Tishk International University
Faculty of Applied Science
Cybersecurity Department

Lecture 7 : Hacking, Whistleblowing, and Digital Activism

CBS221/A : Ethics and Legal Issues in Cybersecurity

Week 8 : 23-27/11/2025

Instructor: Prof. Dr. Qaysar Salih Mahdi

Introduction

- - Explore ethical dilemmas in hacking, whistleblowing, and digital activism.
- - Ethical Theories:
- Utilitarianism,
- Deontology,
- Virtue Ethics
- - Legal: CFAA, Whistleblower Protection Act
- - IEEE Code of Ethics

What is Ethical Hacking?

Ethical Hacking

The Certified Ethical Hacker (CEH) credentialing and provided by EC-Council is a respected and trusted ethical hacking course in the industry. Since the inception of Certified Ethical Hacker in 2003, the credential has become one of the best options for industries and companies across the world. The CEH exam is ANSI 17024 compliant, adding value and credibility to credential members. It is also listed as a baseline certification in the US Department of Defense (DoD) Directive 8570 and is a NSCS Certified Training.

Today, you can find Certified Ethical Hackers working with some of the finest and largest companies across industries like healthcare, financial, government, energy, and much more!

What Does an Ethical Hacker Do?

An ethical hacker is a cybersecurity professional trained to identify and fix vulnerabilities in systems before malicious hackers can exploit them. They simulate real-world cyberattacks to assess risk and strengthen security posture.

- **Ethical Hackers help organizations answer critical cybersecurity questions:**
- **What vulnerabilities could an attacker exploit?**
- **What systems or data are most at risk?**
- **What damage could an attacker cause with the compromised information?**
- **How many security layers detect or log the intrusion?**

Ethical hackers learn and perform hacking in a professional manner, based on the direction of the client, and later, present a maturity scorecard highlighting their overall risk and vulnerabilities and suggestions to improve.

- **What are the best ways to mitigate these vulnerabilities?**

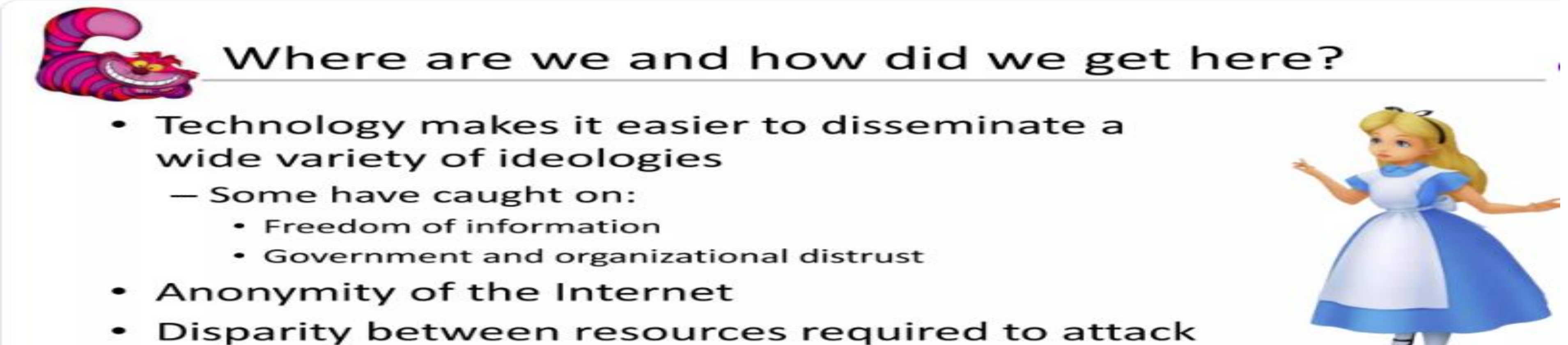
They operate under strict authorization, document their findings, and deliver a comprehensive risk and vulnerability scorecard along with actionable recommendations.

Exercise: Identify ethical issues in the Equifax breach.

Solution: Internal disclosure aligns with utilitarian ethics; external disclosure aligns with deontology but may violate law.

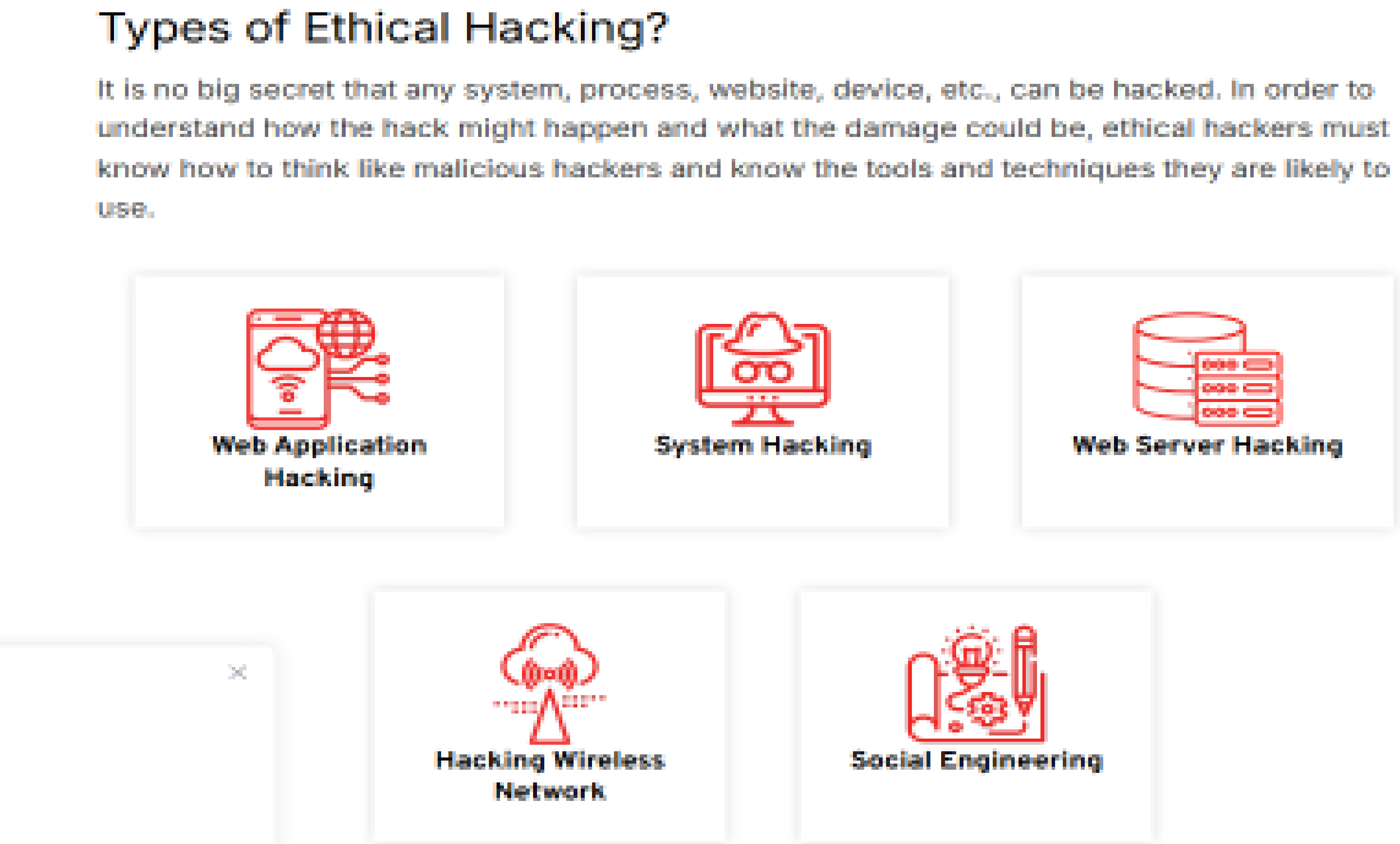
Hacktivism

Motivations, Tactics, and Threats



Where are we and how did we get here?

- Technology makes it easier to disseminate a wide variety of ideologies
  - Some have caught on:
    - Freedom of information
    - Government and organizational distrust
- Anonymity of the Internet
- Disparity between resources required to attack



Types of Ethical Hacking?

It is no big secret that any system, process, website, device, etc., can be hacked. In order to understand how the hack might happen and what the damage could be, ethical hackers must know how to think like malicious hackers and know the tools and techniques they are likely to use.

