan he had granted her. This subsidiary was able to deduce the sum in question which had subsequently been transferred to another company in the group located in Dubai, where it benefited from a total exemption taxes.

The Court of Appeal considered that the information relating to two groups of companies could certainly challenge and scandalize, but not did not constitute essential information or fundamentally new. Thus, it concludes that the tax returns submitted by the applicant only endorsed the result of the journalistic investigation by the EP team and that "they were as such, certainly useful to the journalist, but does not provide any cardinal information hitherto unknown which could revive or fuel the debate on escape tax ".

3. Analysis of the sixth criterion of the Guja case law

35. With regard to criterion (6), based on the proportionality of the sanction, the Court of Appeal made a distinction between the two defendants.

She retained that AD, who was to have the cause of justification applied the whistleblower with regard to the facts of the handing over of documents summer 2011 to the journalist EP, was to acquit of any reproach in relation with these facts, therefore the offense of breach of professional secrecy. To the gaze facts not covered by this cause of justification, namely those in report with the appropriation of documents in October 2010, the Court

appeal reduced the prison sentence to six months, with a suspended full, and maintained the fine of EUR 1,500.

With regard to the applicant, the Court of Appeal considered that the offenses found in real competition, so that, according to domestic criminal law, the

Recalling then that the applicant could not benefit from the supporting fact the heaviest penalty could be increased to double the maximum, i.e. oneimprisonment from 3 months to 5 years and a fine of 251 to 5,000 EUR. whistleblower, it decided on the other hand to take into account, as a attenuating circumstance, "of the motive which he thought to be honorable which [had] urged him to act ", as well as" the disinterested nature of his gesture ". Therefore, she decided to disregard any pain.
imprisonment and maintained a fine of EUR 1,000.

36. The Court of Appeal upheld the civil conviction of AD and the requesting payment of a symbolic euro in compensation for the damage morale suffered by PwC.

C. The judgments of the Cour de cassation rendered with regard to AD and the applicant

37. AD and the applicant appealed on points of law against the judgment of the Court of Appeal.

1. Judgment of the Court of Cassation rendered in respect of the applicant

38. In a judgment (n o 2/2018 criminal) of 11 January 2018, the Court of cassation dismissed the applicant's appeal.

39. The applicant had made a plea alleging violation by the Court appeal of Article 10 of the Convention, stating in particular the following:

> "The Court of Appeal disguises the facts and case law of the European Court of rights, engaging in a tendentious interpretation of "the weak relevance of the documents "submitted to [EP], leading to an assessment of the damage suffered by the employer above the general interest and to refuse the implementation of the cause justification of the whistleblower, since the condition of the proportionality of the damage caused in relation to the general interest would not be fulfilled. "

In the "discussion of the plea", the applicant had underlined, by way of for example, that the annexes to the tax returns of group A. (see paragraph 34 above) showed annual general meetings lasting an average of one minute, which would have convinced the total absence of substance in Luxembourg. He had insisted on the fact that the tax declarations communicated by him enabled him to verify the economic substance of the entity created in Luxembourg and to analyze thus the practice of tax rulings.

40. In response to this plea, the Court of Cassation decided in particular this :

"Whereas the assessment of the facts on the basis of which it is necessary to decide whether a accused may or may not benefit from the justification based on the status of the launcher alert comes under the sovereign power of the trial judges and escapes the control of the Cour de cassation, provided that this assessment should not be inferred from insufficient or contradictory reasons;

Whereas in the present case the appellate judges based their assessment on the nature of the documents apprehended by [the applicant], on their use in the context of of a television program on tax evasion, on the declarations of [u applicant] and those of [EP] as to the relevance of the documents apprehended, to conclude that the apprehended tax returns, if they had certainly could have been useful to the journalist [EP], did not however provide any cardinal information, hitherto unknown, which could revive or nourish the debate on tax evasion ;

Whereas, contrary to [the applicant's arguments], the findings in facts made by appellate judges are not contradictory; (...)

That the appeals judges' assessment is thus based on exempt grounds of insufficiency and contradiction; (...) "

2. Judgment of the Court of Cassation rendered in respect of AD

41. The appeal brought by AD was, on the other hand, allowed by the Court of cassation.

42. In its judgment (n o 1/2018 criminal) of 11 January 2018, she broke the judgment of the Court of Appeal on the grounds that recognition of the status of whistleblower should apply in principle to all offenses for which a person, availing himself of the exercise of his right guaranteed by Article 10 of the Convention, was prosecuted, on pain of voiding the protection to result from the whistleblower status of its substance. The Court of Cassation thus decided that the Court of Appeal had disregarded Article 10 of the Convention by refusing to allow AD to benefit from the case justification drawn from the status of the whistleblower with regard to the facts appropriation of the documents produced in October 2010, since it had accepted this cause of justification concerning the delivery of these documents to EP reporter in summer 2011.

D. The judgment of the Court of Appeal rendered, on reference, in respect of AD

43. By a judgment of May 15, 2018, the Court of Appeal held that AD owed, to following the judgment of the Court of Cassation, to be acquitted, on the basis of Article 10 of the Convention, of all the offenses committed in connection with the documents given to the EP reporter in the summer of 2011, including those relating to the adoption of these documents in October 2010.

The Court of Appeal, on the other hand, decided that the first appeal judgment was passed in force of res judicata, and therefore remained maintained, with regard to AD in with regard to these same offenses in relation to documents of internal training that he also took over in October 2010 to

the occasion of the appropriation of the tax documents transmitted subsequently to EP It was limited to this title to pronounce the suspension of the pronouncement of the conviction.

44. This judgment was accepted by the parties, so that it became res judicata.

RELEVANT LEGAL FRAMEWORK AND PRACTICE

I. RELEVANT DOMESTIC LAW

45. The various offenses against the applicant are provided for in the penal code.

46. Thus, the provisions relating to domestic flight read as follows:

Article 461 paragraph 1

"Anyone who has fraudulently removed something or an electronic key that does not not belonging to him is guilty of theft. "

Article 463

"Thefts not specified in this chapter will be punished by imprisonment. from one month to five years and a fine of 251 to 5,000 €. "

Article 464

"The imprisonment will be at least three months, if the thief is a servant or a hired service man, even when he has committed the theft against people whom he did not serve, but who were either in the master's house, either in the one where he was accompanying him, or if he is a worker, journeyman or apprentice, in the house, workshop or store of his master, or a working individual usually in the house where he stole. "

47. As to fraudulent retention in a processing system Automated data, Article 509-1, paragraph 1 st states:

"Anyone who fraudulently has accessed or maintained himself in all or part of of an automated data processing or transmission system will be punished by a imprisonment from two months to two years and a fine of € 500 to € 25,000 or one of these two penalties. "

48. The offense of breach of professional secrecy is provided for by section 458, which reads as follows:

"Doctors, surgeons, health officers, pharmacists, midwives and all other persons who are custodians, by state or by profession, of the secrets entrusted to them, who, except in the case where they are called to bear witness in justice and where the law forces to make known these secrets, will have revealed them, will be punished with a imprisonment from eight days to six months and a fine of € 500 to € 5,000. "

49. Laundering-holding of the proceeds of domestic theft is provided for in article 506-1 which referred to article 32-1.

Article 506-1, as in force at the material time, provided that:

"Are punished by imprisonment from one to five years and a fine of € 1,250 to 1,250,000 € or one of these penalties only:

1) those who have knowingly facilitated, by any means, the false justification of the nature, origin, location, arrangement, movement or ownership of the goods referred to in Article 32-1, first paragraph, under 1), forming the object or product, direct or indirect: (...) of an infringement of articles 463 and 464 of the Criminal Code (...) or constituting a financial advantage derived from one or more of these offenses;

(...)

3) those who have acquired, held or used goods referred to in article 32-1, paragraph first, under 1), forming the object or the product, direct or indirect, of the offenses listed in point 1) of this article or constituting a financial advantage derived from one or more of these offenses, knowing, at the time they received them, whether they came from one or more of the offenses referred to in point 1) or participation in one or more of these offenses. "

This "article 32-1, first paragraph, under 1)", meanwhile repealed (by a Law of 1 st August 2018), provided:

"In the event of a money laundering offense referred to in Articles 506-1 to 506-8 (...) the special confiscation applies: 1) to property including property of any kind, tangible or intangible, movable or immovable, as well as legal acts or documents attesting to a title or a right to property, property forming the object or product, direct or indirect, of an infringement or constituting a financial advantage derived from the offense, including the income from such property (...) "

Article 506-4 also supplements Article 506-1 and provides that:

"The offenses referred to in article 506-1 are also punishable when the author is also the perpetrator or the accomplice of the primary offense."

II. EUROPEAN UNION LAW

50. Directive (EU) 2016/943 on the protection of business secrets was adopted on 8 June 2016. According to Article 1 st of this Directive, Member States are invited to include in their legislation "measures, procedures and repairs' in order to allow holders of trade secrets prevent or obtain redress for "the obtaining, use or unlawful disclosure of their business secrets ". Recital 20 of said Directive indicates, however, that these measures, procedures and remedies "do not should not interfere with the activities of whistleblowers "; he specifies by elsewhere than "the protection of trade secrets should therefore not extend to cases where the disclosure of a trade secret is in the public interest insofar as it allows to reveal a fault, a reprehensible act or directly relevant illegal activity. It shouldn't be understood as preventing the competent judicial authorities from authorizing a exemption from the application of measures, procedures and remedies when the defendant had every reason to believe, in good faith, that his

behavior met the appropriate criteria set out in this directive ".

51. Next, Directive (EU) 2019/1937 on the protection of individuals which report breaches of EU law was adopted on 23 October 2019. This directive, which aims to protect whistleblowers who denounce infringements of European Union law in various fields, such as that public procurement, financial services, prevention of money laundering or public health, will have to be transposed by Member States no later than December 17, 2021.

III. INTERNATIONAL TEXTS

A. The United Nations

52. In his report A / 70/361 of 8 September 2015, the Rapporteur

UN Special on the Promotion and Protection of the Right to Liberty opinion and expression, D. Kaye, deals with the protection of information and whistleblowers.

53. In his view, the term "whistleblower" refers to "a person who discloses information they have reasonable grounds to believe truthful at the time it makes their disclosure and which relate to facts which it considers to constitute a threat or prejudice to a general interest, such as for example the case of a violation of the right internal or international, abuse of authority, waste, fraud or damage to the environment, public health or safety public ". D. Kaye specifies, moreover, that "the alert does not always carry on specific unlawful acts, it may consist in revealing withheld information that it is in the legitimate interest of the public to to know ".

54. On January 24, 2017, the Secretary-General of the United Nations, António Guterres, approved an update to the United Nations concerning whistleblowers, thus seeking to "strengthen the protection of employees of the Organization who report a possible fault or cooperate with official audits or investigations ".

B. The Council of Europe

55. In its *Heinisch v. Germany* (no.28274 / 08, § 37, ECHR 2011 (extracts)) and *Bucur and Toma v. Romania* (n o 40238/02, § 63, 8 January 2013), the Court summarized Resolution 1729 (2010) on the protection whistleblowers, adopted by the Parliamentary Assembly of the Council of Europe April 29, 2010.

56. Another instrument has been adopted in this area by the Committee of Ministers of the Council of Europe, April 30, 2014. Certain passages

relevant to this Recommendation CM / Rec (2014) 7 are reported in the case of *Medžlis Islamske Zajednice Brčko and Others v. Bosnia and herzegovina* ([GC], n o 17224/11, § 44, 27 June 2017).

This recommendation considers that the whistleblower is assimilated to anyone who "makes reports or reveals information

concerning threats or harm to the general interest in the context of their employment relationship, whether in the public sector or in the private sector ".

57. On 23 June 2015, the Parliamentary Assembly of the Council of Europe adopted Resolution 2060 (2015) and Recommendation 2073 (2015) tending to "improve the protection of whistleblowers".

In the first, she referred to "revelations concerning the massive surveillance and intrusions into privacy to which the Agency United States National Security Agency (NSA) and other security services information [had] proceeded "and called for the adoption of" a binding legal instrument (convention) on the protection of whistleblowers on the basis of Recommendation CM / Rec (2014) 7 of Committee of Ministers (...) ".

In the second, she invited the Committee of Ministers to "promote further improvements in the protection of whistleblowers, in particular initiating the process of negotiating a binding legal instrument in the form of a framework convention open to non-member states and relating to the revelation of wrongdoing committed by individuals employed in the field of national security and intelligence ".

58. The 1 st October 2019, the Council's Parliamentary Assembly Europe adopted Resolution 2300 (2019) and Recommendation 2162 (2019) aiming to "improve the protection of whistleblowers everywhere in Europe ".

In the first, she welcomed the directive (EU) 2019/1937 (see paragraph 51 below) and invited Member States of the Council of Europe which are also members of the European Union at adopt its provisions, while adding that nothing prevented them by elsewhere to protect, according to the same principles, the reports of violations or abuse of their national law. As for the Member States of Council of Europe which are not members of the European Union, it invited them to review their relevant legislation or to adopt new laws inspired by the proposal for a European directive question.