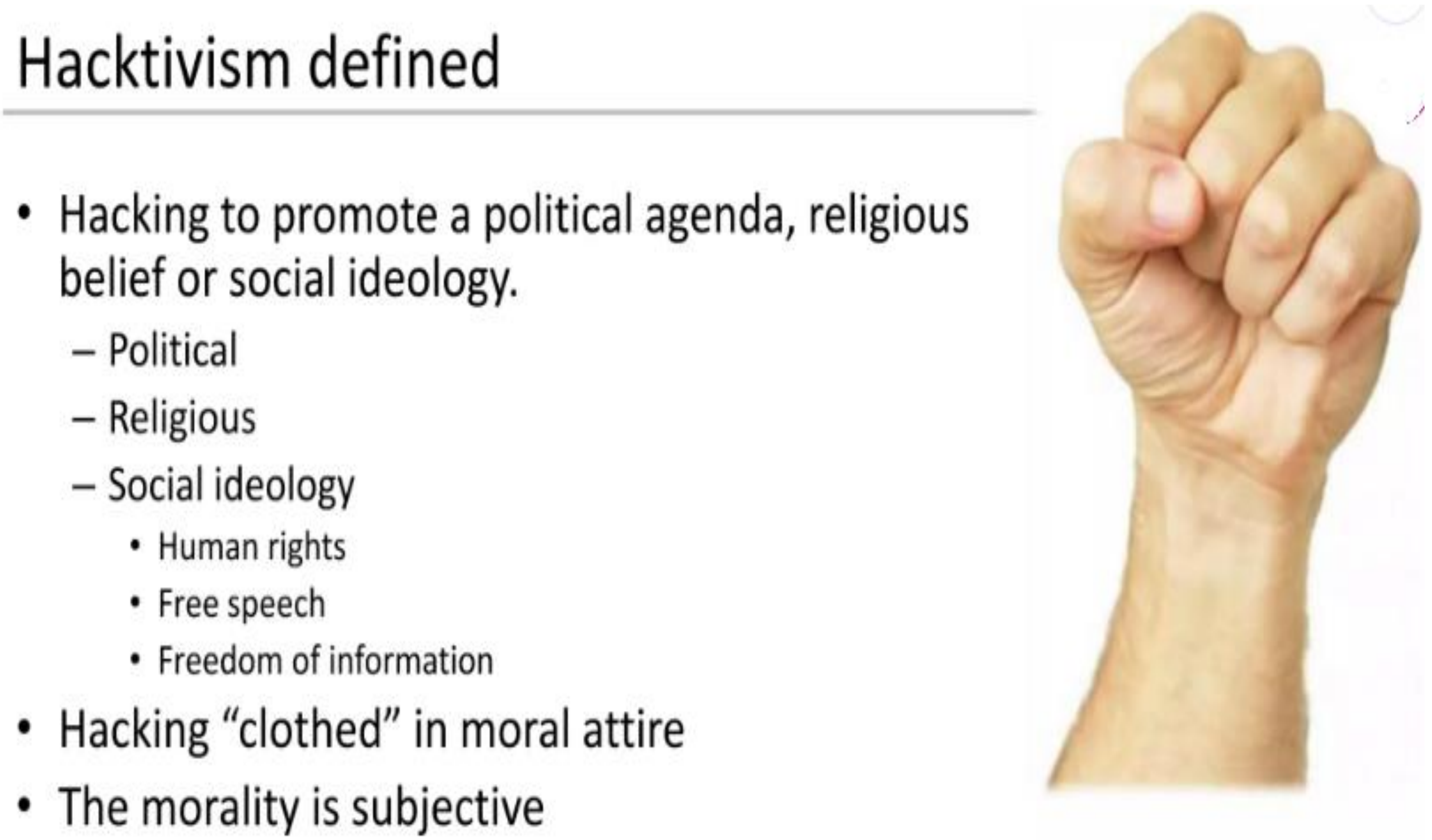
Web Application Hacking

System Hacking

Web Server Hacking

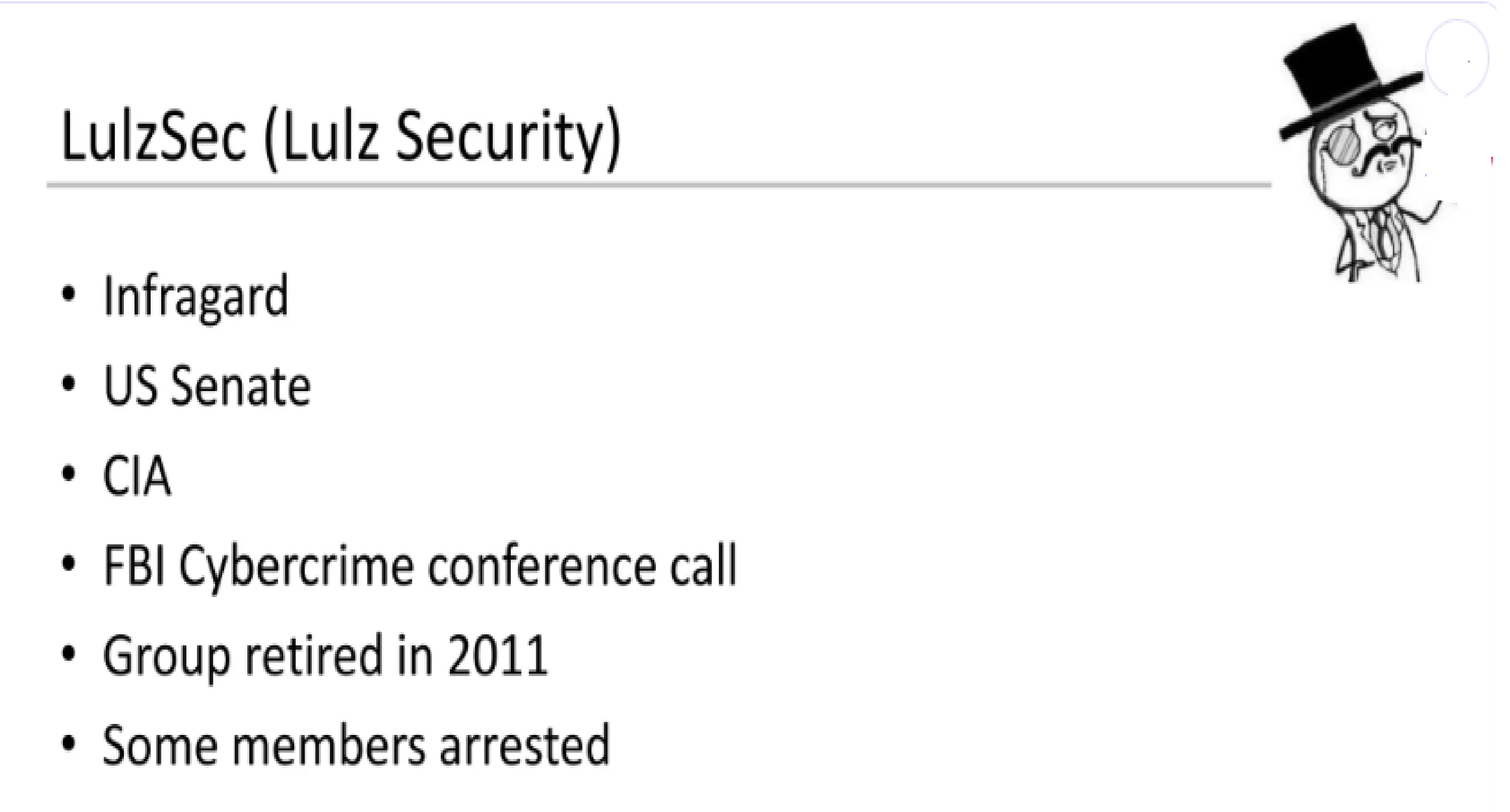
Hacking Wireless Network

Social Engineering



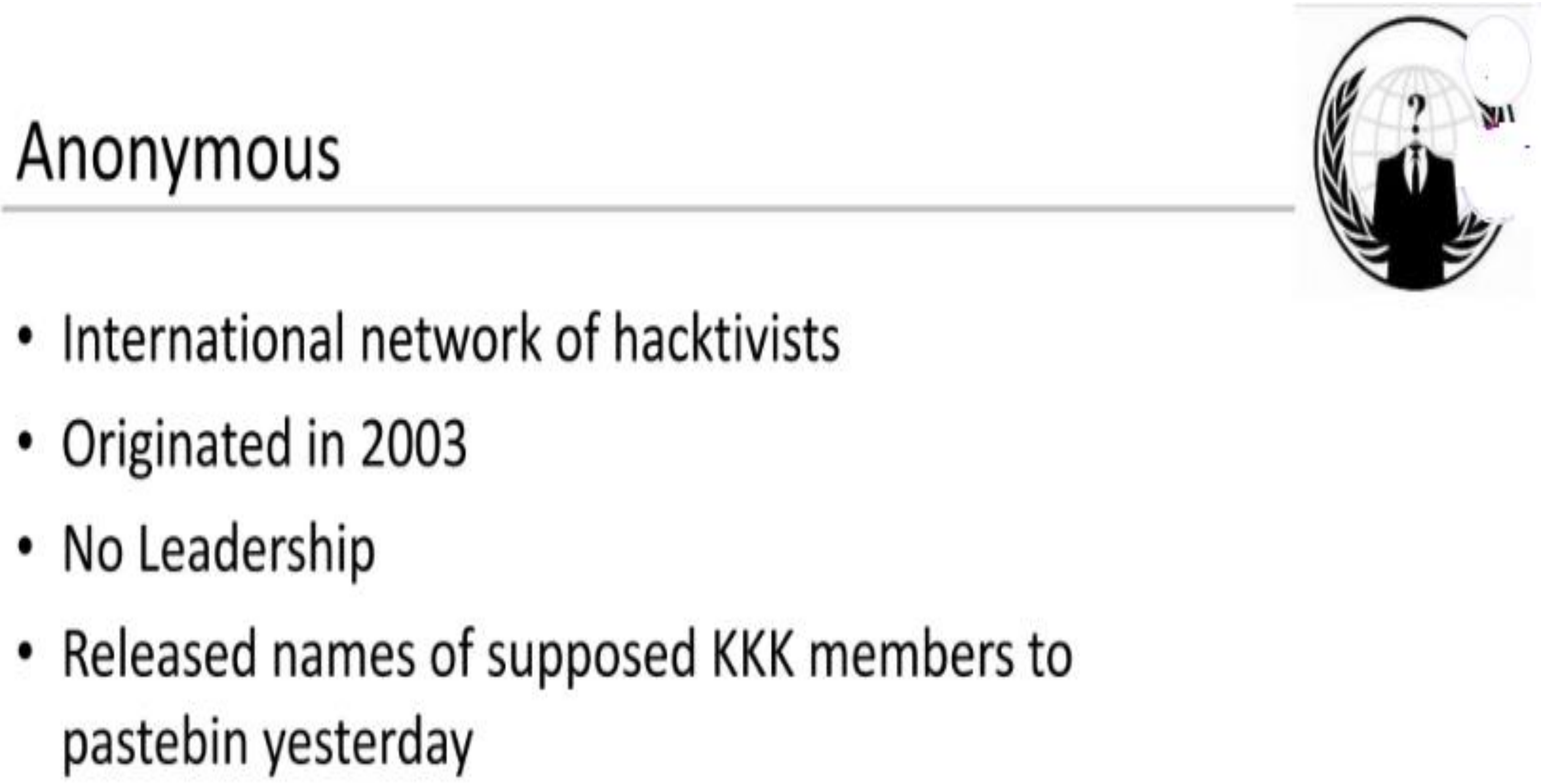
Hacktivism defined

- Hacking to promote a political agenda, religious belief or social ideology.
  - Political
  - Religious
  - Social ideology
    - Human rights
    - Free speech
    - Freedom of information
- Hacking “clothed” in moral attire
- The morality is subjective



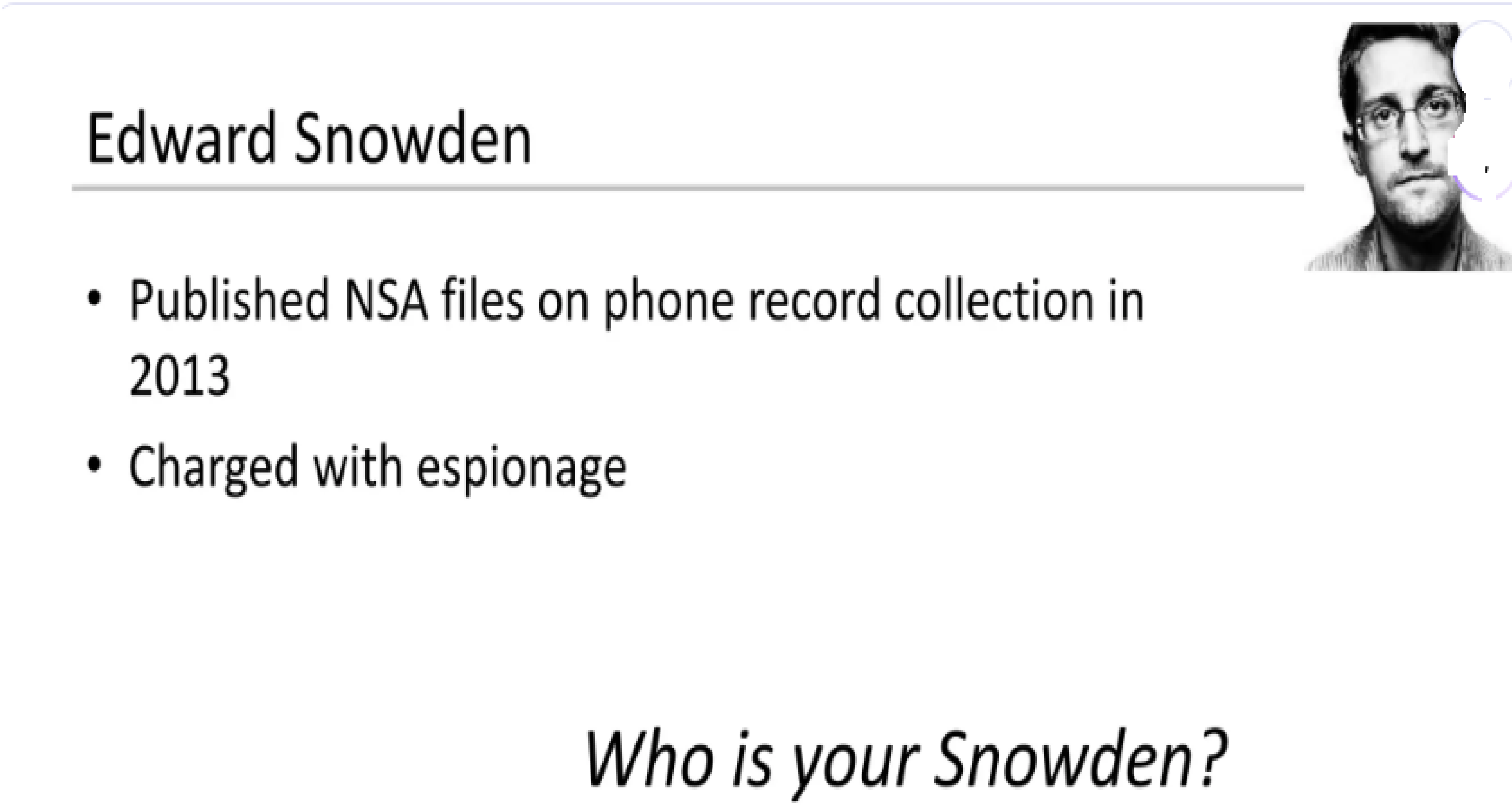
LulzSec (Lulz Security)

- Infragard
- US Senate
- CIA
- FBI Cybercrime conference call
- Group retired in 2011
- Some members arrested



Anonymous

- International network of hacktivists
- Originated in 2003
- No Leadership
- Released names of supposed KKK members to pastebin yesterday



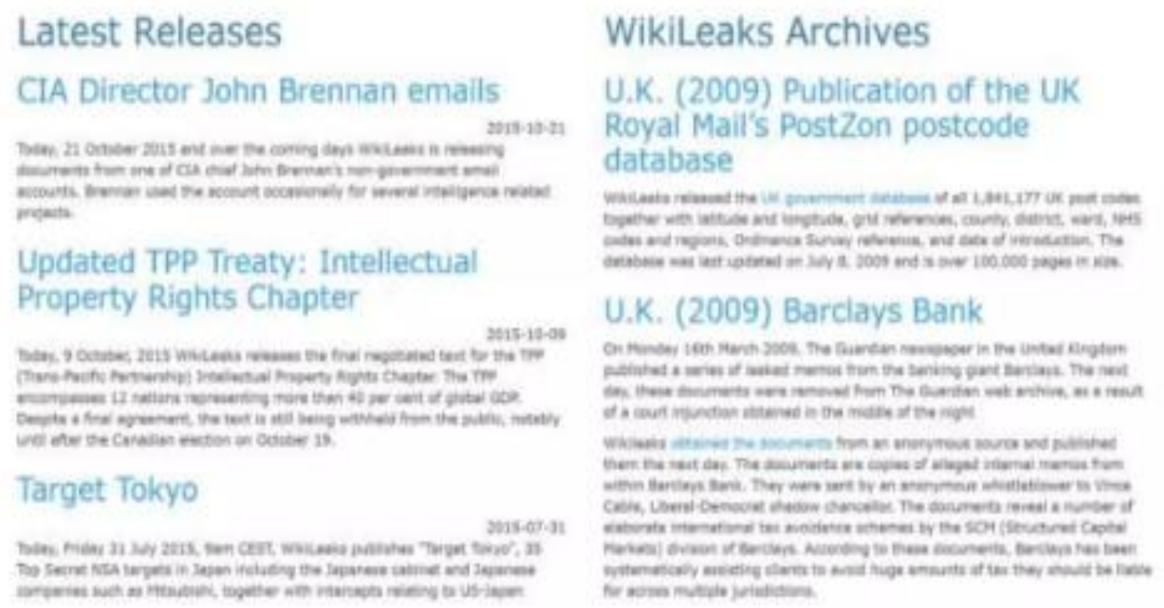
Edward Snowden

- Published NSA files on phone record collection in 2013
- Charged with espionage

Who is your Snowden?

Wikileaks

- Site that publishes secret information, classified files, and news leaks from anonymous sources



Latest Releases

CIA Director John Brennan emails

2015-10-21

Today, 21 October 2015 and over the coming days WikiLeaks is releasing documents from one of CIA chief John Brennan's non-government email accounts. Brennan used the account occasionally for several intelligence related projects.

Updated TPP Treaty: Intellectual Property Rights Chapter

2015-10-09

Today, 9 October, 2015 WikiLeaks releases the final negotiated text for the TPP (Trans-Pacific Partnership) Intellectual Property Rights Chapter. The TPP encompasses 12 nations representing more than 40 per cent of global GDP. Despite a final agreement, the text is still being withheld from the public, notably until after the Canadian election on October 19.

Target Tokyo

2015-07-31

Today, Friday 31 July 2015, 9am CEST, WikiLeaks publishes "Target Tokyo", 35 Top Secret NSA targets in Japan including the Japanese cabinet and Japanese companies such as Mitsubishi, together with intercepts relating to US-Japan

WikiLeaks Archives

U.K. (2009) Publication of the UK Royal Mail's PostZon postcode database

WikiLeaks released the UK government database of all 1,841,177 UK post codes together with latitude and longitude, grid references, county, district, ward, NHS codes and regions, Ordnance Survey reference, and date of introduction. The database was last updated on July 8, 2009 and is over 100,000 pages in size.