In the second, she reiterated her invitation to the Committee of Ministers initiate preparations to negotiate a binding legal instrument in the form of a Council of Europe convention which should be inspired by the aforementioned directive, while taking into account the details and additions proposed in Resolution 2300 (2019).
In its response, adopted on 22 April 2020, the Committee of Ministers reiterated,

with regard to the recommendation of the Parliamentary Assembly to prepare a binding legal instrument, its position expressed in its response to Recommendation 2073 (2015). He thus considered that "the negotiation of a binding instrument, such as a convention, would represent a long process and uncertain outcome given the complexity of the subject and the diversity of solutions adopted by Member States to protect whistleblowers ”and considered that it was“ more appropriate, at this stage, encourage states to fully implement the recommendations which have been adopted by the Committee of Ministers or other bodies (...) ”.

PLACE

ON THE ALLEGED VIOLATION OF ARTICLE 10 OF THE CONVENTION

59. The applicant alleged that his conviction following the disclosure by him to a journalist of sixteen documents from his employer PwC constitutes a disproportionate interference with his right to freedom of speech. He relies on Article 10 of the Convention, which is thus wording :

> “1. Everyone has the right to freedom of expression. This right includes freedom opinion and the freedom to receive or impart information or ideas without there being any interference from public authorities and without consideration of frontier. This article does not prevent States from subjecting companies to broadcasting, cinema or television to a licensing regime.
>
> 2. The exercise of these freedoms involving duties and responsibilities may be subject to certain formalities, conditions, restrictions or penalties provided for by law, which constitute measures necessary, in a democratic society, for the security national, territorial integrity or public safety, the defense of order and prevention of crime, the protection of health or morals, the protection of reputation or the rights of others, to prevent disclosure of information confidential or to guarantee the authority and impartiality of the judiciary. "

A. Admissibility

60. The Government raised an objection of inadmissibility based on a manifest lack of basis for the complaint. He refutes the assertion of applicant, according to which, inter alia, the Court of Appeal had "held that he was possible to circumvent the Court's case-law on the violation of Article 10 [of the Convention] ”, and had“ only pretended to engage in balance of interest ”. Relating to certain passages of the judgment in question, the Government states that the Court of Appeal recalled that it was required to give full effect to the Convention and then applied the case law of the courtyard. It considers the applicant's assertion to be manifestly erroneous and invites the

Court to declare the application inadmissible under Article 35 § 3 (a) of the Convention.

61. The applicant replies that, through this argument, the Government analyzes in detail the balance of interests achieved by the domestic courts, which would come under the merits of the case. He adds that the Government, recognizing the existence of an interference with the law protected by Article 10 of the Convention (see paragraph 76 below), cannot not contradict oneself by raising an objection based on a manifest lack of basis of a grievance which he otherwise recognizes as being partially based. He therefore requests that the objection raised by the Government be joined to the merits before being dismissed.

62. The Court considers that the argument in question raises questions calling for an examination of the merits of the complaint under Article 10 of the Convention and not an examination of the admissibility of the complaint (see, *mutatis mutandis, Gürbüz and Bayar v. Turkey* , no.8860 / 13, § 26, 23 July 2019).

63. Noting thus that the complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention and that it is not elsewhere on no other ground of inadmissibility, the Court declares it admissible.

B. On the merits

1. Submissions of the parties

a) The applicant

64. The applicant, who had indicated in his application that he was “originally of the *Luxleaks* affair ”, takes note of what the Government admits the existence of an interference with his right to freedom of expression.

65. He considers that the question of law crystallizes around that of the proportionality of the interference.

66. He argues first of all that the Government “is trying to put in scene (...) an innocent and objective transmission ”of the facts by asserting that the tax returns sent by the applicant would be of "Simple assertions by the taxpayer". According to the applicant, this would be unlike legal acts - developed and drafted by PwC on behalf of of its customers and invoiced to them - who "demonstrate the existence concrete tax package contained in the tax ruling (creation of

Luxembourg and *offshore* companies , movement of intra-group, payment of dividends, etc.). "

He also makes various allegations and criticisms with regard to the judgment of the Court of Appeal.

The Court of Appeal would have ruled that "neither the Convention, nor the law Luxembourg did not provide the whistleblower with an exemption from criminal proceedings, (...) so that Article 10 would only allow find that lawsuits were not necessary in a company

democratic, without allowing to relax [equivalent of the term "Acquit" under Luxembourg law] the accused ".

By "judging that the public interest in knowing the information transmitted by [him] was less severe than the damage caused to [PwC] ", the Court of Appeal - which would in this have been approved by the Court of Cassation - he allegedly "refused [...] protection of the status of the whistleblower". The courtyard appeal having "ruled that the employer's damage was (...) one euro symbolic ", the exercise of the balance" presupposes that the interest of public knowledge of the information in question was, in this case, less than a symbolic euro, that is, equal to zero. »However, the Court of Appeal did not claimed that the value of the information provided by the applicant was nil, she would have "only pretended to engage in the balance of interests".

The national courts have "noted that there was indeed a documentary evidence which may in this case allow the acquittal of the applicant, [but], having regard to the circumstances, they [would] have decided that the applicant (...) [may [it] invoke [only] a lesser protection, [that of] the recognition of mitigating circumstances ".

67. There is no objective reason to distinguish the fate reserved for AD of his, insofar as they were both employees indivisibly linked to the leaks of documents that led to the scandals *Luxleaks.* The elements he revealed would have "come to the reinforcement of the [AD] position ".

68. Considering that "his criminal conviction could not be justified that by a single concern: its dissuasive function ", it is of the opinion that the existence of this sanction can, by itself, justify the finding of a violation of Article 10 of the Convention.

69. Finally, he “takes up and endorses the (...) observations of the [third party part] ”, which can be summarized as follows.

70. Retain the three new criteria of “essential information, new and unknown ”as the Court of Appeal did (see paragraph 28 below). above) would have serious repercussions on the effectiveness of the protection of whistleblowers.

71. On the one hand, the addition of such criteria would generate insecurity legal.

Thus, the criterion of the "essential" nature of the information disclosed would introduce a legal vagueness as soon as this notion would be circumscribed. In addition, this criterion, unprecedented and non-existent in all of the legislation or case law of States protecting whistleblowers, would be complicated to apply by the courts and would give rise to disparities in interpretation.

The criterion of "new" information would lead to limiting the number alerts, particularly in the event that an alert relates to a information relating to facts already known but not dealt with in the past. the French case of Céline Boussié, who launched the alert, in 2008, on facts

already known to abuse children with disabilities - denounced by former colleagues since the late 1990s - would be an example.

Finally, as to the criterion of "unknown" information, it could be "Necessary in a democratic society" than the revelation of evidence additional - unknown but helping to highlight facts known and denounced beforehand - constitutes an ethical alert worthy of a protection under Article 10 of the Convention.

72. On the other hand, it would be impossible in practice for the pitchers alert to meet these new criteria.

The six criteria adopted by the Court - not including at any time a examination of the new, essential and original character of information - would have made it possible to find a satisfactory balance between the interests of employers and the public's right to information.

Such a conception on the part of the Court would comply with the standards international organizations and in particular to the European directive adopted in matter, which would generally require only a "reasonable belief"

in the veracity of what is denounced, to the exclusion of any appreciation prior to the new, novel or essential nature of the information.

This design would also be adapted to the profiles of the launchers. alert which, in the age of digital networks, would have access to extremely easy to a large amount of information. In this context, the *Guja* case-law model would *act as* a safeguard against illegal leaks, in that it would ensure that the information disclosed is genuinely of general interest. However, when the launchers alert would be convinced that they could no longer be protected, they would be encouraged to anonymously leak information.

73. In addition, the new criteria adopted by the Court of Appeal would lead to an indirect infringement of the obligation of States to investigate on human rights violations.

In fact, the public authorities would thus be relieved of their responsibility for their mission to conduct investigations into the facts disclosed by the whistleblowers and decide whether or not to prosecute the alleged offenders. When an alert is launched very upstream of damage and that whistleblowers would not have for this reason not the means to base their allegations on a factual basis sufficient, only an investigation by the public authorities would make it possible to day the whole problem to which the whistleblower would have had only one partial access. Examples of the Court's case-law would show that protection would have been granted to whistleblowers who disclosed, without necessarily having been able to prove them, information highlighting evidence of the existence of damage to the environment, to the physical integrity of people or rights contributing to the pluralism that characterizes companies.

74. Finally, beyond these problems, the new criteria adopted by the Court of Appeal would also lead to an infringement of the right of journalists and democracy watchdogs.

Whistleblowers would already be reluctant to alert the public because of the serious consequences on their personal situation that they would risk undergo. However, the adoption of the aforementioned criteria would have a dissuasive

additional information on potential “whistleblower” sources of journalists. The media would thus be less able to play their role of watch dog. In many cases, the right of journalists to protect their sources would be intimately linked to the need to protect disclosure information by whistleblowers. In conclusion, require launchers warning that the information they transmit to the press is "essential, new and unknown ”and denying them protection if necessary would lead to necessarily undermine the protection of sources and could deter whistleblowers to work with journalists.

b) The Government

75. The Government contested the applicant's allegation that he was "at the origin of the *Luxleaks* affair ". According to the Government, it was AD who had been at the origin of the revelations, both from a point of view temporal than that of the number and nature of the documents disclosed. AD's disclosures would have testified to the fiscal fate of the authorities to the companies concerned, unlike those of the applicant who would have consisted of simple unilateral declarations which did not light the practice of tax rulings. It would be the difference in quality between the documents sent by AD and those sent by the applicant who would explain that the first was acquitted while the second was not seen apply only extenuating circumstances.

76. On the other hand, the Government acknowledged that, the applicant having been sanctioned in criminal and civil matters for having transmitted documents to a journalist who then published them, there was an "interference" in the right to freedom of expression of the person concerned.

77. He notes that the appellant is only discussing the issue of proportionality of the interference and thus does not call into question the fact that it ci was "prescribed by law" and pursued a "legitimate aim".

78. As to the question of proportionality, the Government considers that the Court of Appeal scrupulously analyzed the six criteria laid down by the the case-law of the Court in the matter with regard to the applicant. He specifies that the discussion can only focus on criteria (5) and (6), the only on which the applicant would dispute the merits of the analysis made by the Court of Appeal.

79. He first refutes the applicant's assertions as to a “bet en scene ”of the facts by the Government, stressing that it was limited to

faithfully summarize the findings relevant to the courts
national.

It also considers it necessary to rectify the criticisms formulated by the applicant in respect of the judgment of the Court of Appeal (see paragraph 66 above).

Thus, the applicant would deduce his conclusion as to the absence of a acquittal of a quotation out of context of a passage from the appeal judgment, regardless of the subsequent reasoning. The Government recalls in fact that, according to the Court of Appeal, even in the absence of a legal provision special, express and formal, an acquittal was likely to be based on a *sui generis* justifying fact ; and, when the criminal conviction violated the protection recognized by the Court on the basis of Article 10 of the Convention, the whistleblower benefited from such a supporting fact, which had the effect of neutralize the unlawfulness of the violation of the law and result in acquittal of the accused.

The applicant would not have been refused any protection under Article 10 of the Convention in so far as the Court of Appeal held account, in determining the sentence, of the motive of the applicant and the character disinterested in his gesture, which would have been recognized as worth extenuating circumstances. The magistrates would not have proceeded to a sham of appreciation, as the applicant would try to make it believe. The Court of Appeal, by allocating a symbolic euro as compensation for the moral damage suffered by the civil party, would not have considered that the damage of this was limited to one euro. In civil matters, PwC had waived, for reasons that were personal to him, to claim compensation for damage material or to attempt to assess moral damage at its real value. Born may, according to domestic law, allocate an amount greater than that requested, the Court of Appeal would thus have limited itself to assessing whether the civil party had suffered non-pecuniary damage equivalent to at least the amount requested. She would, on the other hand, have given a detailed ruling on the damage suffered by PwC when it proceeded, in full compliance with the case-law of the Court, to the assessment of the criterion of the balancing of the interests involved.

In so far as the applicant complains that he was only granted one "Lesser protection" (see paragraph 66 above), the Government replied which the Court of Appeal did not accept, contrary to the assertions of applicant, that the circumstances were met to invoke the protection of Article 10 of the Convention, but, on the contrary, it held that the applicant could not benefit from the justifying fact of the whistleblower (see paragraph 28 above).

80. With regard to the fifth criterion, the Court of Appeal found, by of the relevant grounds, the existence of real and certain harm, and then weigh this against the public's interest in being informed of the content of documents disclosed by the applicant. The Court of Appeal would have carried out a detailed analysis of the elements, estimating that the

disclosure of the documents by the applicant had neither served to supplement the revelations previously made by AD concerning the practice Luxembourg administrative tax rulings, nor to illustrate this last. The Government also indicates that the relevance of documents revealed by the applicant was limited to allowing the journalist EP to illustrate a report describing the fact - which was neither new nor original - that, in order to limit their tax burden, groups of companies multinationals took advantage of the lack of international harmonization of tax laws. Thus, contrary to AD's disclosures, the documents revealed by the applicant had only served to “illustrate the fact, notorious and in itself commonplace, that companies, in order to reduce their tax, structure their assets through the creation of subsidiaries ”, but do not would not be relevant "to establish or illustrate that the use of these structures had been approved in advance by the administration or for understand the scope, scope and systematic nature of tax optimization techniques approved in advance by administration within the framework of the tax rulings revealed by " *Luxleaks* ".