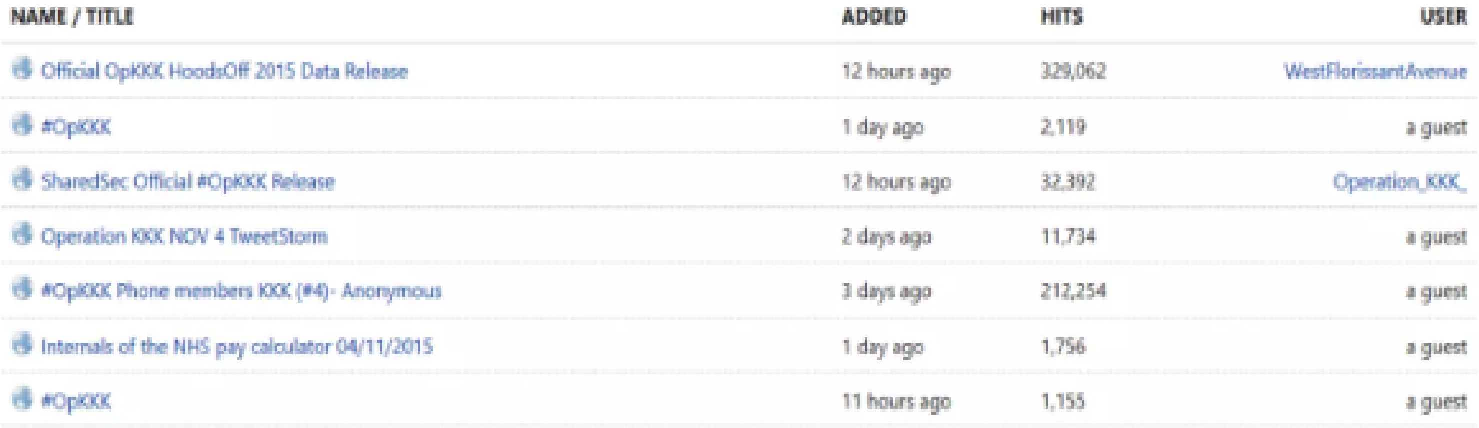
U.K. (2009) Barclays Bank

On Monday 16th March 2009, The Guardian newspaper in the United Kingdom published a series of leaked memos from the banking giant Barclays. The next day, these documents were removed from The Guardian web archive, as a result of a court injunction obtained in the middle of the night.

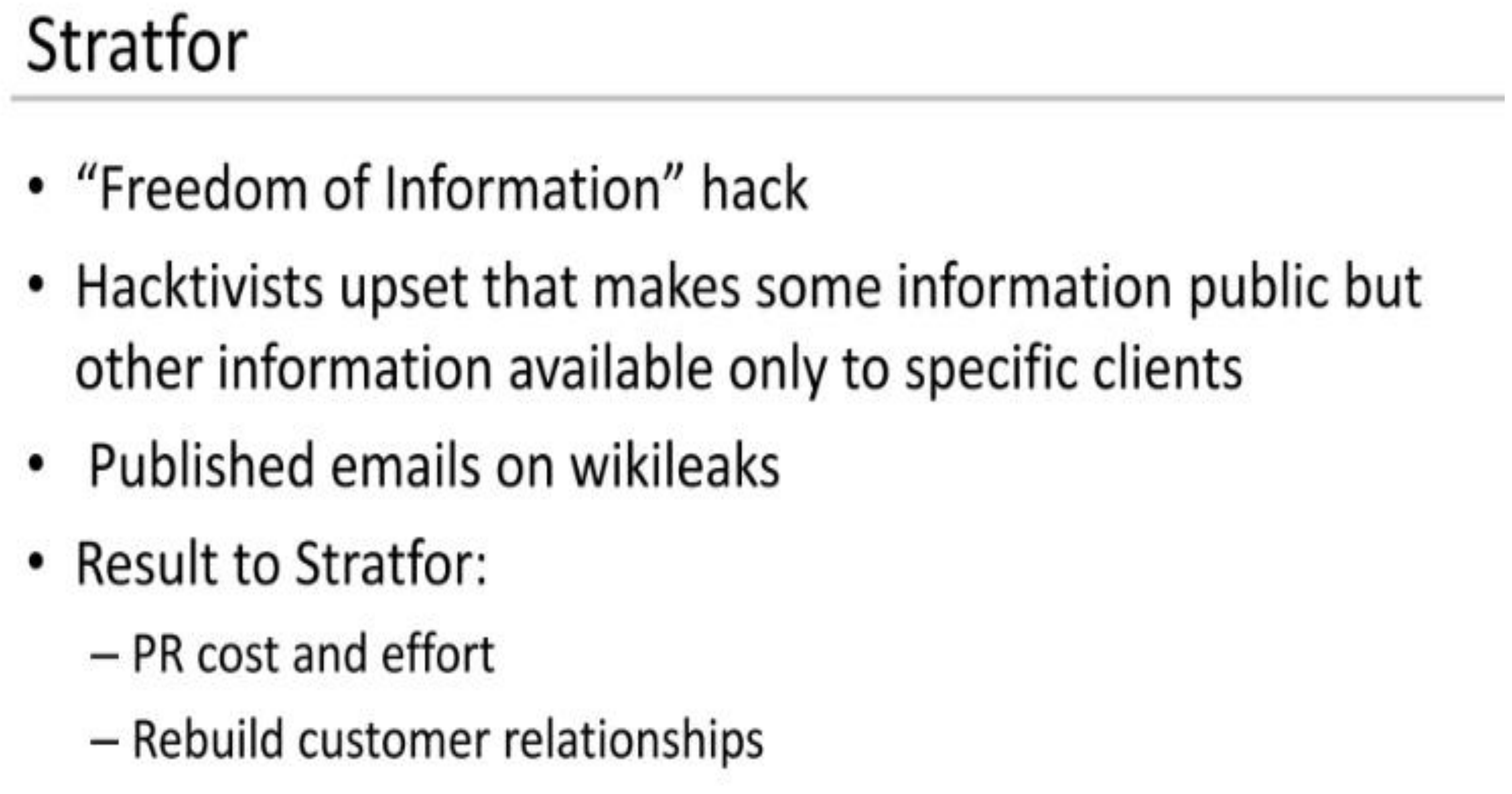
Wikileaks obtained the documents from an anonymous source and published them the next day. The documents are copies of alleged internal memos from within Barclays Bank. They were sent by an anonymous whistleblower to Vince Cable, Liberal-Democrat shadow chancellor. The documents reveal a number of elaborate international tax avoidance schemes by the SCM (Structured Capital Markets) division of Barclays. According to these documents, Barclays has been systematically assisting clients to avoid huge amounts of tax they should be liable for across multiple jurisdictions.

Pastebin

- Public data repository
- Anonymous posting allowed
- Commonly find hacker loot and malicious code or copyright infringement source code



NAME / TITLE	ADDED	HITS	USER
Official OpKKK HoodsOff 2015 Data Release	12 hours ago	329,062	WestFlorissantAvenue
#OpKKK	1 day ago	2,119	a guest
SharedSec Official #OpKKK Release	12 hours ago	32,392	Operation_KKK_
Operation KKK NOV 4 TweetStorm	2 days ago	11,734	a guest
#OpKKK Phone members KKK (#4)- Anonymous	3 days ago	212,254	a guest
Internals of the NHS pay calculator 04/11/2015	1 day ago	1,756	a guest
#OpKKK	11 hours ago	1,155	a guest

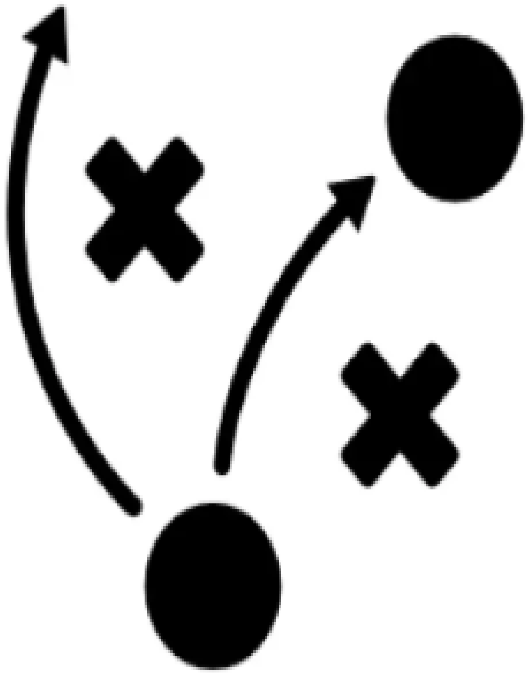


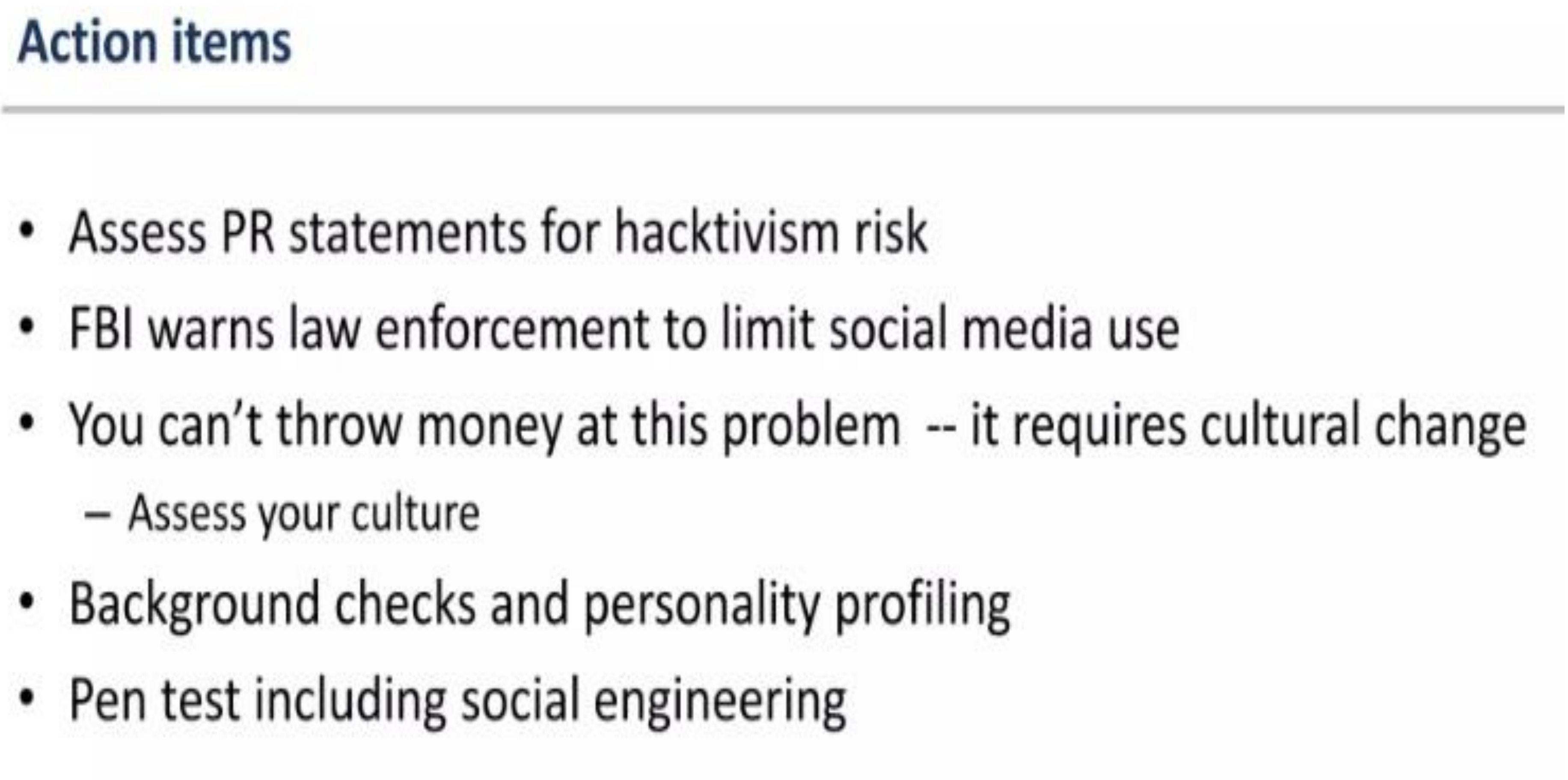
Stratfor

- “Freedom of Information” hack
- Hacktivists upset that makes some information public but other information available only to specific clients
- Published emails on wikileaks
- Result to Stratfor:
  - – PR cost and effort
  - – Rebuild customer relationships

Tactics

- DDoS
- Most common hacking methods
- Negative SEO
  - Google bombing – associate negative keywords with your name
  - Utilize penalized SEO tactics on your sites / social media
- Email flooding
- Fax spam
- Phishing, Spam and SPIM





Action items

- Assess PR statements for hacktivism risk
- FBI warns law enforcement to limit social media use
- You can't throw money at this problem -- it requires cultural change
  - Assess your culture
- Background checks and personality profiling
- Pen test including social engineering

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Ethical Dilemmas in Hacking

Introduction

- Ethical dilemmas in hacking are situations where a hacker must choose between two or more options, each of which presents a conflict with a professional or ethical principle. These situations often arise when balancing the need to find vulnerabilities (for the client's security) with the potential for causing damage or violating privacy and legal boundaries. Common dilemmas include deciding how much sensitive information is necessary to expose, managing the risk of unintentionally disrupting systems, and handling findings that fall outside the scope.
- Ethical dilemmas in hacking often involve the balance between privacy and security, such as when an organization must monitor user activity to

Gray Hat Hackers: Walking the Line Between Ethical and Unethical Hacking

Theoretical Principles:

- White-hat: ethical, authorized
- Black-hat: malicious, unauthorized
- Grey-hat: ambiguous

Practical Examples:

- White-hat: Bugcrowd testing
- Black-hat: Sony Pictures 2014 hack
- Grey-hat: Disclosed vulnerability