81. As to the sixth criterion, the 'proportionality of the sanction and the deterrent effect thereof ”should be“ assessed against a person who does not meet all the criteria of the whistleblower ”. The Court of Appeal having held that the fifth criterion was not met concerning the applicant, his situation is different from that of people who meet all the criteria for the whistleblower.

The Court of Appeal allegedly held that the applicant was protected under Article 10 of the Convention, even if it could not prevail over the cause of justification of the whistleblower. Thus, the Court appeal would have, in accordance with the Court's case-law, applied a lower level of protection, allowing the applicant to benefit from extenuating circumstances. Indeed, to pronounce a sentence limited to one a relatively small fine, the Court of Appeal would have held account of the motive and the disinterested character of his gesture. the Government concludes that the fine could not, due to the circumstances particular to the species, be considered neither as being disproportionate nor as having a dissuasive effect on the exercise of the freedom of expression of the applicant or other employees.

c) The intervening third party

82. The “House of whistleblowers”, in its capacity as intervenor, insists on the major interest presented by the present case, since it would lead the Court to rule on the modalities of analysis of the proportionality of attacks on the freedom of expression of whistleblowers.

83. It exposes, through a representative sample of jurisdictions having put in place a protective law for whistleblowers, the definitions retained in the matter in the legislation concerned. Then relating the

the case-law of the Court, it emphasizes only the criteria taken into account by it, which would not at any time include a review of the "new, essential and unpublished" character of information, as was the case case in the present case.

2. Assessment of the Court

a) General principles applicable

84. The fundamental principles to be applied in order to assess the point of whether an interference with freedom of expression is "necessary in a democratic society ”are well established in the Court's case-law and have been summarized as follows (see, among others, *Magyar Helsinki Bizottság vs. Hungary* [GC], n o 18030/11, § 187, 8 November 2016):

> “I. Freedom of expression is one of the essential foundations of a society democratic, one of the essential conditions for its progress and the development of each. Subject to paragraph 2 of article 10, it is not only for "information" or "ideas" received with favor or considered harmless or indifferent, but also for those that offend, shock or worry: this is what pluralism, tolerance and the spirit want openness without which there is no “democratic society”. Such as enshrines Article 10, it is accompanied by exceptions which however call for a narrow interpretation, and the need to restrict it must be established convincing (...).
>
> ii. The adjective "necessary", within the meaning of Article 10 § 2, implies a "social need imperious ”. Contracting States enjoy a certain margin of appreciation to judge the existence of such a need, but it is coupled with a European control dealing both with the law and with the decisions that apply it, even when they emanate from an independent court. The Court therefore has jurisdiction to rule in

last place on whether a "restriction" is reconciled with freedom
expression protected by section 10.

iii. The task of the Court, when exercising its control, is not to take the place of
competent national authorities, but to verify under Article 10 the
decisions they have rendered under their discretion. It does not follow
not that it should confine itself to determining whether the respondent State has used this power to
in good faith, with care and in a reasonable manner: he must consider the interference
contentious in light of the whole case to determine whether it was
"Proportionate to the legitimate aim pursued" and if the grounds invoked by the authorities
to justify it appear "relevant and sufficient" (...) In so doing, the
Court must be satisfied that the national authorities applied rules in accordance with
to the principles enshrined in Article 10 and this, moreover, based on a
acceptable assessment of the relevant facts (...). "

85. More specifically, in the context of denunciation, by employees, of illicit conduct or acts observed by them at their place of work, the Court established certain fundamental principles on which the assessment of the proportionality of an interference with liberty expression. Thus, the Court must take into account several factors, namely the public interest of the information disclosed, its authenticity, the

whether or not other means are available to make the disclosure, employee's good faith, the harm caused to the employer and the severity of the sanction (*Guja v. Moldova* [GC], n o 14277/04, §§ 69-79, ECHR 2008 , *Heinisch* , cited above, §§ 62-70, and *Bucur and Toma* , cited above, §§ 92 and 93).

b) Application in the present case of the above-mentioned principles

i. On the existence of an "interference"

86. The parties agree that the applicant's conviction for forwarding confidential documents to a journalist who had them subsequently published constitutes interference with the exercise by the person concerned of his freedom of expression. Recalling that Article 10 of the Convention extends to the professional sphere, including when relations between employer and employee are governed by private law (see *Heinisch* , cited above, § 44, as well as references cited therein), the Court considers that the applicant's conviction amounted to an interference within the meaning of Article 10 § 1.

ii. On the question whether the interference was "in accordance with the law" and pursued a "legitimate aim"

87. The Court observes that it is not disputed that this interference was "Prescribed by law" and that it pursued a "legitimate aim". Indeed, the applicant was convicted of having committed various offenses provided for by the Criminal Code (see paragraph 45 above) on the one hand, and the prosecution and sanction of these offenses were intended to prevent the disclosure confidential information and protect the reputation of the employer PwC on the other hand.

88. It therefore remains to be analyzed whether the interference was “necessary in a democratic society ”, in particular by investigating whether there was a proportionality between the interference and the objective pursued.

iii. On the question of the "necessity" of the interference

α) On the qualification of "whistleblower"

89. At first glance, upstream of the analysis of the question of the need interference, the Court considers it useful to determine whether the applicant can be qualified as a "whistleblower" in accordance with the elements identified in this subject of the Court's case-law. In the different affairs she has examined in this area, the Court has sometimes explicitly placed the debate on the field of freedom of expression for whistleblowers to conclude the applicability of the principles set out in the *Guja* judgment (*Heinisch* , cited above, § 64), she said earlier that the protection of whistleblowers was not in question (see, for example, *Rubins v. Latvia* , n o 79040/12, § 87, January 13, 2015, or *Aurelian Oprea v. Romania* , no.12138 / 08, § 69, January 19, 2016).

90. In the present case, the Court of Appeal explained that the admission of the fact proof of the whistleblower, deduced from Article 10 of the Convention, had in Luxembourg law for the effect of neutralizing the illegality of the violation of the law. She also clarified that in such a case it was the legal element of the offense - necessarily committed by disclosing, in good faith, a in a measured and adequate manner, information of general interest - which

was thus neutralized and resulted in the acquittal of an accused (see paragraph 18 above). In the applicant's case, it concluded that the person concerned could not benefit from the justifying fact of the whistleblower at the meaning of national law (see paragraph 28 above).

91. The Court considers that it is not for it to give its opinion on the whether the legal element of the offense alleged against the applicant was to be neutralized or not, such an examination coming under national law alone. In this sense, she considers that it is not necessary to study the arguments relative, developed by pplicant and contested by the Government (see paragraphs 66 an bove). On the other hand, it considers that, for the purposes of the examination of the plaint under Article 10 of the Convention submitted to it, it it is up to him to assess whether it is a case relating to a whistleblower in which the established principles apply. About this, she firstly recalls that the applicant had with his employer PwC a bond of subordination which had held him to a duty of loyalty, reserve and discretion. However, this duty constitutes a particular characteristic of the concept of whistleblowing (see, *conversely* , *Medžlis Islamske Zajednice Brčko and Others* , cited above, § 80). Then, she recalls that the applicant had contacted a journalist for him reveal confidential information that he had obtained in the context of his working relationship. Believing that parallels can be drawn between this approach of the interested party and those adopted by the applicants in the aforementioned *Guja* and *Heinisch cases* , the Court concludes that the applicant is *a priori* to be considered as a whistleblower within the meaning of case law of the Court. Therefore, it is up to him to verify whether the different criteria laid down by the *Guja* case law have been met.

β) On compliance with the criteria laid down by the *Guja* case-law

92. The Court notes that the first four criteria laid down by the *Guja* jurisprudence is not the subject of any controversy between the parties.

93. The only issue at issue is compliance with the fifth and sixth criteria.

- As to the fifth criterion

94. As to the fifth criterion, the Court notes that the applicant's right to the protection of his freedom of expression is confronted with that of his employer, PwC, to protect its reputation.

95. The present application calling for an examination of the fair balance to be struck between these competing interests, the Court will take into account the following factors.

96. First of all, if the balancing act by the national authorities made in accordance with the criteria established by the Court's case-law, it must have serious reasons for it to substitute its opinion for that of the domestic jurisdictions (*Von Hannover v. Germany (n o 2)* [GC], no bone 40660/08 and 60641/08, § 107, ECHR 2012).

97. In terms of valuation - as part of the balancing act respective interests - the damage suffered by the employer, the Court recalled that there is an interest in protecting the commercial success and viability of companies, for the benefit of shareholders and employees, but also for the economic good in the broad sense (*Heinisch* , cited above, § 89). Nevertheless, as regards more particularly the reputation of the company, the Court has also took care to clarify that there was a difference between a damage to a person's reputation regarding their social status, which could have repercussions on her dignity, and an attack the commercial reputation of a company, which has no dimension moral (*Uj v. Hungary* , n o 23954/10, § 22, 19 July 2011).

98. In the present case, the domestic courts held that the fifth criterion of the *Guja* case law was not fulfilled, on the grounds that the disclosure by the applicant of documents covered by secrecy professional cause damage to PwC - resulting in particular from damage to its reputation and loss of customer confidence in the security system within company - superior to the general interest (see paragraphs 26 and above). When balancing interests in cause, they therefore gave more weight to the damage suffered by PwC than the interest of the disclosure made by the applicant.

99. At the outset, the Court must reject the argument formulated by the applicant that the Court of Appeal "only pretended to engage in balance of interest "(see paragraph 66 above).

In this regard, it joins the exhaustive and convincing explanations provided by the Government and refers to these (paragraph 7 9 above).

Indeed, the Court of Appeal did indeed assess the moral prejudice suffered by PwC before proceeding to a balancing of the respective interests. However, according to national law, the Court of Appeal does not could not award as compensation for damage an amount greater than beyond that which was requested by the civil party. In fact, according to a custom widespread in Luxembourg, a person - natural or legal - who has undergone moral prejudice, however significant, often forgoes monetization of its prejudice. Thus, it is common for a civil party to simply ask recognition of his prejudice as such, which involves the technique of the request for the allocation of a symbolic euro.

However, the damage cannot be considered to be non-existent simply because it was valued by PwC at one euro (formerly a symbolic franc, worth forty times less). Thus, the Court does not notes in itself no contradiction between the fact that the Court of Appeal found damage, on the one hand, and then set the amount of the damage to a symbolic euro, on the other hand.

100. It cannot be argued that PwC had necessarily suffered prejudice by the very fact of the widely publicized controversy triggered by the *Luxleaks* affair (see, *mutatis mutandis* , *Heinisch* , cited above, § 88). Press articles confirm, moreover, that the company had "had a difficult year" following the breakdown of the affair (see paragraph 8 *in fine* above).

101. On the other hand, - still according to the press, and it is a fact not contested - beyond this first difficult period, PwC experienced a growth in turnover, going hand in hand with an increase large number of staff (see paragraph 8 *in fine* above). This is a element which the Court cannot disregard in the context of the present case, especially in light of the distinction it made in its *Uj* judgment (cited above, § 22). Thus, it is important to know whether, in the present case, the damage caused by the damage to reputation had ultimately effective and concrete existence. However, due to the growth of its business - once the first "difficult year" has passed - health PwC's economy does not appear to have been permanently affected and all suggests that PwC's reputation was ultimately not shaken, from less with regard to the companies constituting its clientele.

102. The Court concludes that, while PwC has undoubtedly suffered firstly, the extent of the prejudice concerning the infringement of PwC's reputation is not proven over the long term.

103. In order to continue examining the balance of respective interests, it henceforth for the Court to examine the reasons given by the national authorities concerning the interest of the disclosures made by the applicant.

104. In this regard, the motivation of the Court of Appeal, which is at the heart of the debate, is as follows: “(...) the documents submitted by [the applicant] to the journalist had neither contributed to the public debate on the practice Luxembourgish [fiscal rulings] nor triggered [a] debate on evasion tax or provided essential, new and unknown information

until then ”(see paragraph 28 above).

105. In reasoning thus, the Court of Appeal took into account a series of elements.

It noted in particular that the applicant's revelations related to simple corporate tax declarations that did not allow to illustrate the attitude of the tax administration towards the latter. She has considered that there were no compelling reasons for the applicant to

disclose the confidential documents in question, at a time when the practice tax rulings had already been unveiled by AD She specified that the documents revealed by the applicant - which had been used to illustrate the thesis of tax evasion practiced by two groups of companies multinationals - were certainly useful to the journalist, but not provided no previously unknown cardinal information that could revive or fuel the debate on tax evasion (paragraphs 28 to 34 below above).

106. By proceeding in this way, the Court of Appeal explained its reasoning as to the fifth criterion of the *Guja* case law in a statement of reasons detailed. There must therefore be serious reasons for the Court to substitutes its opinion for that of the domestic courts (*Von Hannover (n o 2)* , cited above, § 107). However, this cannot be the case for the reasons set out above. below.

107. The Court of Appeal was careful to assess the interest of the disclosures of the requester by engaging in an in-depth analysis of their content and repercussions they had on the thematic of the practices multinationals tax.

108. In this context, she did not deny that the revelations presented a general interest (see paragraph 21 above). She even took into account the effect the information produced, admitting that it could “To challenge and scandalize” (see paragraph 34 above).

109. On the other hand, it concluded that the complainant's disclosures were of a lower interest than the damage suffered by PwC, after having felt that they were of low relevance. For this, she noted that documents did not provide essential, new and unknown until then. The Court cannot agree with the applicant's argument

according to which the Court of Appeal had, in this way, added new
criteria to those laid down by the case-law established by the Court in the matter.
She considers that the three qualifiers - "essential information,
new and unknown "- are instead included in the reasoning
exhaustive review of the Court of Appeal with regard to the fifth criterion relating to the
balance of respective private and public interests. In the opinion of the Court, they are
to be considered as details which, in other circumstances,
might turn out to be too narrow, but which, in the present case, are
used to conclude, with the other data taken into account by the Court
appeal, that the applicant's disclosures were of no interest
sufficient to balance the damage she had recognized in the head
by PwC.

110. The Court considers that the Court of Appeal confined itself to examining meticulously the elements with regard to the criteria set by the
the case-law of the Court in the matter, in order to draw the conclusion that the
documents disclosed by the applicant were not of sufficient interest to
that he can be acquitted. The fact that AD, on the other hand, was acquitted, by

application of these same criteria of the Court's case-law, confirms in
remaining that the national authorities have carried out an analysis
detailed in the exercise of balancing the respective interests.

- As to the sixth criterion

111. In the context of the assessment of the proportionality of
interference with freedom of expression, the Court held that the nature and
the severity of the penalties imposed are also factors to be taken into account.
consideration (*Otegi Mondragon v. Spain* , n o 2034/07, § 58, ECHR
2011). In the present case, the Court observes that the domestic courts held
account, as a mitigating circumstance, of the "disinterested character of the
gesture "by the applicant, only to impose a fine in the amount of
rather weak (see paragraph 35 above). The Court concludes that it is not
unreasonable to consider that such a sanction is relatively moderate
and does not produce a truly dissuasive effect on the exercise of the freedom of
applicant or other employees, but encourages reflection on the legitimacy
of the planned approach.

c) Conclusion

112. Having regard to the margin of appreciation available to States contractors in the matter, the Court concludes that the domestic courts have struck in the present case a fair balance between, on the one hand, the need to preserve the rights of the applicant's employer and, on the other hand, the need to preserve the latter's freedom of expression.

113. Accordingly, there has been no violation of Article 10 of the Convention.

FOR THESE REASONS, THE COURT,

1. *Declares* , unanimously, the complaint concerning Article 10 of the Convention admissible;

2. *Holds* by five votes to two that there has been no violation of Article 10 of the Convention.

Done in French, then communicated in writing on May 11, 2021, in application of Article 77 §§ 2 and 3 of the Regulation.

Milan Blaško
Clerk

Paul Lemmens
President

This judgment is appended, in accordance with Articles 45 § 2 of the Convention and 74 § 2 of the Rules, the statement of the separate opinion of the judges Lemmens and Pavli.

PL
MB

JOINT DISSENTING OPINION TO JUDGES LEMMENS AND PAVLI

(Translation)

1. We regret that we cannot agree with the majority's conclusion that there was no violation of the applicant's rights in the present case arising from Article 10. Our disagreement relates, on the one hand, to the approach general adoption adopted by the majority in the balancing of the rights of the private employer and the general interest in the disclosure of information in question and, on the other hand, on the reasons put forward by the courts national laws to conclude that the interests of the employer should prevail given the circumstances. More specifically, we believe that elements on which the national courts have relied in appreciating the "fifth criterion" defined in *Guja v. Moldova* ([GC], n o 14277/04, ECHR 2008), namely the criterion relating to the balancing the public interest in obtaining the information with the damage that the disclosure caused to the employer (*Guja* , cited above, §§ 76 and 90-91; paragraphs 25-34 of the judgment), run counter to the fundamental concepts of general policy debate in a democratic society. Therefore, at our great regret, we cannot, like the majority, adhere to the reasoning of the domestic courts (paragraphs 94-110 of the judgment).

2. The outcome of the balancing carried out by the national courts is based on the idea that the complainant's disclosures only provided limited contribution to public debate, in particular compared to first revelations made by another employee of the company concerned. The key argument in this regard is that the documents disclosed by the applicant did not bring to light any "essential, new and unknown information until then "(see paragraph 28 of the judgment). From this assessment, the national courts have considered that the damage suffered by the employer of the applicant was superior to the general interest in receiving the information disclosed (*ibidem*).

The nature of the applicant's disclosures

3. Let us recall that the complainant's disclosures related to sixteen documents - fourteen tax returns from multinational companies and two cover letters -, some having been used for the preparation of an episode of the investigative television show " *Cash Investigation* ", which was broadcast on 10 June 2013 (paragraph 8 of the judgment). According to the investigative journalist responsible for this program, the

The applicant's revelations formed the basis of this episode [1] . The journalist also noted that some revelations made during this episode would have been impossible without access to the information provided by the applicant [2] . Subsequently, on November 5 and 6, 2014, the documents submitted by the applicant as well as documents collected in the context of Initial disclosures of another whistleblower were released by the *International Consortium of Investigative Journalists* (paragraph 8 of stop). The record clearly shows that the applicant presented to the national courts convincing arguments (some are mentioned in paragraph 39 of the judgment) to show how the disclosed tax returns - and in particular their annexes - were important to verify and confirm the documents disclosed first place, and to build on these. These arguments have, moreover, been approved by the relevant investigative journalist, who was well placed to assess the importance of the applicant's disclosures for the debate current public on the issue. Therefore, the two series of disclosures appear to have been closely related.

4. It is not disputed that the complainant's revelations presented a general interest (see paragraph 108 of the judgment). National courts have acknowledged that the leaked documents had fostered public debate in the Luxembourg, and even at European level, on corporate taxation multinationals, tax transparency, the practice of "tax rulings" and tax justice in general (see paragraph 21 of the judgment). For jurisdictions internal, the decisive question was *to what extent* this disclosure had responded to the general interest. As we will explain below, we do not think this is the right way to pose the question under Article 10 (see in particular paragraph 8 below).

The weight to be given to the interests of a private employer in business relating to a whistleblower

5. According to the Court's case-law, Article 10 § 2 of the Convention does not leaves little room for restrictions on debate on issues of general interest (*Sürek* v . *Turkey (no o 1)* [GC], n o 26682/95, § 61, ECHR 1999-IV, and *Guja* , cited above, § 74). The exceptions to the principles generals deriving from Article 10 § 1 call for a narrow interpretation, and the need for restrictions must be convincingly established

(*Hertel v. Switzerland* , 25 August 1998, § 46, *Reports of judgments and decisions* 1998-VI, *Steel and Morris v. The United Kingdom* , no.68416/ 01, § 87, ECHR 2005-II, and *Guja* , cited above, § 69).

[1] https://lequotidien.lu/politique-societe/proces-luxleaks-perrin-les-voleurs-nont-pas-ete-condemned / .
[2] *Ibidem* .

6. To assess the proportionality of an infringement of liberty expression of an employee who makes revelations in the general interest, the Court must - according to the "fifth criterion of the *Guja* case law " - assess the weight of any prejudice caused to the employer by the disputed disclosure and determine whether this damage is greater than the interest the public to obtain such disclosure (*Guja* , cited above, § 76). Contrary to the balancing carried out in this case, that carried out in the *Guja* case , which concerned revelations made by a senior public prosecutor general, opposed two types of general interest: on the one hand, interest in informing citizens of pressure and illegal acts in the within the prosecution and, on the other, the interest in maintaining citizens' trust in this institution. In the case of *Heinisch v. Germany* (n o 28274/08, § 89, ECHR 2011 (extracts)), which concerned a public health care provider health, the Court recognized that the balancing could also bring play the (private) interest in protecting commercial success and viability commercial business, for the benefit of their shareholders and their employees, but also for the economic good in the broad sense. Conversely, the Court underlined the general interest in managing public enterprises which meet satisfactory service standards as an argument for disclosures.

7. The “fifth criterion of the *Guja* case law ” must be interpreted and applied in accordance with the overarching principles mentioned in paragraph 5 above. As the Court specifically noted in connection with of the application of this criterion, a free discussion of the issues of interest public is essential in a democracy and care must be taken not to discourage citizens to comment on such problems (*Guja* , cited above, § 91).

8. In my opinion, it follows from these considerations that, once established - as in the present case - that the information disclosed by

the employee was in the public interest, it should be assumed that the disclosures in question are protected by Article 10 of the Convention. In order to rebut this presumption, following the "fifth criterion of the *Guja* case law ", the employer (and, in the context of criminal prosecution) must be required to present compelling reasons, based on concrete and substantial damage to private interests in cause, in order to establish that these clearly outweighed the benefits of disclosure. A less protective approach would lead to greater legal uncertainty capable of deterring future employees from making such disclosures, which would run counter to the fundamental principles that guide the application of the criteria resulting from the *Guja* case law .

9. In addition, the balancing of competing interests in the context of the "Fifth criterion of the *Guja* case law " should not be carried out in isolation, but in light of the comprehensive analysis based on Article 10 which includes all relevant criteria. In other words, the criteria of *Guja* jurisprudence should not be seen as mere boxes

checkmark, but as principles that guide a comprehensive review of national courts. Conversely, this does not mean that we have to admit unfounded disclosures that are made with little regard for the best interests general and / or which cause considerable harm to private interests legitimate.

10. The proposed approach is also supported by recent developments international events in the protection of launchers alert, since the need for enhanced protection in the spheres public and private has been recognized (see paragraphs 50-58 of the judgment). So the Directive (EU) 2019/1937 on the protection of persons who report breaches of EU law (see paragraph 51 of the judgment) does not make protection of whistleblowers from factors related to harm to the employer, as long as the general conditions of protection set out in Article 6 of the Directive are fulfilled.

11. In view of the foregoing, we consider that the Court should have observed take a closer look at how national courts have put in balance the competing interests which were at stake in this case. We note in particular that the considerations arising from the

Guja and *Heinisch* case law were applied in the present case - to our knowledge, the first case relating to a whistleblower who concerns a purely private employer - without taking into account the principles fundamentals of Article 10. Thus, the national courts have founded their decisions on the isolated observation that the "fifth criterion" was not fulfilled, without appreciating the role played by this factor in the overall analysis nor identify compelling private interests that have argued against a disclosure that is generally believed to be in the public interest.

The condition relating to "essential, new and unknown until then "

12. Last but not least, we disapprove of the fact that, in examining the "Fifth criterion of the *Guja* case law ", the national courts are based on the supposed absence of "essential information, new and hitherto unknown "in the applicant's revelations (see paragraph 2 above). In our opinion, this approach does not find any basis in the Court's case-law (see paragraph 13 below), is based on a mistaken view of how public debate works (see paragraph 14 below), may produce a significant deterrent effect (see paragraph 15 below) and is questionable in the circumstances of the species (see paragraph 16 below).

13. The way in which national courts have dealt with the disclosures the applicant's complementary documents hardly fit in with the general position - and one might add common sense - of the Court that the fact that a public debate on a certain issue is underway argues in favor of

new disclosures of information fueling this debate (see, for example, *Dammann v. Switzerland* , no.77551 / 01, § 54, 25 April 2006, and *Colaço Mestre and SIC - Sociedade Independente de Comunicação, SA c. Portugal* , n os 11182/03 and 11319/03, § 27, 26 April 2007).

14. In addition, the distinction made by national courts between first and second series of revelations seem to be based on the idea that, once a public debate has been initiated by the disclosure of certain information, the general interest in receiving information that confirms,

complement or reinforce the initial information is found significantly reduced. Assuming we accept the point of view that the facts disclosed by the applicant in this case were qualitatively less "new" - it was about tax evasion general of companies, and not a fault of the State itself - we are difficult to accept the vision of an instantaneous public debate or frozen in the time. The attitude of citizens on matters of general interest may be constant evolution; in some cases it takes decades argumentation and counter-argumentation before a behavior public or private does not really change. Moreover, if we refer to the object of the revelations made by the applicant in the present case, the complexity of corporate tax policies is hardly the most common topic. accessible to the general public. National courts seem to have underestimated the important power of "illustration" which resides in disclosures similar to those of the applicant: indeed, even when the general outlines of a (perceived) problem are widely known, it is always very useful to sketch the precise dimensions and manifestations. One can, for example, be perfectly aware of the problem of police violence, but the impact of a specific episode of force excessive that was recorded on video may nevertheless be very deep.