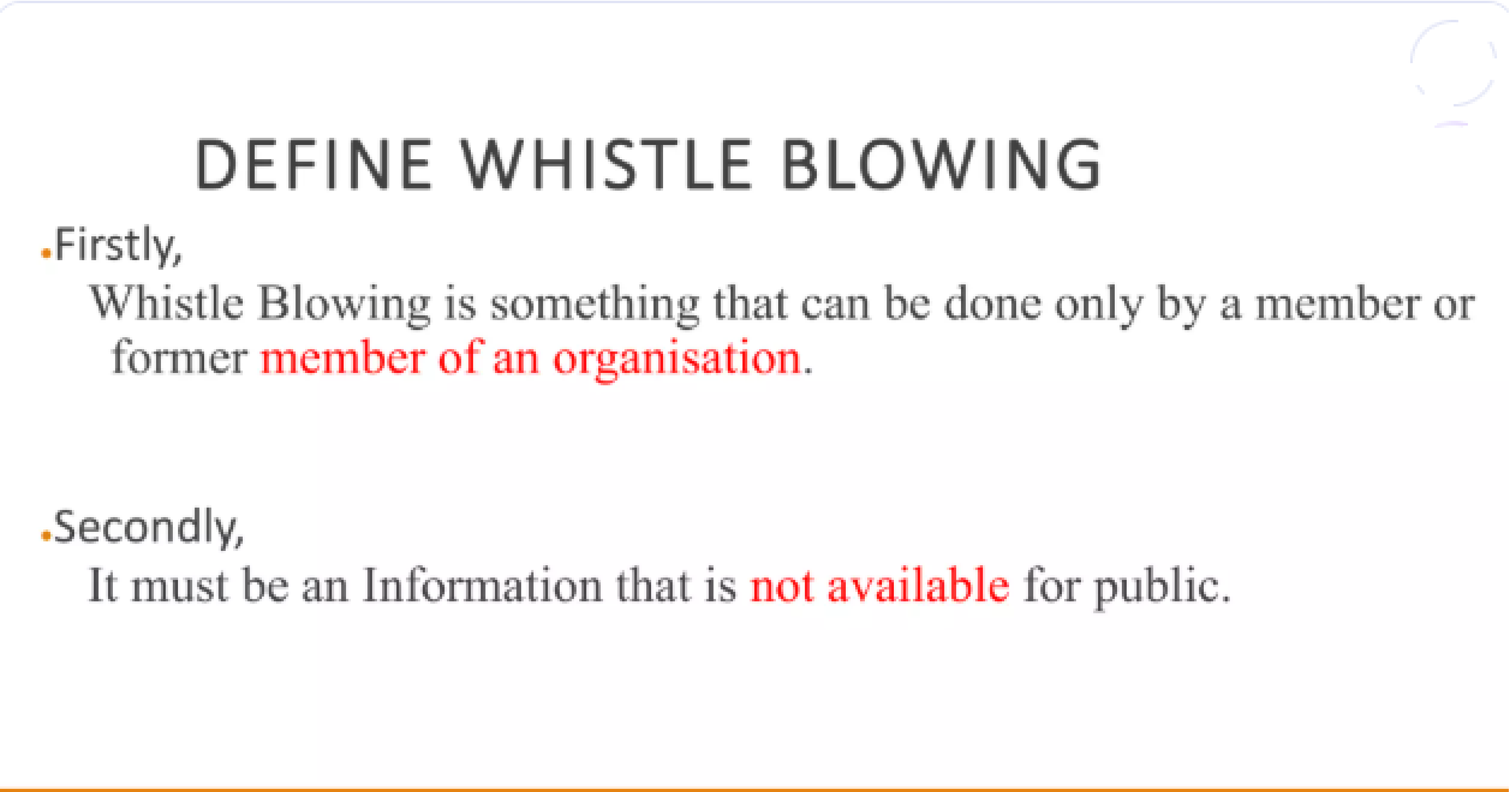
Exercise: Classify hackers in the above examples

Solution: White-hat → Ethical; Black-hat → Illegal/unethical; Grey-hat → Ambiguous

Mathematical Problem: $\text{ERS\_H} = \text{Impact}*\text{Likelihood} / \text{Mitigation} = 8*0.5/2 = 2$

Whistleblowing Concepts

- Introduction:
- Define Whistleblowing
- - Reporting internal wrongdoing; ethical/legal considerations
- Theoretical Principles:
- - Duty to prevent harm
- - Legal protection: Whistleblower Protection Act
- Practical Examples: Edward Snowden, Chelsea Manning, Reality Winner



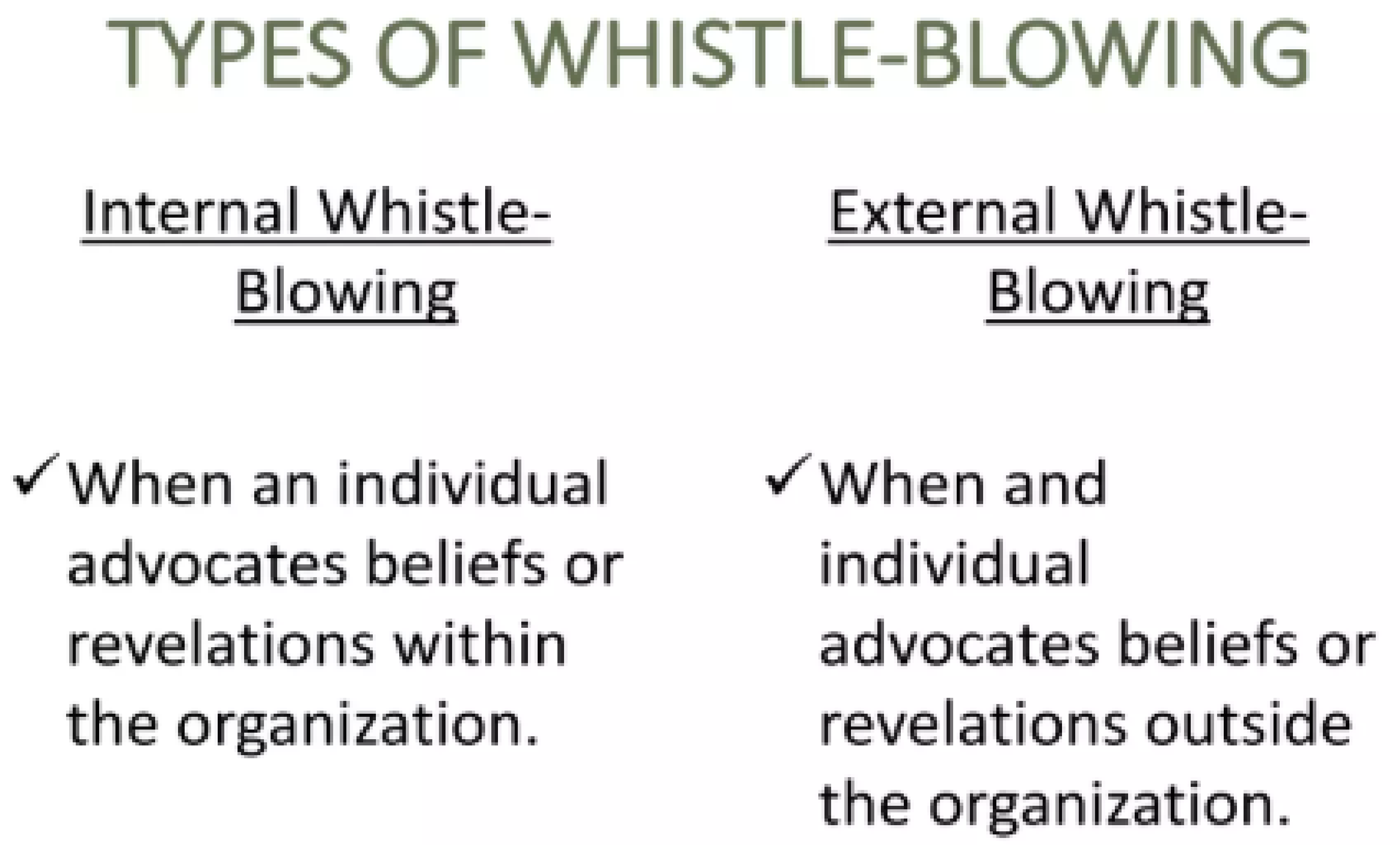
DEFINE WHISTLE BLOWING

- Firstly,

  Whistle Blowing is something that can be done only by a member or former member of an organisation.

- Secondly,

  It must be an Information that is not available for public.



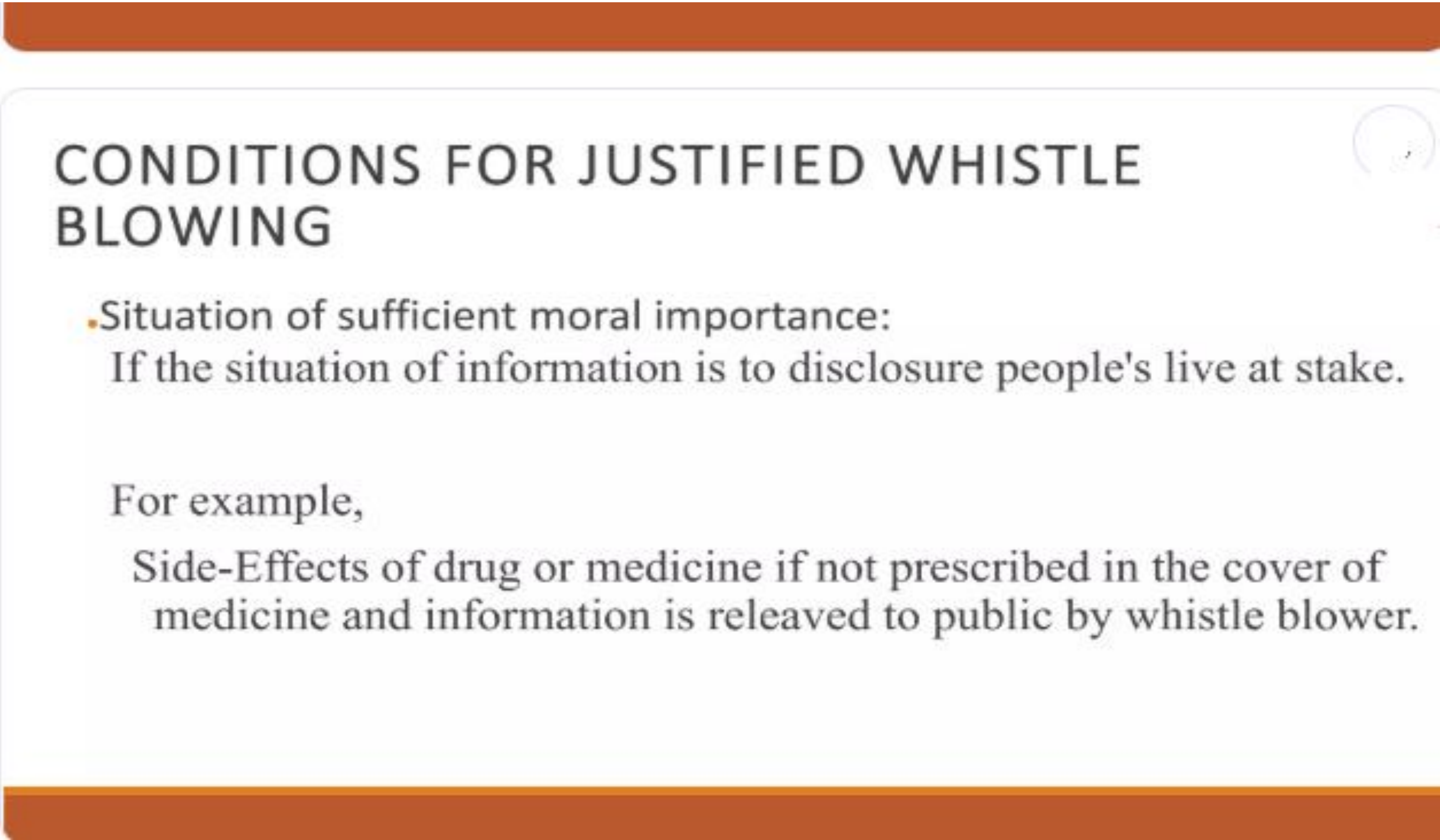
TYPES OF WHISTLE-BLOWING

Internal Whistle-Blowing

- ✓ When an individual advocates beliefs or revelations within the organization.

External Whistle-Blowing

- ✓ When and individual advocates beliefs or revelations outside the organization.



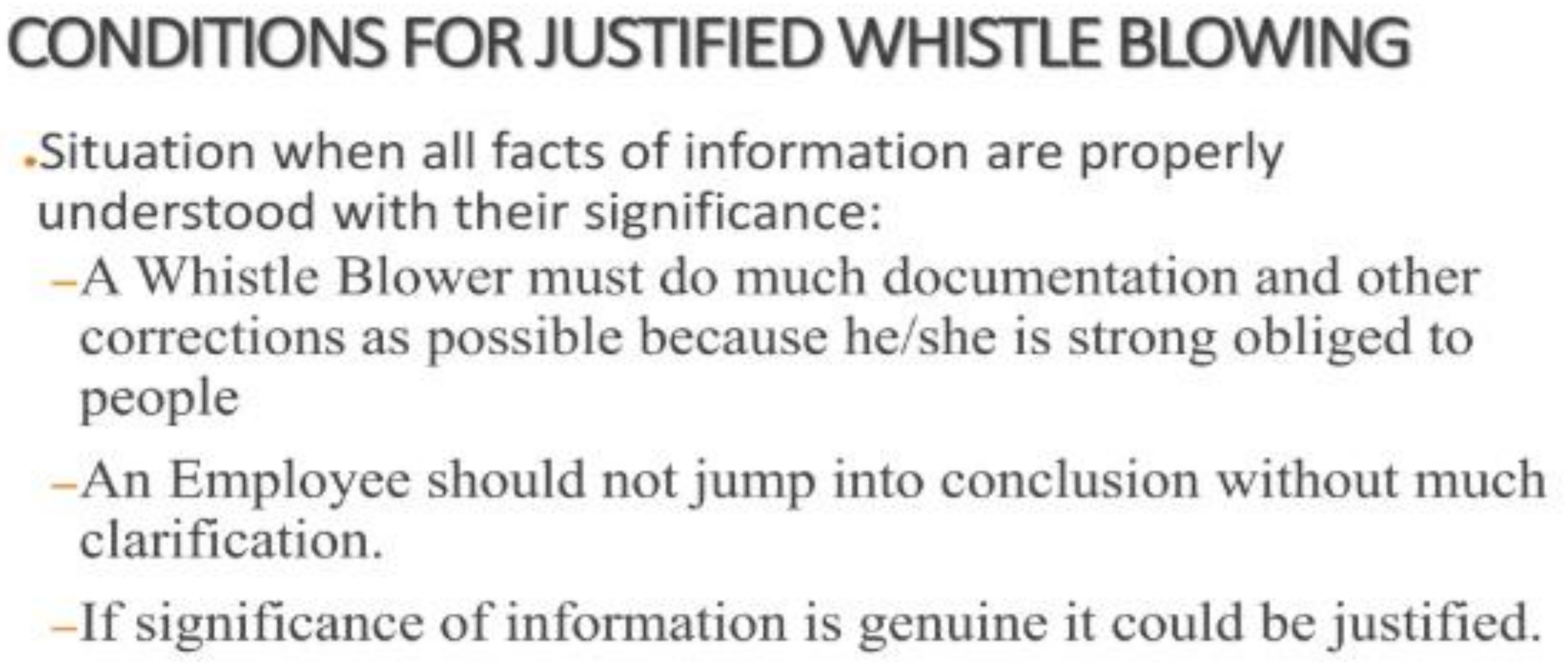
CONDITIONS FOR JUSTIFIED WHISTLE BLOWING

- Situation of sufficient moral importance:

  If the situation of information is to disclosure people's live at stake.