15. The approach of national courts, approved by the majority, is likely to have a significant deterrent effect on future whistleblowers in the private sector, because a person who is considering disclosing information that it considers to correspond to the general interest risks making in the face of great uncertainty in determining whether this information will be considered to meet the much higher criterion of "essential, new and hitherto unknown information". In this regard, it is generally recognized that "the field of disclosures giving rise to the right to protection must be easily understood by whistleblowers potential " [3] and that the protection of whistleblowers should not be "[Subject] to subjective and unforeseeable conditions (...), without clear and precise indication of what is expected of the whistleblower

[3] Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 8 September 2015, A / 70/361, paragraph 33.

potential " [4] . The approach adopted by national courts does not hardly with these requirements.

16. Finally, and as the majority expressly acknowledges, the prejudice in the interests of the employer in this case proved to be negligible in terms of long term (see paragraph 102 of the judgment). Consequently, the applicant's revelations must have been considered to have such a low value in relation to of Article 10 that they had to cede in the face of even more insignificant that was on the other side of the scale. If we are aware of the need for some deterrence against disclosures repeated and potentially unjustified concerning the financial market Luxembourgish, we believe that the assessment of the facts delivered by the national courts in the present case is far from convincing (paragraph 3 above).

17. In conclusion, the balancing act carried out by the majority between, on the one hand, the general interest linked to the revelations of whistleblowers and, the other, the private interest in maintaining secrecy, is in conflict with the *Guja* case law of the Court as well as with the new standards European countries in this area. In our humble opinion, this hinders the protection effective whistleblowers in the private sector.

[4] Resolution 2300 (2019) of the Parliamentary Assembly of the Council of Europe, paragraph 12.7.

5.2 Classic retaliation and cover-up tactics

EXCERPTS FROM WHISTLELOWER'S SURVIVAL GUIDE ON RETALIATION TACTICS

CHAPTER 2

The Red Flags

The previous warnings notwithstanding, if you are going to challenge the company that employs you, you must understand how large organizations operate. In particular, you should know how corporate bureaucracies function to target troublemakers and neutralize dissent.

Targeting Dissenters: Tactics of Retaliation

Corporate hierarchies employ intimidation and fear to convince their workers that the power of the organization is stronger than the power of the individual—even individuals who have truth on their side. Often, making an example out of one troublemaker is sufficient to keep the majority silent. The following section illustrates tactics your employer may use to "shoot the messenger" of bad news.

None of these techniques of retaliation is unique or new. More than three decades ago, the classic institutional response to whistleblowers was captured on tape in the instructions of President Richard Nixon to top aides H. R. Haldeman and John Ehrlichman. After learning that Pentagon cost-control expert Ernie Fitzgerald had blown the whistle on $2.3 billion in accounting irregularities in the construction contract of military cargo planes, Nixon said simply, "Fire that son of a bitch."[1]

In 1973 President Nixon took reprisal techniques to a new level. Fred Malek, director of the White House Personnel Office, issued the "Malek Manual," a secret report on how to purge the career civil service system of "unresponsive" employees—whistleblowers or Democrats—without running afoul of the law. The following reprisal tactics are drawn largely from the Malek Manual and apply equally to corporate and federal government employees, though we draw our illustrations primarily from the

private sector. Ironically, whistleblowers exposed the Malek Manual, and it was published in the Watergate Committee's report.[2]

Keep in mind that the following list is not exhaustive; the forms of harassment are limited only by the imagination and, as in Orwell's *1984*, likely will be customized to strike at a whistleblower's unique vulnerabilities. Further, they vary in intensity. There is a direct relationship between the significance of a whistleblower's threat and the severity of the retaliation. Often the higher up the chain of command the whistleblower sits, the greater the perceived threat and the more vicious the retaliation.

Spotlight the Whistleblower, Not the Wrongdoing

This is also known as the smokescreen tactic, and it operates almost like a knee-jerk instinct. The first imperative of retaliation is to make the whistleblower the issue: obfuscate the dissent by attacking the source's motives, credibility, professional competence, or virtually anything else that will work to cloud the issue. The point is to direct the spotlight at the whistleblower instead of the alleged misconduct.

A typical initial management response to a whistleblower's disclosures is to launch an internal investigation and retaliate against the employee on trumped-up charges. Retaliatory travel, reimbursement, and time audits are so common they could be classified as bureaucratic knee-jerk reactions against whistleblowers. Allegations of everything from sexual harassment to stealing paper clips are possible—even charges that have already been investigated and discredited. Moreover, smears of alleged misconduct similar to what the whistleblower is exposing are not unusual.

Chutzpah in selecting the smear charges is a common tactic to demonstrate the organization's invincibility. Soft-spoken, humble individuals have been branded loudmouth egomaniacs. There is no limit to the petty and outrageous depths to which an unscrupulous employer may be willing to sink. An example is charging an employee with gambling at work for buying a charitable raffle ticket from a colleague.

Often a private security firm will be hired to do the dirty work of investigating a whistleblower. Sometimes investigations and surveillance are conducted by "babysitters," spies assigned by management to "assist" the whistleblower. Increasingly, employers also seek criminal prosecution

for theft or misappropriation of company property—materials that are frequently the very evidence of illegality being used by the whistleblower.

Richard Parks and Wrongdoing at Three Mile Island

When Three Mile Island engineer Richard Parks challenged sloppy cleanup practices that could have triggered a nuclear meltdown, his employer's first reaction was to brush aside the safety issues and place Parks under investigation for an alleged financial conflict of interest. The company's search for incriminating evidence took on some extreme measures. Parks returned home one day to find that his house had been broken into and ransacked. Parks was not vindicated until he went public and sought help from the Department of Labor (DOL), Congress, and the Nuclear Regulatory Commission (NRC). All three acknowledged the substance of his claims, and after a six-month investigation the NRC ordered his employer to redo the entire cleanup with revised procedures and to conduct extensive safety tests.[3]

A related technique is to open an internal investigation—and then deliberately keep it pending for an indefinite period. The idea is to leave the whistleblower twisting in the wind, with the clouds of an unresolved, never-ending investigation hanging over his head. Indeed some whistleblowers endure a series of nearly seamless investigations for decades. The intent is not only to create uncertainty and stress but also to undermine the whistleblower's credibility. Potential media, government, and other officials may be discouraged from listening to and taking seriously the allegations of a whistleblower who is "under investigation." A related tactic is "chain witch hunts," in which a new investigation is opened as soon as an old one is closed without action.

Spotlighting whistleblowers, as opposed to their claims, often involves public humiliation—the bureaucratic equivalent of placing them in the public stocks. When Resolution Trust Corporation (RTC) enforcement attorneys Bruce Pederson and Jacqueline Taylor protested political sabotage of savings and loan prosecutions, they were publicly denigrated and assigned to work in buildings not staffed by any other RTC employees, such as the cafeteria.[4] Psychiatric fitness-for-duty exams are one of the ugliest forms of retaliation and have long been used as a way to spotlight the whistleblower. At the same time, companies can hide

behind privacy laws to hint that there is a problem with the employee that the corporation is not at liberty to disclose.

"Crazy Like a Fox"

When Dr. James Murtagh, a physician at Atlanta's Grady Hospital, blew the whistle on fraud involving the hospital's federal medical care grants, an alert was issued that he was armed and dangerous. He was alleged to be mentally unstable and ordered to keep off the hospital grounds, with instructions to security that he could be dangerous. Eventually, Dr. Murtagh successfully settled a Federal False Claims Act lawsuit against the hospital for $1.6 million and organized other Grady whistleblowers into a relentless coalition that led to widespread white-collar prosecutions, including the felony conviction of a notorious Georgia state senator for his involvement in an extensive corruption scandal. Dr. Murtagh resumed his career and has become a leader in the whistleblower community, organizing two national conferences.

Build a Damaging Record against the Whistleblower

This tactic goes hand in glove with spotlighting the whistleblower. Not infrequently, companies spend years manufacturing an official personnel record to brand a whistleblower as a chronic "problem employee" who has refused to improve. The idea is to convey that the employee does nothing right. In truth, many whistleblowers have a history of sterling performance evaluations—*until* this tactic is used against them.

An employer may begin by compiling memoranda about any incident, real or contrived, that projects inadequate or problematic performance on the job. This is often followed by a series of confrontational "counseling" sessions, in which the employee is baited to lash back. Reprimands and comparatively mild disciplinary actions are taken first, in part because the employee has few (if any) due process rights in defense and in part because company policy may require progressive discipline. By the time something more serious such as termination is proposed, the employer is armed with a long and contrived history of "unsatisfactory performance."

The Wayward Whistleblower

Several years ago an individual herein pseudonymously referred to as John Doe began working at a major US pharmaceuticals production facility. This facility was charged with manufacturing a new infant vaccine for meningitis and pneumonia. Doe's role was to ensure that the facility's employees were sufficiently trained to the level required by Food and Drug Administration (FDA) standards. He soon became aware of gaps and shortcuts that were being taken both with the employees' training and with the manufacturing process itself. These shortcuts in the training program were particularly alarming because producing biological vaccines required more-complex processes than regular pharmaceutical production.[5]

Doe's concerns led him to send a written memorandum to his supervisor, explaining that the facility was not satisfying FDA regulations and the company's own code of conduct and that he would not be complicit in misrepresenting that fact. Doe filed complaints with both the company's Office of Compliance and its Office of Ethics and revealed the depth and the breadth of manufacturing, quality assurance, and product release problems to one of the company's attorneys. He was told that the resulting investigation found no problems with the facility, though internal memoranda unearthed later in discovery revealed a much different picture.[6]

Two months later Doe was placed on a personal improvement plan (PIP) for 90 days. The PIP stated that he had to stop making comments to anyone regarding the company's noncompliance with training requirements.[7] Doe was promptly suspended and fired two months later, after he had a hostile encounter with the human resources director at a holiday party.[8] It later surfaced that this manager was brought in to "deal with" Doe after his predecessor was terminated for refusing to fire Doe and that the manager himself was later dismissed for cause, including harassment, expense report "discrepancies," and unauthorized disclosure of proprietary information to a competitor.

Doe filed a lawsuit against his former employer under the then recently enacted Sarbanes-Oxley Act, claiming his termination was in retaliation for calling attention to the regulatory violations. It became a major test case warning of the new law's frailty. A federal magistrate dismissed the case, reasoning that the reported violations were immaterial to shareholders and therefore not within the scope of Sarbanes-Oxley. The Fourth Circuit Court of Appeals agreed. The law's new boundaries cancel protections for warnings, disclosures of risk, or even actual illegality unless the government punishes the company in a way that is severe enough to damage shareholder

value. Under this standard, Sherron Watkins would not have had whistleblower rights when she warned CEO and Chairman Ken Lay of the risks from Enron's fraud. Doe's fate was not an aberration. The devastated legal landscape is discussed more fully in chapter 6.

In addition, the judge was swayed by the drug company's contention that Doe would have been fired regardless of his whistleblowing efforts—pointing to the hostile incident at the holiday party and the fact that Doe was reprimanded for professional misconduct prior to his initial memorandum.[9] Doe's advice to future whistleblowers: Don't rely on codes of conduct, agency investigators, or the courts to protect you."The best way to blow the whistle is to gather all of the facts yourself and anonymously provide the evidence to a newspaper reporter. Then, walk away and find another job."

Threaten Them

Warning-shot reprisals for whistleblowing, such as reprimands, often contain an explicit threat of termination or other severe punishment if the offense is repeated. In some cases employees may have signed nondisclosure agreements as a condition of employment. The penalty for violating these agreements, which typically fail to outline legitimate exceptions for fraud, waste, or illegality, includes the threat of criminal sanctions.

A Tobacco Scientist Blows the Whistle

Dr. Jeffrey Wigand was a scientist and a manager who had worked in different aspects of the corporate world for much of his adult life, including at Union Carbide and Johnson & Johnson, before he was recruited for a position at Brown & Williamson Tobacco Corporation (B&W), one of the four largest cigarette manufacturers in the United States. Dr. Wigand was given a prestigious position as head of research and development, a large salary, and what he thought was a good opportunity to help develop a safer cigarette.[10] He was not blind to the moral difficulties that his position might entail, but the offer was too good to turn down.