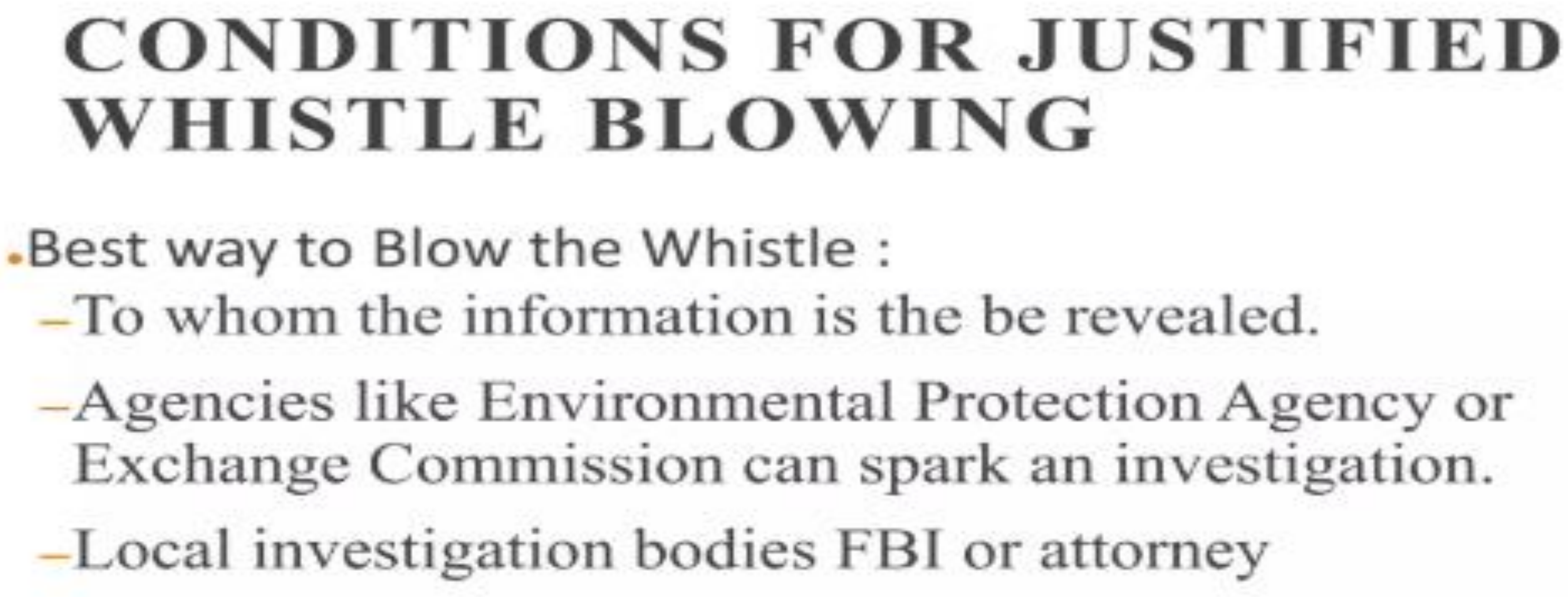
  For example,

  Side-Effects of drug or medicine if not prescribed in the cover of medicine and information is releaved to public by whistle blower.



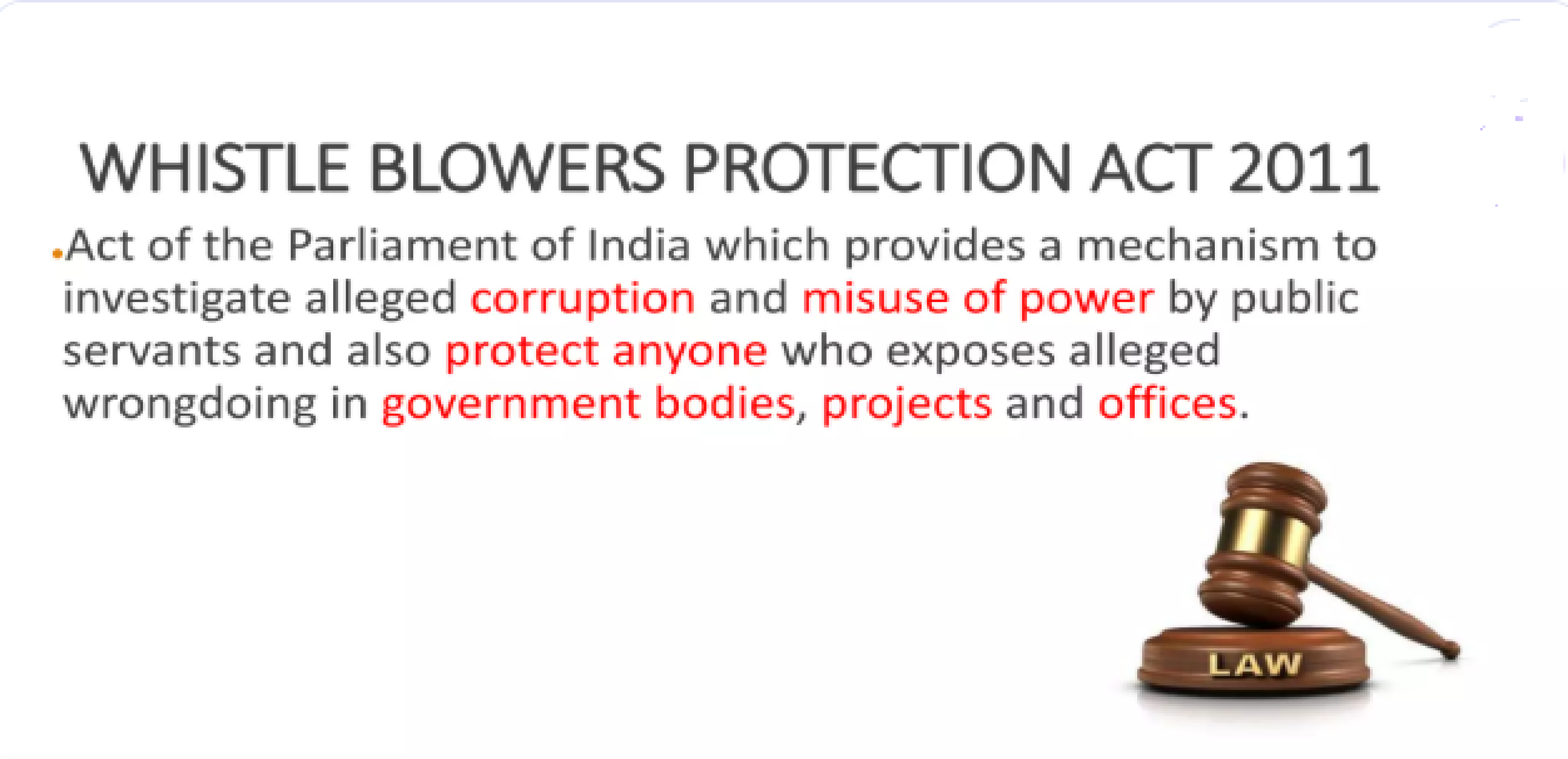
CONDITIONS FOR JUSTIFIED WHISTLE BLOWING

- Situation when all facts of information are properly understood with their significance:
  - A Whistle Blower must do much documentation and other corrections as possible because he/she is strong obliged to people
  - An Employee should not jump into conclusion without much clarification.
  - If significance of information is genuine it could be justified.



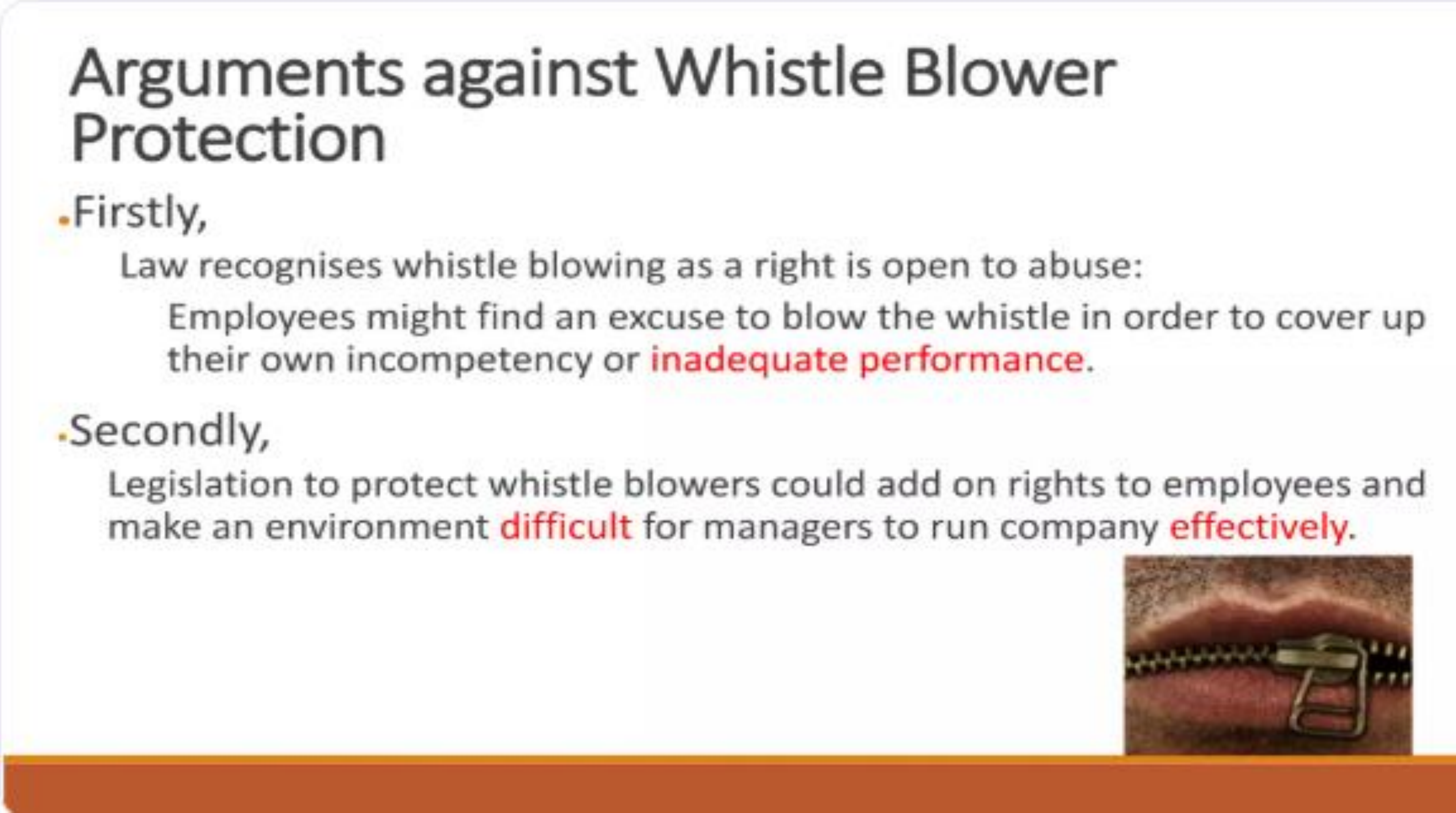
CONDITIONS FOR JUSTIFIED WHISTLE BLOWING

- Best way to Blow the Whistle :
  - To whom the information is the be revealed.
  - Agencies like Environmental Protection Agency or Exchange Commission can spark an investigation.
  - Local investigation bodies FBI or attorney



WHISTLE BLOWERS PROTECTION ACT 2011

- Act of the Parliament of India which provides a mechanism to investigate alleged corruption and misuse of power by public servants and also protect anyone who exposes alleged wrongdoing in government bodies, projects and offices.



Arguments against Whistle Blower Protection

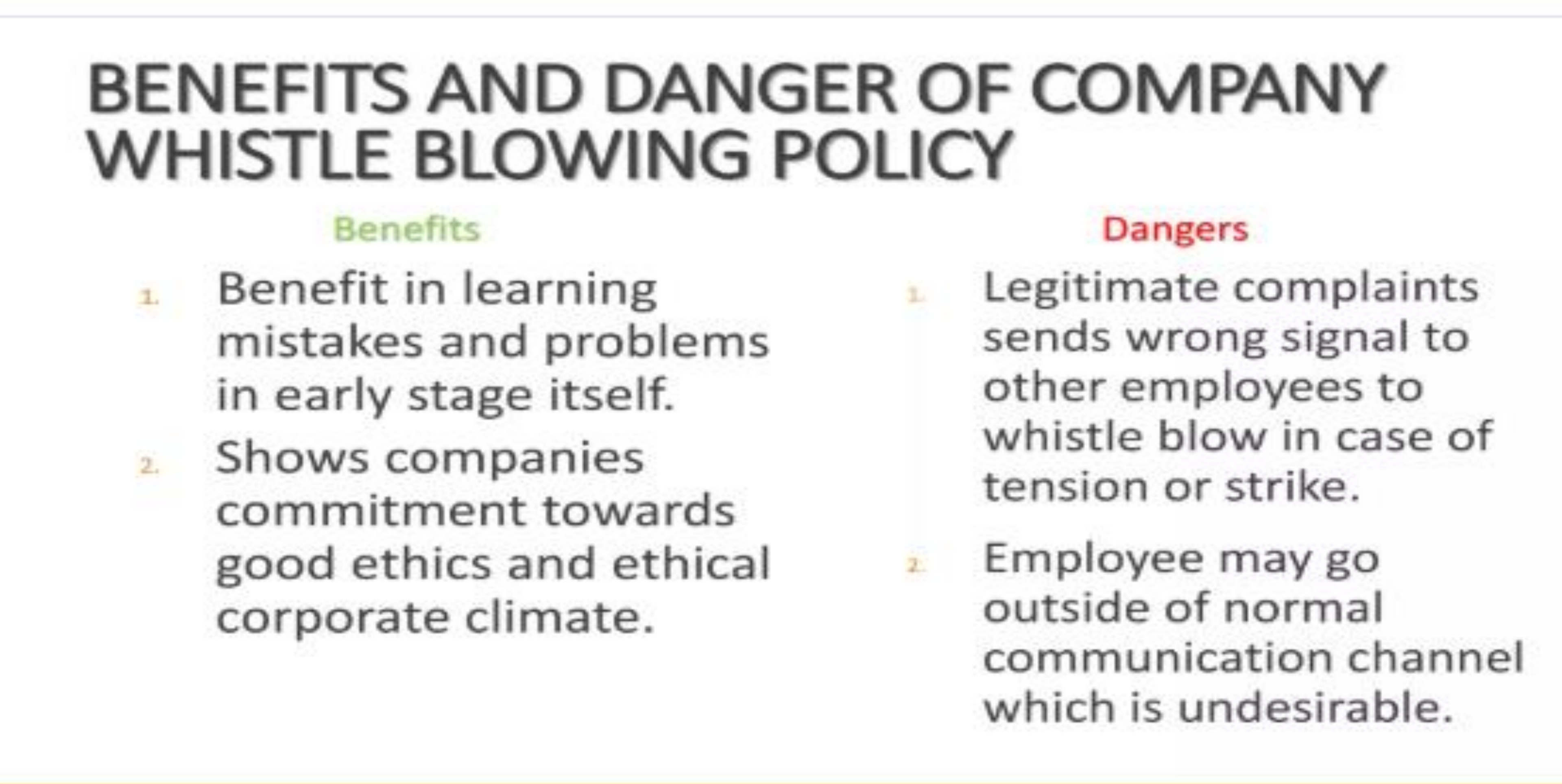
- Firstly,

  Law recognises whistle blowing as a right is open to abuse:

  Employees might find an excuse to blow the whistle in order to cover up their own incompetency or inadequate performance.

- Secondly,

  Legislation to protect whistle blowers could add on rights to employees and make an environment difficult for managers to run company effectively.



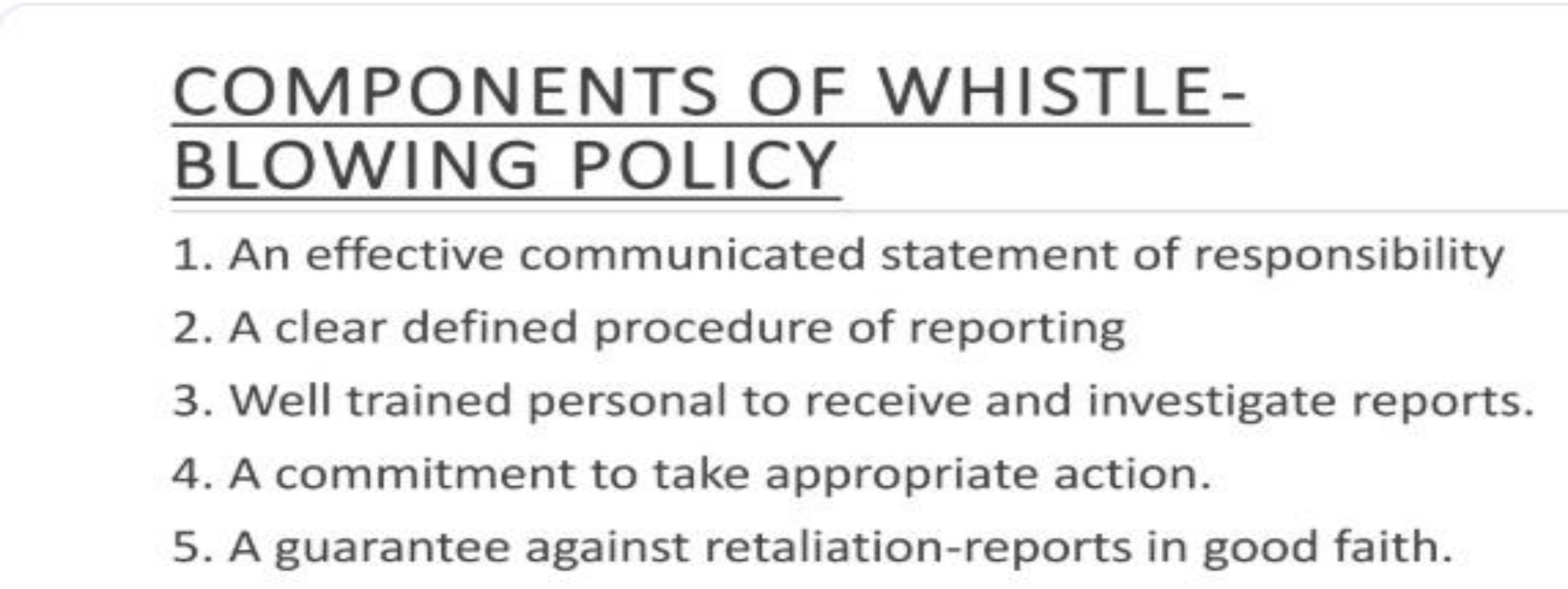
BENEFITS AND DANGER OF COMPANY WHISTLE BLOWING POLICY

Benefits

1. Benefit in learning mistakes and problems in early stage itself.
2. Shows companies commitment towards good ethics and ethical corporate climate.

Dangers

1. Legitimate complaints sends wrong signal to other employees to whistle blow in case of tension or strike.
2. Employee may go outside of normal communication channel which is undesirable.



COMPONENTS OF WHISTLE-BLOWING POLICY

1. An effective communicated statement of responsibility
2. A clear defined procedure of reporting
3. Well trained personal to receive and investigate reports.
4. A commitment to take appropriate action.
5. A guarantee against retaliation-reports in good faith.

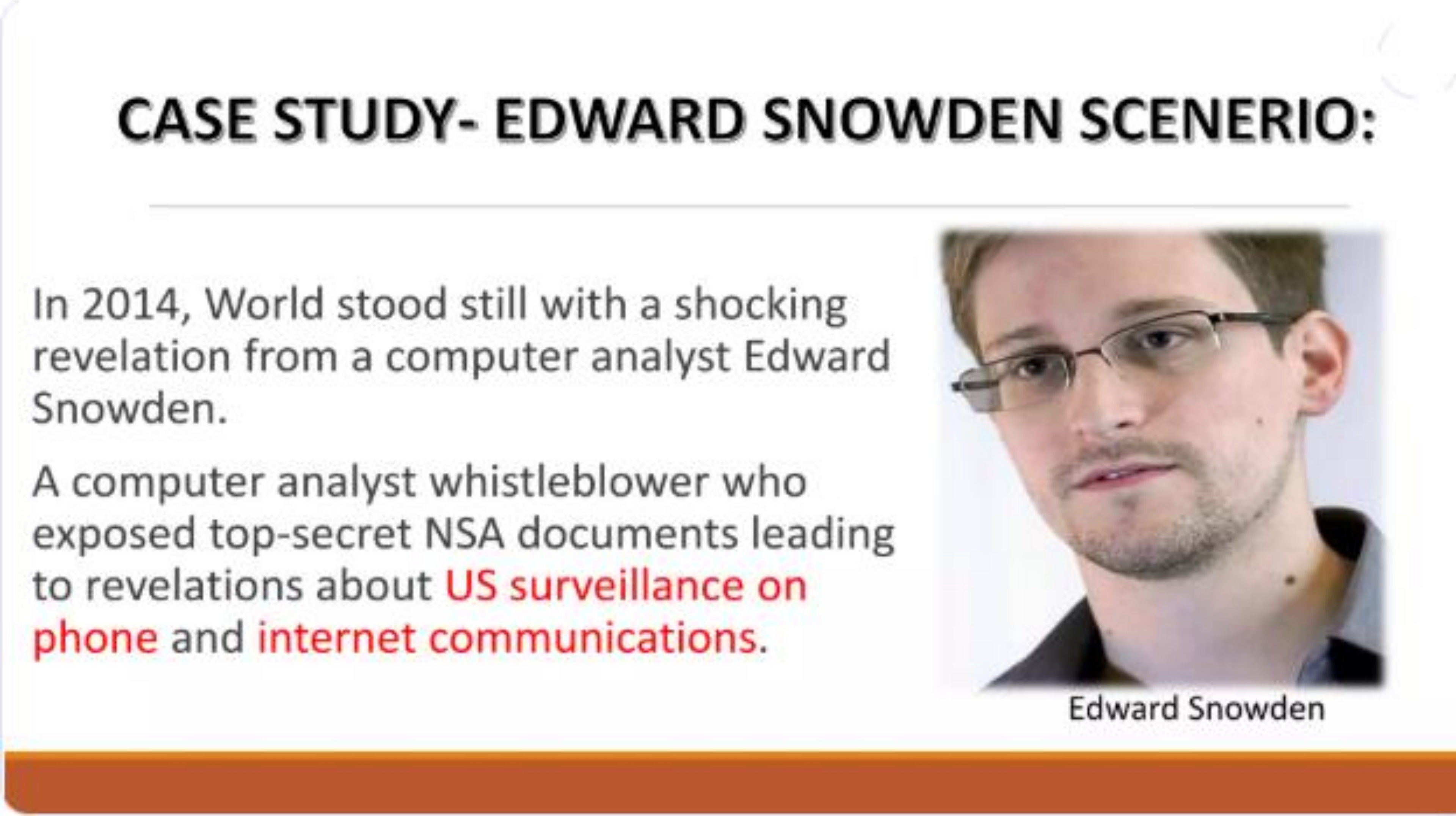
Snowden Case Study

- Introduction:
- - Conflict between ethics and legality in NSA leaks

- Theoretical Principles:
- - Utilitarian: Public interest vs national security harm
- - Deontology: Duty to uphold law vs moral duty

- Exercise: Evaluate ethical and legal aspects
- Solution: Ethical: justified; Legal: violates Espionage Act

- Mathematical Problem: Decision Score = (Benefit-Harm)/(Legal Risk+Ethical Risk) = (10-7)/(9+2) = 0.27

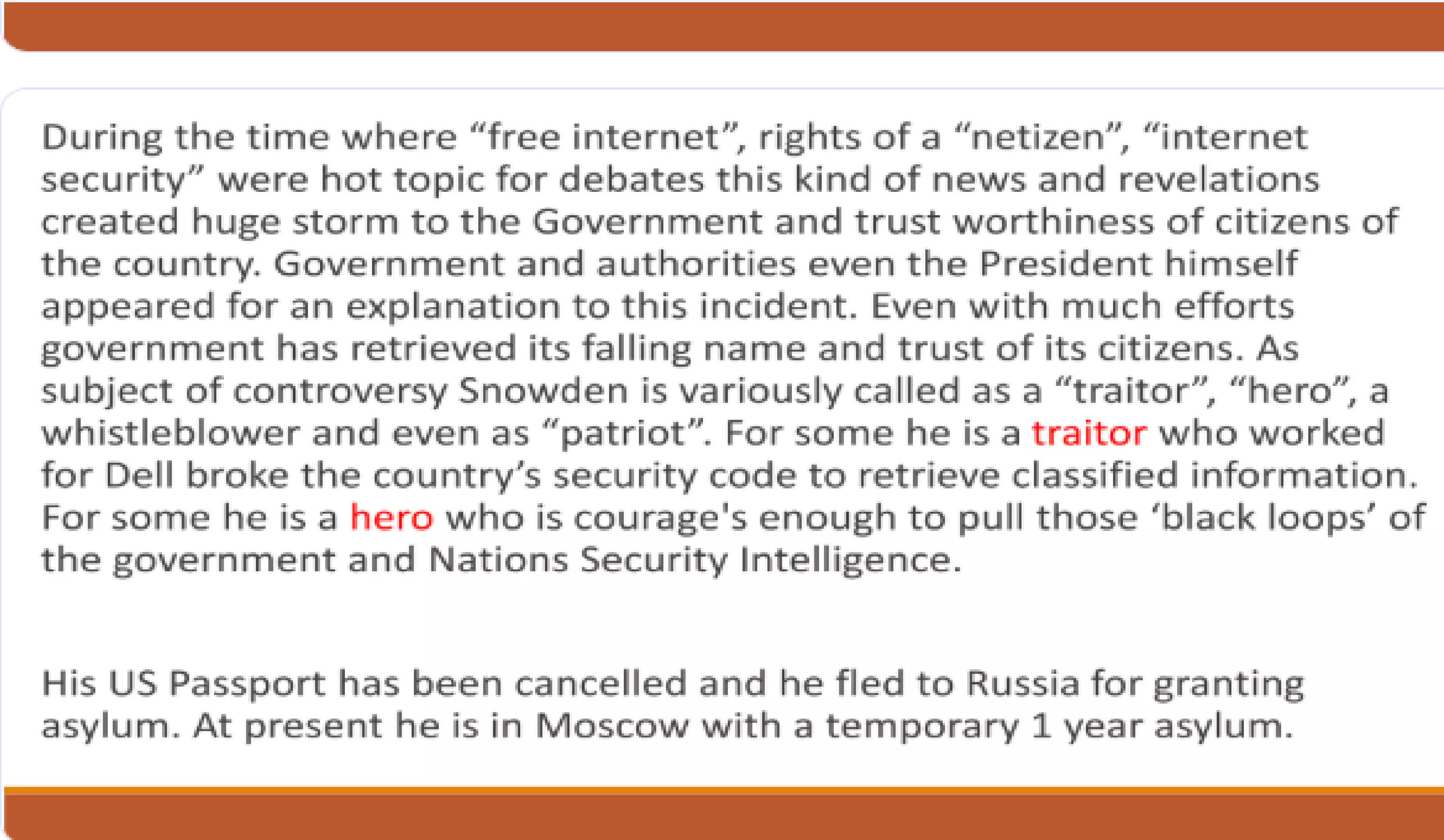


CASE STUDY- EDWARD SNOWDEN SCENERIO:

In 2014, World stood still with a shocking revelation from a computer analyst Edward Snowden.