As Dr. Wigand settled into his position, his illusions of helping the public faded. B&W's"safer cigarette" was not high priority, and research was canceled. He discovered that the lab was sorely out of date and did not have any staff on hand to perform thorough toxicological and chemical analyses or to assess the propensity of a given cigarette formulation to start fires.[11]

He was sent to an orientation session on tobacco litigation and found out that B&W retained scientists only to help shield the company in the event of a lawsuit. In addition, "document management" was practiced to keep information away from any discovery process.[12] These practices and more made Dr. Wigand increasingly wary of his employer. Nevertheless, he continued working for B&W for four years until he was fired in 1993.[13] The company was not pleased with Dr. Wigand's efforts to determine the health effects of some cigarette additives and terminated him. While he was looking for other jobs, B&W sued him for breach of contract, eventually forcing him into signing a stringent confidentiality agreement to retain his medical benefits and severance package.[14]

The corporate bullying had the opposite of the desired effect. Dr. Wigand decided that instead of just walking away, he would fight back. Through an intermediary, he was connected with a *60 Minutes* producer, Lowell Bergman, who had a stack of internal tobacco industry documents that he could not fully understand.[15] This initiated a series of events that ended in the extensive tobacco industry trials of the midnineties. Despite threats and delays, and emboldened by the *Wall Street Journal*'s printing of Dr. Wigand's depositions, *60 Minutes* eventually ran multiple stories revealing the tobacco industry's flagrant disregard of the health of its customers. The industry did not want to make "safer" cigarettes or ones that were more resistant to starting fires.[16] The November 1998 master settlement agreement between US state attorneys general and the four largest cigarette manufacturers that resulted from the tobacco suits was one of the largest in US history, some $206 billion.[17]

These victories were not easy ones for Dr. Wigand, however. He received multiple death threats.[18] Every moment of his past life was scrutinized by B&W, which spent more than $8 billion on a 500-page smear campaign. Anything that could be twisted and used against him was put into the public record.[19] His marriage ended, and he was distanced from his family. Amidst the showdown of 1996, Dr. Wigand's attorneys hired a private investigation firm to dismantle the campaign against his character. Dr. Wigand was compelled to travel with a bodyguard.[20]

In the end, however, his testimony worked and was one of the linchpins of the government's prosecution. Dr. Wigand stood up to some of the biggest bullies of the corporate world and defeated them. After leaving B&W he began a new career as a high-school Japanese and science teacher and has been recognized as a Fannie Mae First Class Teacher of the Year. He also runs Smoke Free Kids, an organization to combat teen tobacco use.[21]

Isolate Them

Another retaliation technique is to transfer the whistleblower to a "bureaucratic Siberia." Similar to public humiliation, the isolation makes an example of the whistleblower while also blocking the employee's access to information and severing contact with other concerned employees. Moreover, like any good retaliation tactic, isolation puts pressure on the whistleblower to be compliant or resign.

Employers may also isolate whistleblowers by forcing them to work from home or take administrative leave with or without pay. They may be moved around within the same building to a new office with dim lights, dreary surroundings, and no desk or phone. Isolation does not necessarily require geographic relocation, however, as it may be sufficient to take away the employee's work duties, position, or clearance. This technique has been called the "potted palm" gambit because the employee's new post-whistleblowing duties are as extensive as those of an office plant.

Set Them Up for Failure

The converse of retaliating against whistleblowers by stripping them of their duties is the tactic of putting them on a "pedestal of cards." This involves setting whistleblowers up for failure by overloading them with unmanageable work and then firing or demoting them for nonperformance. This tactic commonly includes making it impossible to fulfill assigned responsibilities by withdrawing the necessary privileges, access, or staffing. Another variation of this tactic is to appoint the whistleblower to solve the problem he exposed and then make the job impossible through a wide range of obstacles that undercut any possibility of real reform. The employee may then be turned into the scapegoat and fired for incompetence when the problem is not solved. In extreme cases this retaliatory tactic may extend to setting the whistleblower up for criminal charges, disciplinary action, or even injury, such as by ordering people with poor backs to move heavy furniture.

Physically Attack Them

Karen Silkwood from Oklahoma's Kerr-McGee nuclear facility was killed after her car ran off the road on the way to meet a reporter under

circumstances that led many to suspect murder. Shortly after Dr. James Murtagh successfully settled his False Claims lawsuit and made FBI disclosures in a political corruption case that sent the Georgia State Senate leader to prison, he was hospitalized for arsenic poisoning.[22] Dr. Jeff Wigand experienced anonymous death threats against himself and his loved ones. These whistleblowers' fates demonstrate the risk of physical retaliation for speaking out. Physical attacks on whistleblowers are not common but do occur. Sometimes organizations encourage or wink at "the boys" who do their dirty work, as the whistleblower gets beaten up by thugs on the work floor. Sometimes physical retaliation is more subtle. Whistleblowers at nuclear or chemical facilities may find themselves assigned to work in the hottest radioactive or toxic spots in the plant.

Eliminate Their Jobs

Another common tactic is to lay off whistleblowers even as the company is hiring new staff. Employers may "reorganize" whistleblowers out of jobs or into marginal positions. A related tactic is to eliminate—through reorganization—the structural independence of particular oversight units. A nuclear engineering firm may de-emphasize the quality control department by making it a component of the production staff.

"Reorganizing" Whistleblowers' Jobs at Fluor

Created as part of the Manhattan Project and operating in secrecy for more than 40 years, the Hanford Nuclear Reservation located in Washington State supplied plutonium for the federal government's nuclear weapons program. In 1989 all production ended and the Department of Energy, the Environmental Protection Agency (EPA), and the Washington State Department of Ecology began a concerted cleanup effort of the widespread hazardous chemical and radioactive waste.[23] Fluor Federal Services Inc. was hired by the Department of Energy to assist with the cleanup.

Fluor's crew at the Hanford site was instructed to install a particular kind of valve on a system of pipes used for handling the highly radioactive nuclear waste. The crew of seven refused to obey, however, because they feared that the underrated valves would burst, potentially causing the leakage of millions of gallons of radioactive waste into the surrounding environment.[24] Because of their protests, stronger valves were used, but all seven

workers were laid off within days. They brought a retaliation claim against Fluor, which later agreed to reinstate them.[25]

Unfortunately, Fluor fired seven other employees to make room for the original workers.[26] This was both unexpected and unnecessary. It seemed to be an effort to cause tension between the seven rehires and the rest of the crew. One Fluor executive even spread a false rumor that the seven original workers agreed to the layoffs as part of their agreement.[27] In a matter of months, five of the original workers were once again laid off along with six others who testified on their behalf, were witnesses, or were merely too closely associated with them. The eleven newly fired workers filed another claim against their former employer for wrongful termination. The case came before a jury this time, and the workers were awarded more than

$4.7 million in damages for both back pay and emotional distress.[28] The verdict was upheld by the Washington State Supreme Court and the case finally ended in 2008.

Paralyze Their Careers

An effective retaliation technique—and one that also sends a signal to other would-be dissenters—is to deep-freeze the careers of whistleblowers who manage to thwart termination and hold on to their jobs. These employees become living legends of retaliation when employers deny all requests for promotion or transfer. A related tactic is to deny whistleblowers the training needed for professional development. The message is clear: "She is going nowhere."

Bad references for future employment openings are common, and any whistleblower settling a legal case should be careful to take this into account. Sometimes this tactic can be subtle, using buzzwords to signal that a former employee should not be hired. Common examples are statements that an employee "is not always a team player" or "needs to work on maintaining cooperative relationships."

They Would "Make Sure I'd Never Work Again"

Inez Austin was a senior engineer–turned–whistleblower at the 586-square-mile former plutonium production facility in Washington State known as the Hanford site. An employee of Westinghouse Hanford, a company con-

tracted by the Department of Energy at Hanford, Austin served as a member of a task group responsible for certifying the safety of cleanup procedures.

In June 1990, after her warnings about the dangers of a plan to pump radioactive waste from an aging underground single-shell tank to double-shell tanks went unheeded, Austin refused to approve the process. She was concerned that the ferrocyanide present in some of the tanks was potentially explosive and posed the risk of widespread radioactive contamination. In the face of pressures to meet deadlines and maintain productivity, Austin's proposal to postpone the pumping and conduct more research was met with threats of disciplinary action by company management.[29]

In further retaliation, Austin received the lowest performance rating in her 11 years at Westinghouse. She was labeled as mentally unstable and asked to see a psychiatrist. Her office was moved to a dusty trailer that provoked her asthma and where she was given inconsequential work assignments.[30] She was the target of illegal wiretapping, interception of her mail, and a house break-in.[31]

When Austin filed an official harassment complaint with the DOE, Westinghouse offered her a new position, a month of paid leave, a clearing of her personnel files, and attorney's fees if she dropped the charges. She accepted but then found herself isolated from any meaningful work assignments for the next three years. After being demoted in October 1993, Austin called a news conference and told the press of this continuing retaliation. Media pressure landed her a position as an environmental compliance officer for Westinghouse.[32]

In 1995 Austin again felt compelled to disclose questionable prac- tices at the Hanford site, including allowing untrained workers access to restricted areas. Again her warnings were not well received, and she lost her job in February 1996. Austin finally took her story to the secretary of energy and filed a complaint with the Department of Labor, which ruled in her favor. She also sued Westinghouse Hanford in state court for harassment and wrongful termination and eventually settled out of court.[33]

Unfortunately, Austin's long-running problems were not over. "They [Westinghouse Hanford] told me that they'd'make sure I never work again,'" said Austin in 1998, "and so far, that's been true."[34] Indeed it took her three years and hundreds of résumés to find another job, a position with the Oregon Department of Environmental Quality enforcing solid waste and water quality standards that entailed a daily 80-mile commute. Despite her troubles, Austin stands by her efforts to protect the health and the safety of the public and her fellow cleanup workers. "I can't see how I could have done anything differently, and believe me I have had time to think about it."[35]

Blacklist Them

Sometimes it is not enough merely to fire or make whistleblowers rot in their jobs: the goal is to make sure they "will never work again" in their chosen field or industry. After several oil-industry whistleblowers exposed illegal pipeline practices, for example, the company placed them on a list of workers "not to touch" in future hiring. It does not matter whether you are completely vindicated. As Professor Alford summarized the experience of a Medicare fraud whistleblower, "Her boss went to jail, but she couldn't get a job in the state where she worked. 'They were all afraid I might commit the truth.'"[36]

Blacklisting Dunn

Resolution Trust Corporation whistleblower Richard Dunn, a quiet financial management expert, blew the whistle on overbilling by contractors who were seeking to exploit failed savings and loans. After being terminated by RTC, he recounts trying to make a fresh start with a big-name accounting firm. A week into this new job, however, Dunn was summarily dismissed. He later learned that RTC had undermined him by telling his new boss that he had been fired for threatening a co-worker with a gun, thus making him ineligible for the new position. The firearms allegation lacked any substantiation in RTC's personnel records or elsewhere.[37]

Employers in scientific professions have exercised some of the ugliest forms of blacklisting. Dr. James Murtagh has endured a steady pattern of receiving new jobs in supportive environments just to get terminated without explanation within weeks. He subsequently found that his former employer had posted the equivalent of a smear dossier about him on its website. Another creative method is extradition. Whistleblowing foreign nationals at university laboratories, including students, have been warned that their visas will not be renewed and that the Department of Homeland Security is available to ensure their departure. Many other forms of retaliation against scientists have also arisen.

These experiences are not unique. They illustrate what you can expect. A massive study by Dr. David Welch, a pioneer SOX whistleblower whose seven-year ordeal illustrated the unreliability of those rights, summarizes what you can expect based on 27,000 whistleblowers'

fates from 1994 to 2008 who filed retaliation complaints with the Occupational Safety and Health Administration (OSHA):

- 78 percent struggled financially for the first five years after blowing the whistle;
- 83 percent found it "extremely difficult to impossible" to find a new job in their field;
- 66 percent found it "extremely difficult to impossible" to find a new job after changing professions;
- 54 percent could not find work until they changed professions.[38]

Neutralizing Dissent: Tactics of Cover-Up

The point of the tactics just described is to overwhelm whistleblowers in a struggle for preservation—to undermine their credibility, career, family, finances, and even sanity until they are silenced and the issues that triggered the whistleblowing are forgotten. Typically, these tactics are only one of two fronts. In addition to "shooting the messenger," employers also strive actively to bury the message by covering up the alleged wrongdoing.

Employers often rely on longstanding secrecy tactics to camouflage institutional misconduct. Large corporations will devise systems and written or unwritten policies for keeping dissent—including information about possible wrongdoing—from surfacing or creating problems for the company. Some are standing policies. Others are adopted when companies become aware of their own wrongdoing and seek to avoid getting caught. Still others are put into place as a means of damage control after a whistleblower has publicly exposed an instance of misconduct. Illustrative tactics follow.

Gag the Employees

The most direct way to silence potential whistleblowers is to gag employees through repressive nondisclosure agreements as a job prerequisite or by excessively designating information as "proprietary" or with government contractors as "classified." Private employers often build gag orders into company manuals or employment contracts and then enforce them

through civil suits for breach of contract or theft of proprietary information. More subtly, companies routinely order staff not to respond directly to the media or community but rather to refer all inquiries to an in-house public relations office.

Fighting a Gag Order on Nuclear Employees

At the Knolls Atomic Plant near Schenectady, New York, workers were threatened with termination, a $100,000 fine, and life imprisonment if they commented on operations at the facility. The gag order was issued sitewide following a visit by GAP attorneys who spoke to workers about radiation leaks.[39] Several plant employees and their labor union subsequently filed suit against General Electric, the plant's owner, and the US Department of Energy, seeking declaratory and injunctive relief.[40] They claimed the gag order violated their First Amendment right to free speech because GE was acting as a government contractor. Although the case was pending, the plant issued a second newsletter clarifying that any security policy"must be read in the context of the applicable statutes and regulations"and could not be used "to prevent proper reporting of matters involving compliance with health, safety, or environmental standards." As a result, the district court dismissed the case because this second newsletter rightly acknowledged the constitutional limits of the plant's ability to silence its employees.[41]

Study It to Death

A related tactic is to launch an investigation that is toothless or never ends, leaving the allegations of wrongdoing unresolved.