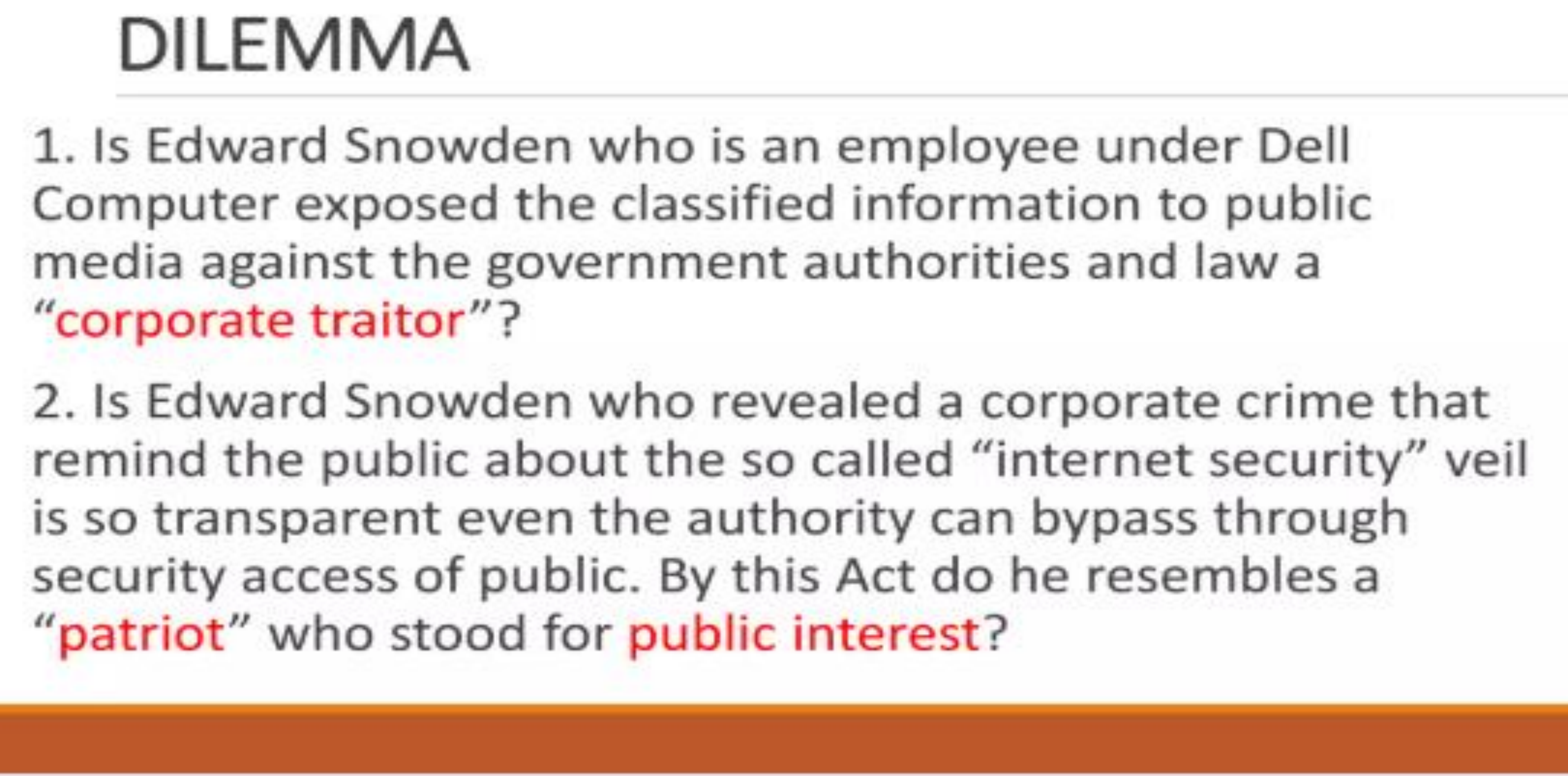
A computer analyst whistleblower who exposed top-secret NSA documents leading to revelations about US surveillance on phone and internet communications.

Edward Snowden



During the time where “free internet”, rights of a “netizen”, “internet security” were hot topic for debates this kind of news and revelations created huge storm to the Government and trust worthiness of citizens of the country. Government and authorities even the President himself appeared for an explanation to this incident. Even with much efforts government has retrieved its falling name and trust of its citizens. As subject of controversy Snowden is variously called as a “traitor”, “hero”, a whistleblower and even as “patriot”. For some he is a traitor who worked for Dell broke the country’s security code to retrieve classified information. For some he is a hero who is courage's enough to pull those ‘black loops’ of the government and Nations Security Intelligence.

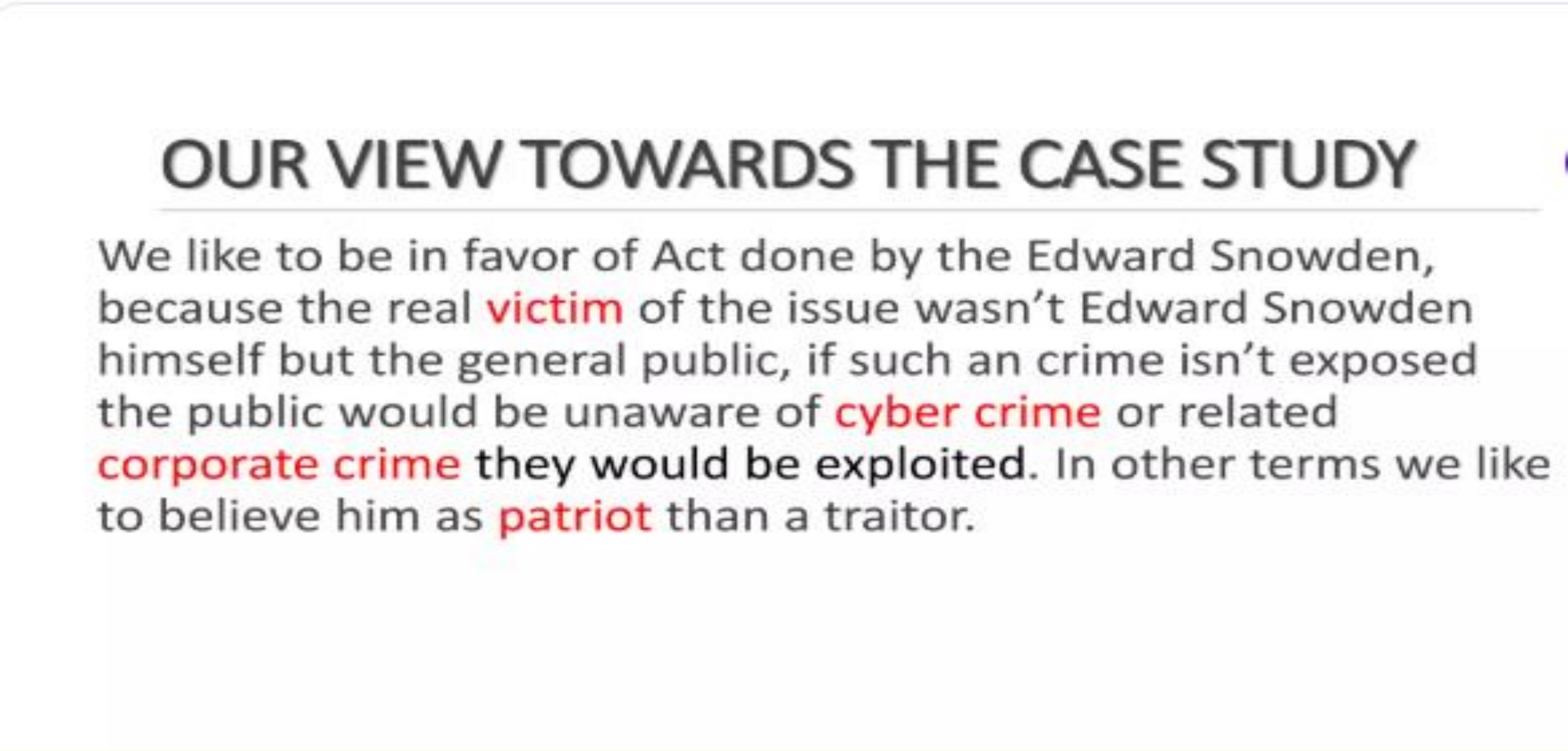
His US Passport has been cancelled and he fled to Russia for granting asylum. At present he is in Moscow with a temporary 1 year asylum.



DILEMMA

1. Is Edward Snowden who is an employee under Dell Computer exposed the classified information to public media against the government authorities and law a "corporate traitor"?

2. Is Edward Snowden who revealed a corporate crime that remind the public about the so called "internet security" veil is so transparent even the authority can bypass through security access of public. By this Act do he resembles a "patriot" who stood for public interest?



OUR VIEW TOWARDS THE CASE STUDY

We like to be in favor of Act done by the Edward Snowden, because the real victim of the issue wasn't Edward Snowden himself but the general public, if such an crime isn't exposed the public would be unaware of cyber crime or related corporate crime they would be exploited. In other terms we like to believe him as patriot than a traitor.

WikiLeaks Case Study

- Introduction:
- - Ethical tension between transparency and national security

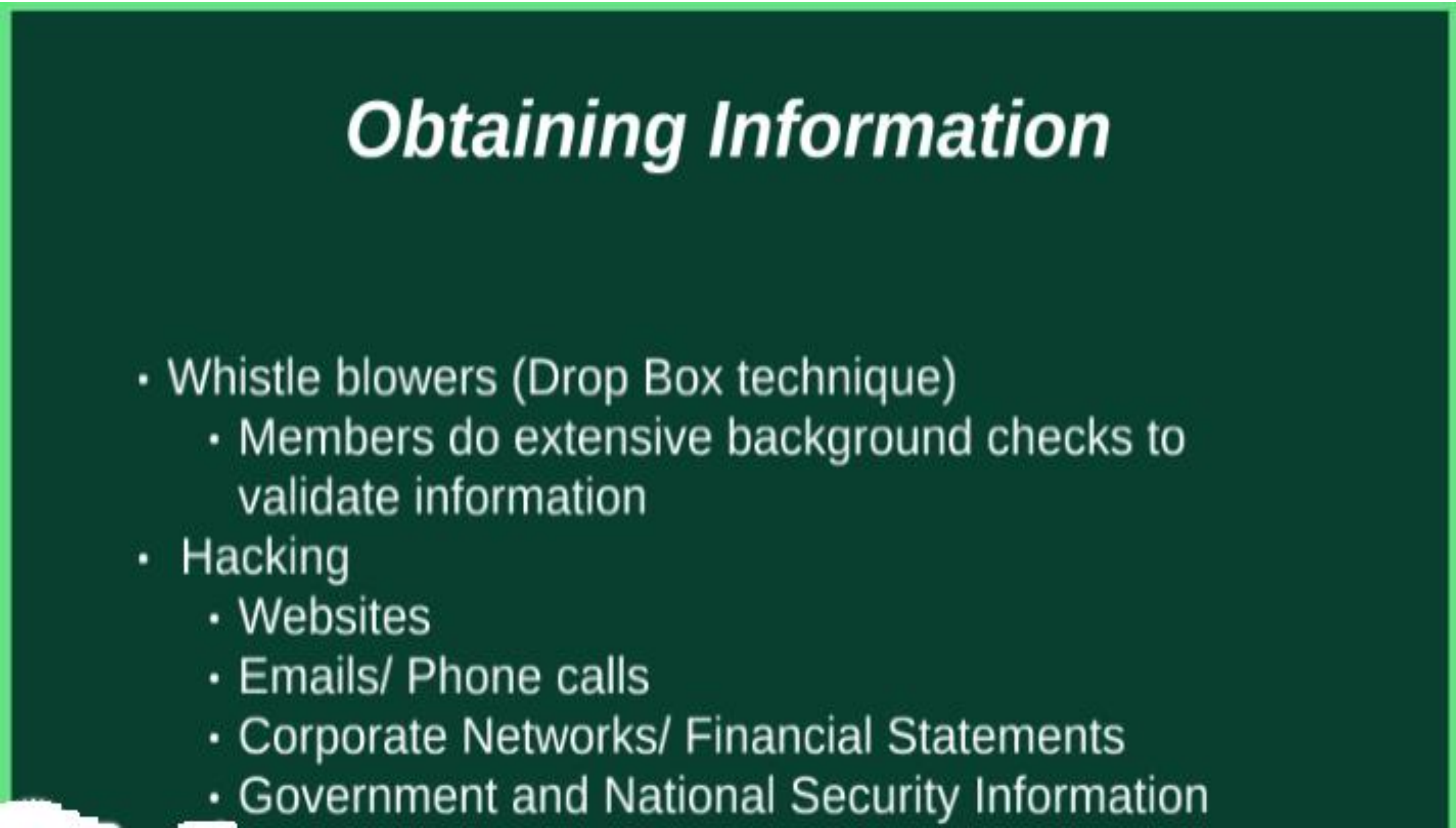
- Theoretical Principles:
- - Freedom of information vs potential harm
- - Accountability of organizations

- Practical Examples: Collateral Murder video, DNC email leak

- Exercise: Evaluate ethical justification
- Solution: Public benefit=8, Harm=6 → Ethical score=2