Roger Boisjoly and the O-Ring Taskforce

Roger Boisjoly was an engineer for the firm Morton Thiokol, which contracted with NASA to work on the solid rocket boosters of the space shuttle *Challenger*. Boisjoly claims that any engineer who worked on the *Challenger* knew it was doomed to fail, and so did NASA's upper management. By studying the solid rocket booster's O-rings, the engineers determined that they repeatedly failed to seal at 53 degrees or below. They also determined that if the primary seal was destroyed, the O-ring would almost certainly be destroyed.[42]

In January 1985 Boisjolywrotealettertohismanagersaboutthepossible effects of the faulty O-rings and requested that Morton Thiokol take action.

Initially, his managers simply labeled his letter "private" and filed it away. Morton Thiokol was negotiating a new contract with NASA, and presumably Boisjoly's concerns might have compromised its renewal prospects.[43]

Nevertheless, after several more memos, the company commissioned a "task force" that included Boisjoly to investigate the matter further. Boisjoly soon found out that the task force lacked the power, resources, and management support to serve any meaningful purpose. No further tests were performed on the O-rings, and no further action was taken to address the issue.[44]

On the morning of the launch, Florida experienced record low temperatures that the O-rings could not handle. Boisjoly and his fellow engineers formed a group to petition NASA to stop the launch. Despite the findings about the O-rings, however, Morton Thiokol advised NASA that its data was inconclusive and NASA proceeded with the launch. The *Challenger* exploded 73 seconds after its launch and all aboard were killed—one of the worst disasters in NASA's history. After the crash Morton Thiokol managers tried to claim they did not know about the faulty O-rings, but Boisjoly testified against them. Boisjoly was then shunned by colleagues and managers until he eventually resigned.[45] Though too late to prevent the catastrophe, his concerns were ultimately validated.

Separate Expertise from Authority

The goal of this tactic is to ensure that corporate loyalists make all the important decisions, even technical judgment calls, with only a limited advisory role for the experts.

When NASA Sidelines the Experts...

As just described, Morton Thiokol's engineers were overruled by NASA managers determined to launch the space shuttle *Challenger* in 1986, even though all the company's practicing engineers opposed the decision.[46] Morton Thiokol's management admonished these engineers for not taking off their "engineering caps" and putting on their "management caps." Managers, of course, had their reasons not to postpone the launch of the *Challenger*, for one, so that President Ronald Reagan could refer to the orbiting space vehicle during his State of the Union address to Congress that evening.[47]

One variation of this tactic is to use a rigged version of "the democratic process" to control information and outcomes. Other experts—selected for their proven loyalty—are called in to "out-vote" the whistleblower, effectively overruling the scientific method. A more subtle version of this technique is to misuse the peer review process, either as a discrediting tactic by packing the panel with a particular bias or as a stalling tactic by instituting duplicative or unnecessary reviews. This has also become a popular harassment technique against medical whistleblowers. Whistleblowers, their charges, or both are condemned after secret hearings in which they are not allowed to know or respond to the specific issues or evidence. In some instances whistleblowers are not even permitted to participate, and no formal record of the proceedings is kept.

Institutionalize Conflict of Interest

Institutions accused of wrongdoing routinely initiate probes into their own misconduct. In many whistleblower cases, this is the equivalent of appointing the fox to guard the henhouse.

In one sense, it is only fair (and more efficient) to allow companies a chance to resolve allegations and straighten out internal problems. That is the point of internal checks and balances; corporations should be responsible for internal housecleaning. But when confirmation of misconduct could create liability or when individual business leaders are the direct cause of misconduct, this approach inevitably places in-house investigations in a conflict of interest.

Fannie Mae's Troubling Internal Investigations

In 2003 three Fannie Mae employees expressed serious concerns about their firm's accounting. For six years Fannie Mae had promoted a false image of financial security through the systematic use of inappropriate accounting and improper earnings management. This resulted in the company's overstating its income by an estimated $10.6 billion. The board of directors allowed the problem to continue by failing to exercise oversight of Fannie Mae's operations even after the three employees brought it to light.[48]

Roger Barnes, then a manager in the controller's division, made serious allegations about Fannie Mae's accounting for deferred price adjustments, which were promptly passed on to Ann Kappler, senior vice president and general counsel. Similarly, Michelle Skinner, director for e-business,

expressed her reservations to Chief Operating Officer Daniel Mudd, which were echoed by Anthony Lloyd, a securities analyst in the controller's office.[49] Kappler was given a hand in the internal investigation of all three disclosures and was soon found to be making false and misleading statements about the issues raised and their disposition, even to the audit committee of the board of directors.[50]

In violation of Sarbanes-Oxley, Kappler then failed to ask the audit committee to conduct an independent review of Barnes's allegations. When the committee did investigate the complaint, it revealed that a $6.5 million adjustment had been made without explanation or documentation.[51] This was just one of several unexplained adjustments about which Barnes expressed concern. The auditing staff, however, said they could not determine one way or the other whether the adjustment was appropriate and ended their investigation.[52] Clearly, the Barnes investigation should have been expanded to determine the extent of undocumented adjustments. Instead the investigation was abruptly brought to a close because of the purported immateriality of the amount involved.

Kappler's legal department also conducted an investigation into Barnes's allegations but completed its investigation in just four days. Fannie Mae was eager to conclude this investigation because of an approaching deadline regarding its yearly financial statements. If these statements were delayed, Fannie Mae would have to explain why. Kappler signed a letter for this statement that included the following:

> To the best of my knowledge, there were no omissions or misstatements of reported amounts or information in my area that would have had a material impact on the financial statements. For purposes of this statement, matters were generally not considered material if they involved an aggregate absolute value of less than $5 million of net income or $3 billion of balance sheet impact. However, I also considered all the factors in determining whether a matter was material and matters involving less than this amount were material if they would otherwise be of interest to a reasonable investor.[53]

As Kappler was well aware, Barnes had uncovered a flaw greater than her $5 million floor of materiality. It is unknown whether she realized this inconsistency at the time, but she never withdrew her certification.

In October 2003 Barnes's counsel sent a letter threatening to file suit against Fannie Mae for violations of SOX whistleblower provisions, discrimination, and retaliation. This letter included an anonymous letter Barnes sent in September 2002, listing questionable financial decisions with a possible impact of hundreds of millions of dollars. In November 2003 Fannie Mae

hurried to settle the matter with Barnes. As part of the settlement, Barnes quit and returned all documents he maintained during his employment, including those kept to support his allegations.[54]

Though the documents included enough information for Fannie Mae to conduct an internal investigation, Fannie Mae still did not become the vehicle for accountability. About one month after Barnes's first complaint, Michelle Skinner made similar complaints to Mudd. An investigation into her concerns validated most of them, yet Kappler once again determined that Fannie Mae's accounting practices were proper and distributed a response to Skinner's concerns to this effect.[55] Fannie Mae was ultimately fined $400 million by the Office of Federal Housing Enterprise Oversight and the SEC.[56]

Keep Them Ignorant

Like government-classified national security information, companies' information may be restricted to a "need-to-know" basis. Taken to the extreme, this policy can be misused to hide the truth and thereby keep employees too ignorant to threaten the corporation. There is often a link between this tactic and various others, such as isolation and internal reorganization. Employers may seek not only to punish the whistleblowers but also to make it impossible for them to access information and evidence. When information is power, ignorance is anti-bliss.

Fostering Ignorance at Diablo Canyon

Managers at the Diablo Canyon nuclear plant also used transfers to enforce ignorance. Charles Stokes was an engineer who blew the whistle on falsification of results in the plant's seismic design review after discovery that blueprints for the twin reactors were backward, compared with how the facilities were constructed. His disclosures convinced the Nuclear Regulatory Commission to order that all the engineering calculations be redone. Management made sure that it would not fail again with a curious tactic. It transferred out Stokes and other dissenters, substituting replacements unfamiliar with the job history and obedient enough not to ask questions about unrealistic assumptions that made key calculations impossible to fail.[57]

On occasion, employers isolate whistleblowers from the evidence through a longstanding labor-management technique: physically locking them out. More subtly, employers can keep whistleblowers from gathering evidence of wrongdoing by strangling them in red tape. Managers may pull out technicalities and obscure subsections of procedures to paralyze efforts at gathering and disclosing information. Similarly, revoking an employee's security clearance is both a tactic of retaliation and a technique for hiding damaging information from those workers who would otherwise have access to it.

Procter & Gamble Keeps Its Researchers in the Dark

Depriving scientists of access to their own research is a common tactic for enforcing ignorance in that profession. Consider the case of Dr. Aubrey Blumsohn, a researcher at Sheffield University in England. Sheffield entered into a contract with Cincinnati-based corporate giant Procter & Gamble (P&G) to study the response to therapy involving the company's osteoporosis drug, Actonel. P&G sought to conduct research that would cast Actonel in a good light in comparison with Merck's Fosamax, the industry leader.

A double-blind study was conducted, where neither researchers nor patients knew if a patient received Actonel or a placebo. To make sense of the data, Blumsohn needed the randomization codes to identify which patients got the drug and which got the placebo. P&G instead gave Blumsohn its own incomplete summary of the data. Blumsohn repeatedly asked the company for the full data set.[58] P&G persisted in its refusal, however, asserting that the data was proprietary. To make matters worse, not only did P&G withhold from Blumsohn the information necessary to make sense of his own research but the company also began publishing abstracts ghost-written in Blumsohn's name, asserting various research findings about Actonel.

When P&G finally permitted him to review the data on a computer screen in England, Blumsohn observed that 40 percent of the data were missing in some of the graphs—data that later proved critical to the way in which P&G had misrepresented the study's findings.[59] When Blumsohn finally got the data, it showed that the results did not favor Actonel.[60] Blumsohn is now preparing to publish a corrected version of the find- ings. Incidentally, other researchers, most notably the research dean of

Blumsohn's institution, have admitted misinforming a medical journal about access to data in a related P&G study and acknowledged that key reported findings in that study were also false.[61]

Prevent the Development of a Written Record

When policies or suspect activities are indefensible, wrongdoing can best be obscured by keeping the evidence oral. This can be enforced by employer fiat, peer pressure, overscheduling (to ensure that there is not time to construct a written record), purging files—both electronic and hard copy—and "off-the-record" backdoor meetings. Managers recognize that it is difficult for whistleblowers to build a case against them without a paper trail. Verbal orders and agreements diffuse accountability over time and inevitably pit the whistleblower's word against that of his superior.

Rewrite the Issues

One of the more insidious corporate strategies is to trivialize, grossly exaggerate, or otherwise distort the whistleblower's allegations—and then discredit the employee by rejecting the resulting "red herring." A whistleblower who challenges that superiors overlooked problems on the job may, for example, find the concerns exaggerated into allegations of willful misconduct—thus stretched beyond credibility. The corporation then finds that, although mistakes were made, the employer committed no intentional violations. The charges are dismissed, the whistleblower is discredited, and the targets of the investigation promptly issue public statements that they are pleased to be exonerated.

Rewriting the record can degenerate into outright censorship. This may involve deleting evidence or issues that are too hot to handle—and therefore vanish from the ensuing investigative report. In other cases, the findings are "massaged" through edits that ensure that they will not be interpreted as significant. An investigative report—even one diluted by rewritten allegations, censorship, and neutered recommendations—can still be damaging to wrongdoers. As a result, a related technique is to issue a press release declaring that the investigation had concluded

that there was no wrongdoing—but then refuse to release the report containing the record of the investigation.

Scapegoat the Small Fry

Just as corporations may trivialize allegations of wrongdoing by rewriting them, they may lower the scandal volume by shielding institutional leadership from accountability. Instead they target those who do not have a support constituency or who were only following orders from higher-ups.

How a Company Shifted the Blame onto a Government Official

Even regulatory bureaucrats are not immune from corporate attempts to shift the blame. Dr. Victoria Hampshire was an adverse drug event coordinator for the Food and Drug Administration, which required her to monitor animal drug–related problems reported by consumers and veterinarians. In 2001 the FDA approved the drug ProHeart 6, used to prevent heartworm in dogs. As part her postmarket review of the drug, Dr. Hampshire found the incoming data disconcerting. Between 2003 and 2005, more than 5,500 adverse drug event reports came in related to ProHeart 6, including almost 500 canine deaths.[62] Dr. Hampshire first notified other FDA officials of her concerns in 2003, and after a few more attempts succeeded in getting their attention. The drug was recalled in 2004.[63]

Wyeth Pharmaceuticals, the manufacturer of ProHeart 6, requested a review of the FDA decision and launched its own purported investigation into Dr. Hampshire, which, according to her, amounted to little more than an unsuccessful effort to plant evidence of a conflict of interest. After Wyeth presented the "findings" of its investigation to the FDA, the agency removed Dr. Hampshire from the ProHeart 6 review and, without notice or explanation, initiated its own criminal probe of Dr. Hampshire.

The charges were unsubstantiated, however, and the US Public Health Service awarded Dr. Hampshire an achievement medal for her work in 2005 and named her Veterinarian of the Year for 2006. The US Senate Committee on Finance launched its own investigation into the appropriateness of the actions taken by the FDA and Wyeth. In a February 6, 2008, letter to the heads of the FDA and the Department of Health and Human Services, ranking committee member Charles Grassley concluded that "by mishandling an investigation and submitting material to law enforcement that was rife with error, FDA not only wasted resources, it created serious doubts about the integrity of its processes."[64]

These are but a few of the techniques employed by corporate bureaucracies to contain and eliminate dissent. Knowing the potential responses to your whistleblowing will help you prepare for the worst. Nonetheless, remember that corporate ingenuity always creates new and unanticipated innovations reflecting creativity's dark side.

---

6. List of attendees

PUBLIC INSTITUTIONS			
1	Emiljano Kondi	High Inspectorate of Declaration and Audit of Assets and Conflicts of Interest	Albania
2	Enela Duro	Ministry of Education and Sports	Albania
3	Ivana Ljubicic	Ministry of Justice	Bosnia and Herzegovina
4	Aleksandar Damjanovic	Ministry of Justice	Bosnia and Herzegovina
5	Emir Mehmedovic	Ministry of Justice	Bosnia and Herzegovina
6	Mevludin Dzindo	Agency for the Prevention of Corruption and Coordination of the Fight against Corruption	Bosnia and Herzegovina
7	Sanela Latic	Ministry of Justice	Bosnia and Herzegovina
8	Martina Abrasheva-Kancheva	Commission for Anti-Corruption and Illegal Assets Forfeiture	Bulgaria
9	Matea Miloloza	Office of the Ombudswoman	Croatia
10	Sedina Dubravcic	Ministry of Justice and Public Administration	Croatia
11	Diana Mazniuc	People's Advocate	Moldova
12	Stela Rusu	National Anti-corruption Centre	Moldova
13	Dejana Balic	Agency for Prevention of Corruption	Montenegro
14	Nikola Rakocevic	Clinical Center	Montenegro
15	Davor Politov	Ministry of education and science	North Macedonia
16	Irena Popovska	State Commission for the Prevention of Corruption	North Macedonia
17	Adrian Eduard Dumitru	Ministry of Justice	Romania
18	Daniel Belingher	National Integrity Agency	Romania
NGOs			
1	Arjan Dyrmishi	Center for the Study of Democracy and Governance	Albania
2	Dragana Kurti	Civic Resistance	Albania
3	Klaudia Koxha	Center for the Study of Democracy and Governance	Albania
4	Rea Cikali	Albanian Center for Quality Journalism	Albania

5	Alen Vejzagic	Public Interest Advocacy Center Foundation	Bosnia and Herzegovina
6	Dzenana Aladuz	Foundation INFOHOUSE	Bosnia and Herzegovina
7	Lejla Bicakcic	Center for Investigative Reporting	Bosnia and Herzegovina
8	Alexenia Dimitrova	Media Development Center	Bulgaria
9	Kristina Tsabala	Center for the Study of Democracy	Bulgaria
10	Ioanna Balaoura	Transparency International Greece	Greece
11	Arrita Rezniqi	Kosovo Law Institute	Kosovo*
12	Ala Revenco	Parinti Solidari	Moldova
13	Galina Bostan	Center for the Analysis and Prevention of Corruption	Moldova
14	Zorana Markovic	Centre for Development of NGOs	Montenegro
15	Goran Lefkov	Centre for Investigative Journalism SCOOP	North Macedonia
16	Marija Sunchevska	Transparency International – Macedonia	North Macedonia
17	Maria-Alexandra Cezar	Expert Forum	Romania
18	Simona Ernu	Romanian Academic Society	Romania
19	Aleksandra Milicevic	South East Europe Media Organisation	Serbia
20	Vladimir Radomirovic	Pistaljka	Serbia
21	Dragana Matovic	Pistaljka	Serbia
22	Zuzana Grochalova	Transparency International – Slovakia	Slovakia
EU Delegation to Bosnia and Herzegovina			
1	Enrico Visentin	EUD/EUSR	
2	Mirna Bresan	EUD/EUSR	
3	Nicolas Bizel	EUD/EUSR	
Speakers, Presenters and Moderators			
1	Desislava Gotskova	RAI Secretariat	

2	Elmerina Ahmetaj Hrelja	RAI Secretariat	
3	Tom Devine	RAI Secretariat	
4	Mark Worth	RAI Secretariat	
5	Stephani Ayers	T.M. Guyer and Ayers & Friends/GAP	
6	Thad M. Guyer	T.M. Guyer and Ayers & Friends/GAP	
7	Wendy Addison	SpeakOut SpeakUp	
8	Arjan Dyrmishi	SEE Coalition on Whistleblower Protection	
9	Dzenana Aladjuz	Foundation INFOHOUSE	
10	Vladimir Radomirovic	Pistaljka	

7. Four-day event summary as provided on RAI Website

1. https://rai-see.org/peer-to-peer-regional-meeting-of-public-institutions-for-better-whistleblower-protection-held-in-sarajevo/

Peer-to-Peer Regional Meeting of Public Institutions for better whistleblower protection held in Sarajevo

(http://rai-see.org/php_sets/uploads/2021/11/1637080527900-scaled.jpg)The Peer-to-Peer Regional Meeting of Public Institutions hosted by the Regional Anti-Corruption Initiative Secretariat was held in Sarajevo on November 16, 2021. The meeting aimed at equipping professional staff who participate in whistleblower protection policy making, oversight and enforcement with legislative solutions relevant to achieving improved whistleblower protection by addressing shortcomings identified through the Gap Analysis (https://rai-see.org/the-gap-analysis-of-whistleblower-protection-laws-in-the-western-balkans-and-moldova-finalized-and-delivered-to-beneficiaries/) of Whistleblower Protection Laws in the Western Balkans and Moldova published by RAI Secretariat earlier this year. For that purpose, a paper 'Model Provisions for Whistleblower Protection Laws' (http://rai-see.org/php_sets/uploads/2021/11/Model-Provisions-for-WBer-Protection-Laws_FINAL.pdf) was produced, presented and discussed at the meeting. Additionally, the peer-to-peer meeting provided participants with practical knowledge about transparency requirements and solutions relevant to assessing the impact of whistleblower protection laws – all in line with the EU Whistleblower Protection Directive. (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1937)

(http://rai-see.org/php_sets/uploads/2021/11/1637080527897-scaled.jpg)The regional meeting of public institutions enabled the peer-to-peer exchange of experiences and lessons learned for purposes of identifying best practice solutions and translating them into action leading to better whistleblower protection.

The Peer-to-Peer Regional Meeting of Public Institutions was facilitated as part of the four-day regional meeting on whistleblower protection, organized under the auspices of the regional project 'Breaking the Silence: Enhancing the whistleblowing policies and culture in Western Balkans and Moldova (https://rai-see.org/what-we-do/breaking-the-silence/)', which is funded by the European Union and implemented by the RAI Secretariat. This event gathered representatives of public institutions, anti-corruption agencies, ministries of justice and ombudsman institutions from the SEE jurisdictions including Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Moldova, Montenegro, North Macedonia, and Romania.

2. https://rai-see.org/rai-secretariat-delivers-the-second-annual-regional-multi-beneficiary-training-on-whistleblower-protection/

RAI Secretariat delivers the Second Annual Regional Multi-Beneficiary Training on Whistleblower Protection

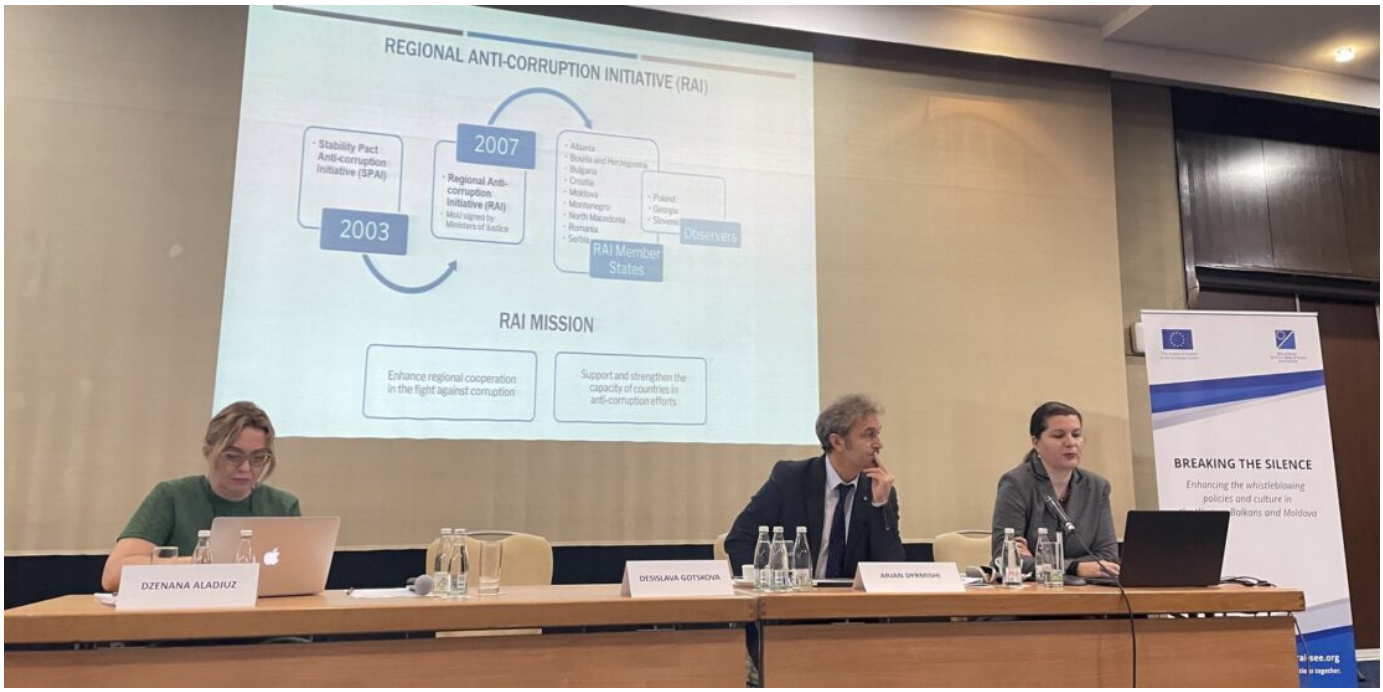
What is required to build an organizational culture in which whistleblowers feel safe to report misconduct? How to inform and educate employees to address underreporting caused by negative perceptions about whistleblowing and whistleblowers? How to improve whistleblower disclosure channels and protection? How to deter retaliation against the whistleblower? These are some of the questions that were addressed and discussed at the two-day Second Annual Regional Multi-Beneficiary Training on Whistleblower Protection that was held last week in Sarajevo, organized by the RAI Secretariat.

The training was delivered by international whistleblowing experts Tom Devine, Thad Guyer and Mark Worth who provided trainees – public institutions and CSO representatives from Western Balkans and Moldova – with practical knowledge and tools relevant to enabling effective whistleblower disclosures and protection.

The multi-beneficiary training was facilitated on November 17-18, 2021, as part of the four-day regional meeting on whistleblower protection, organized under the auspices of the regional project 'Breaking the Silence: Enhancing the whistleblowing policies and culture in Western Balkans and Moldova' (https://rai-see.org/what-we-do/breaking-the-silence/), which is funded by the European Union and implemented by the RAI Secretariat.

3. https://rai-see.org/southeast-europe-coalition-on-whistleblower-protection-annual-meeting-held-in-sarajevo/

Southeast Europe Coalition on Whistleblower Protection Annual Meeting held in Sarajevo



The Annual Meeting of the Southeast Europe Coalition on Whistleblower Protection (https://see-whistleblowing.org/) co-hosted by the Foundation INFOHOUSE, was held in Sarajevo on Friday, November 22, 2021 with the support of RAI Secretariat.

The Coalition's Annual Meeting serves as a platform for discussion of common challenges, strategies, and solutions for improving the protection of whistleblowers. RAI Secretariat has been supportive of the work of the Coalition since its establishment in 2015, in recognition of the importance of collaboration between the government and the non-governmental sector in effectively protecting whistleblowers. The annual meeting of the Coalition was also an opportunity to celebrate success and capture lessons learned.

The participants and Coalition members were presented a valuable insight on the experience and lessons learned of the
Government Accountability Project (GAP), USA, delivered by expert Tom Devine, on how can NGOs help whistleblowers. Additionally, Vladimir Radimirovic, representative of the CSO "Pistaljka" from Serbia presented the experience and engagement of this organization in their mission of whistleblower protection.

The Coalition Annual Meeting was organized under the auspices of the regional project 'Breaking the Silence: Enhancing the whistleblowing policies and culture in Western Balkans and Moldova' (https://rai-see.org/what-we-do/breaking-the-silence/), which is funded by the European Union and implemented by the RAI Secretariat. The Annual Meeting gathered representatives of civil society organizations from Albania, Bosnia and Herzegovina, Bulgaria, Kosovo*, Moldova, Montenegro, North Macedonia, Romania, Serbia, and Slovakia.

** This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration on Independence*

This publication was produced with financial support of the European Union. Its contents are the sole responsibility of its authors and do not necessarily reflect the views of the European Union. Views presented in this publication do not necessarily reflect the official position of the Regional Anti-Corruption Initiative or its member states.