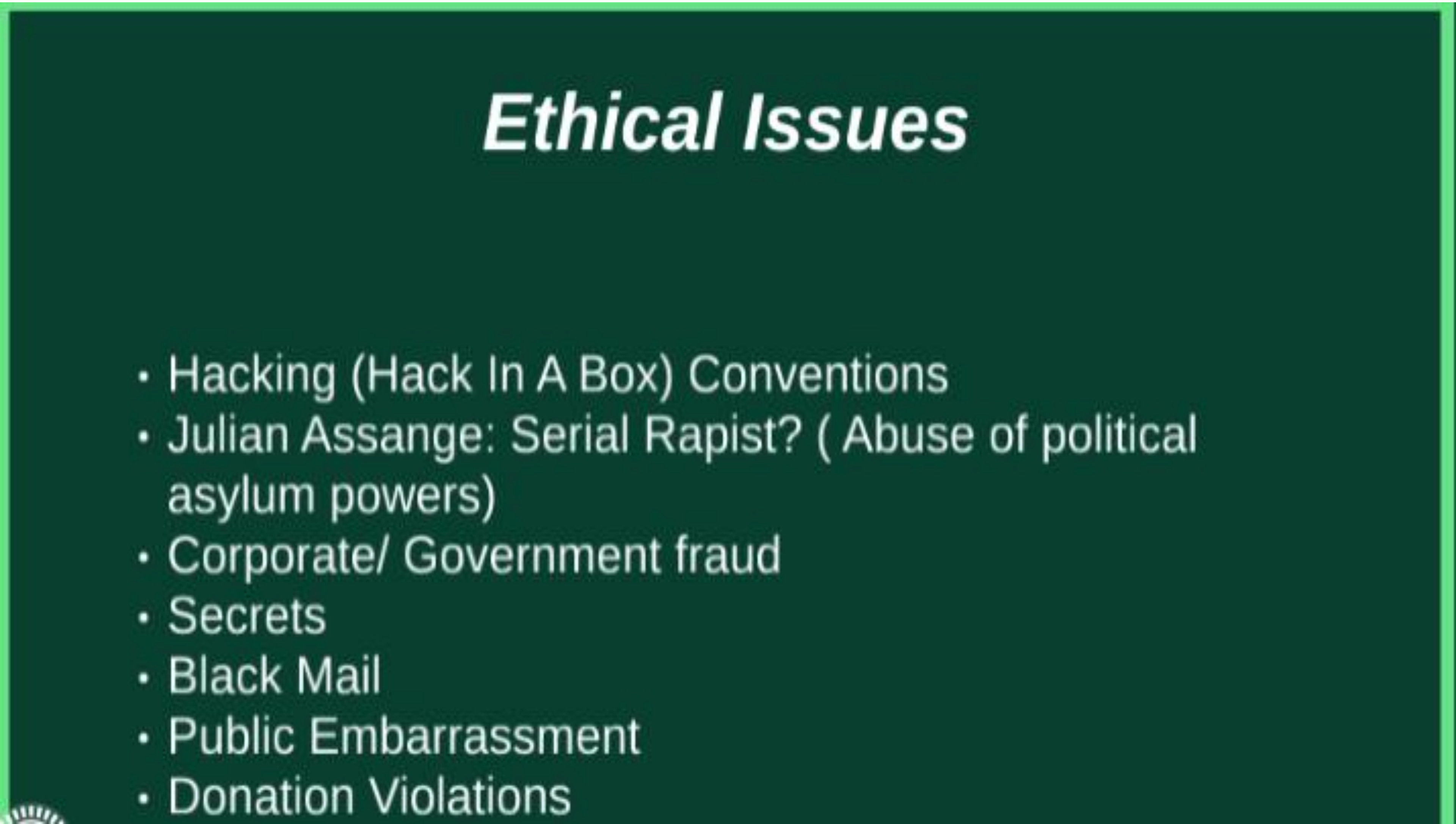
WikiLeaks Background

- Non-profit journalistic organization
- Goal: Bringing important information and news to the public
- Publishes classified media, leaked documents, and secret information
- Founded by Julian Assange in 2006
- 1,200 world wide members, 70 writers, all volunteers



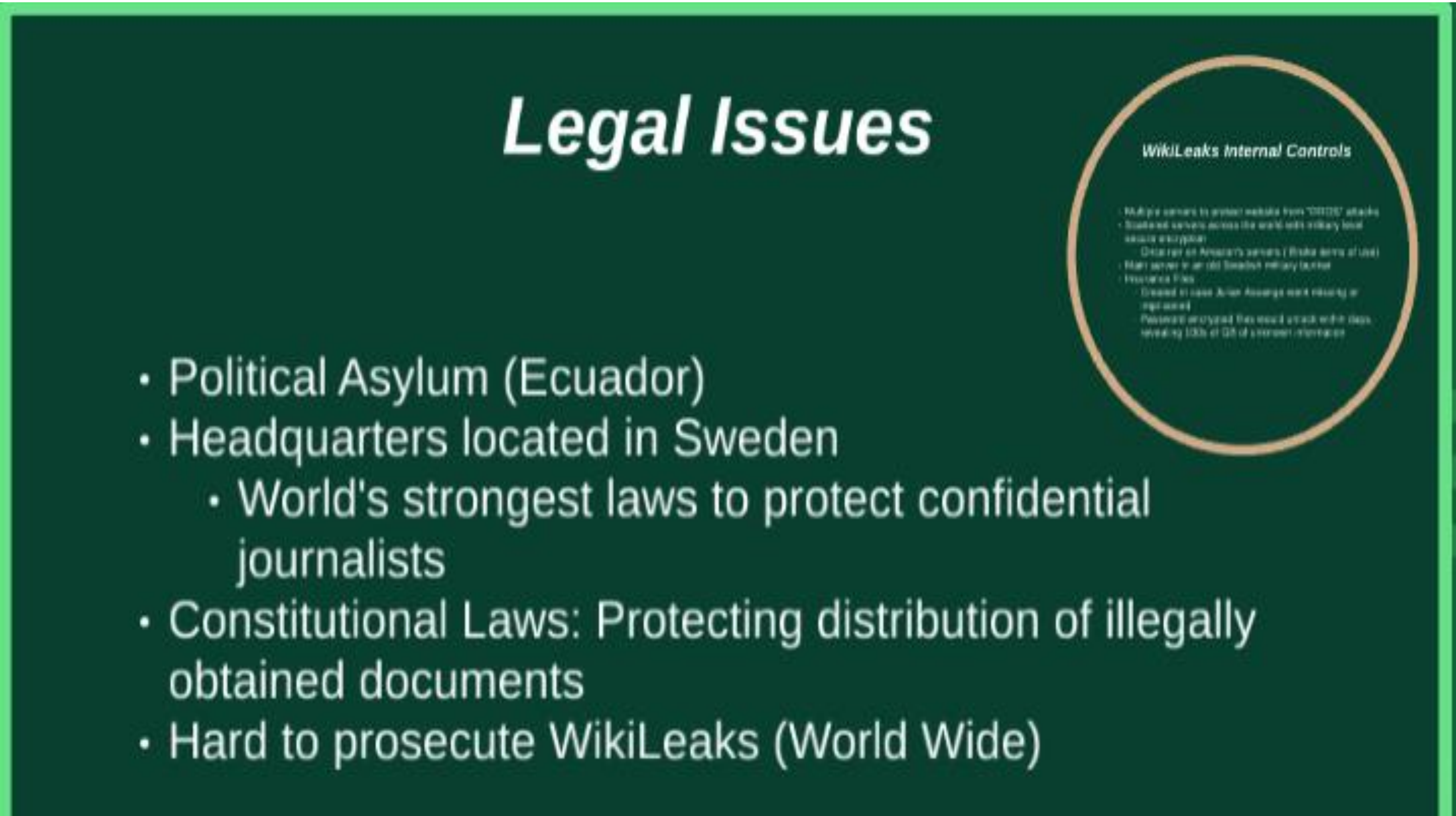
Obtaining Information

- Whistle blowers (Drop Box technique)
  - Members do extensive background checks to validate information
- Hacking
  - Websites
  - Emails/ Phone calls
  - Corporate Networks/ Financial Statements
  - Government and National Security Information



Ethical Issues

- Hacking (Hack In A Box) Conventions
- Julian Assange: Serial Rapist? (Abuse of political asylum powers)
- Corporate/ Government fraud
- Secrets
- Black Mail
- Public Embarrassment
- Donation Violations

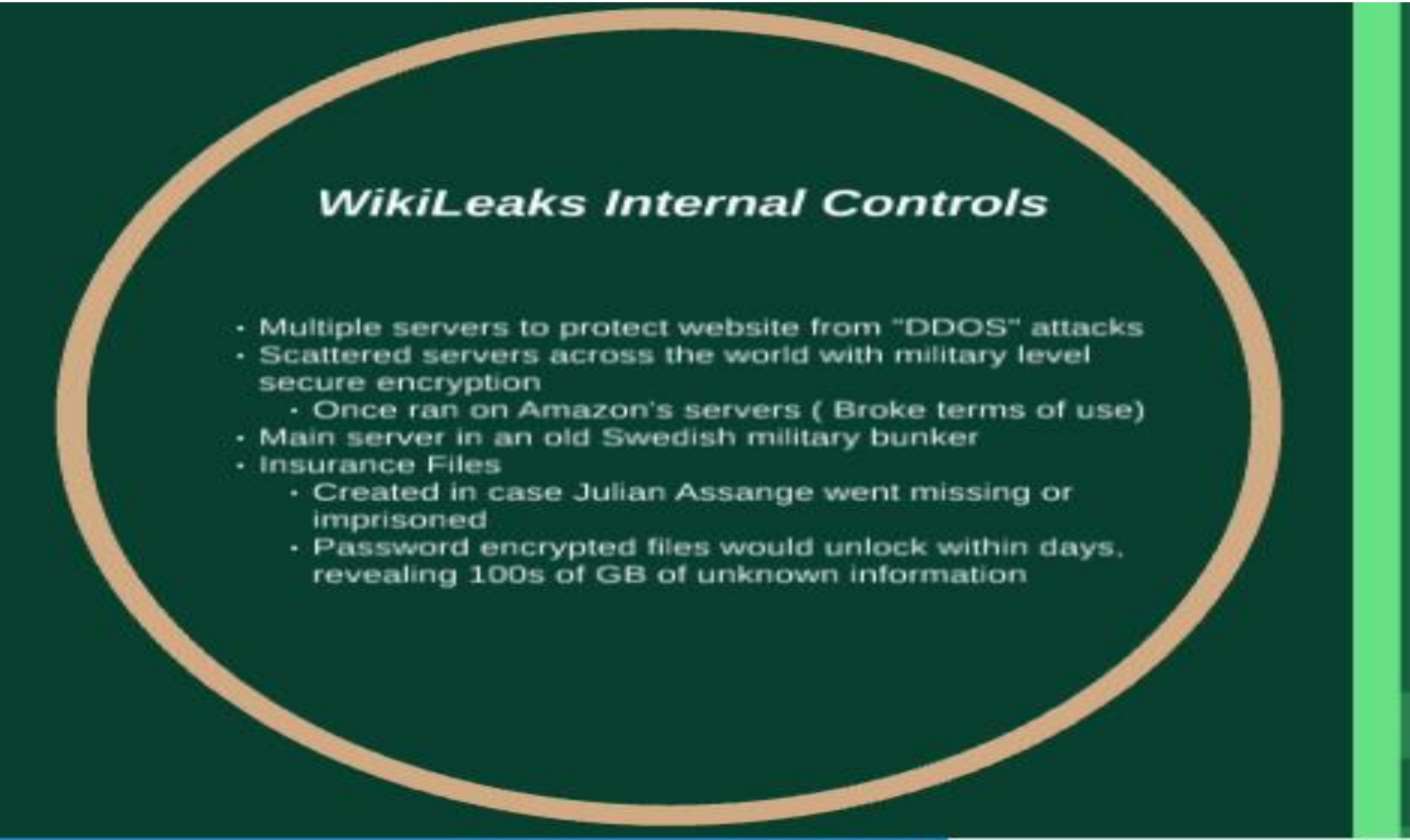


Legal Issues

- Political Asylum (Ecuador)
- Headquarters located in Sweden
  - World's strongest laws to protect confidential journalists
- Constitutional Laws: Protecting distribution of illegally obtained documents
- Hard to prosecute WikiLeaks (World Wide)

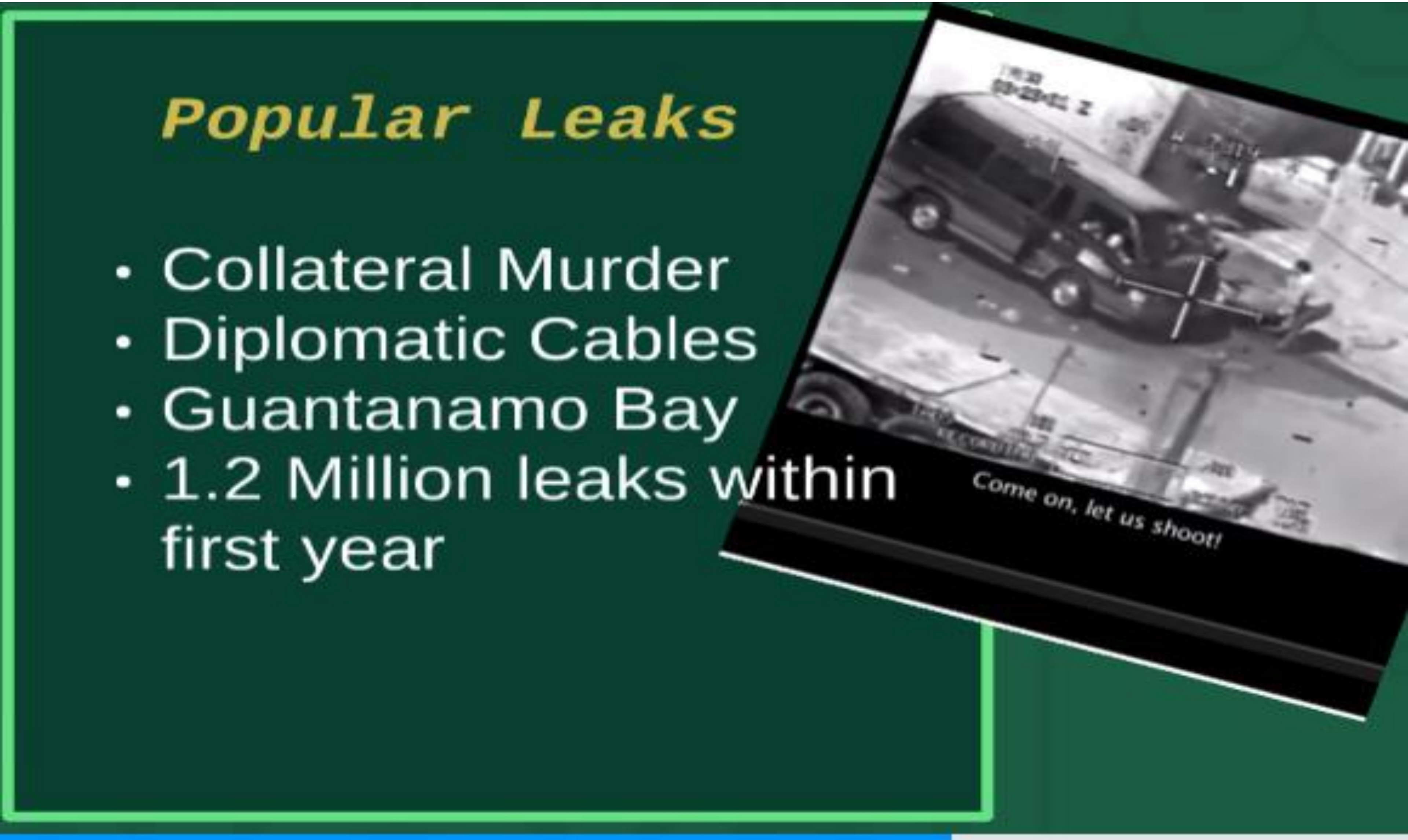
WikiLeaks Internal Controls

- Multiple servers to protect website from "DDOS" attacks
- Scattered servers across the world with military level secure encryption
  - Once ran on Amazon's servers (Broke terms of use)
- Main server in an old Swedish military bunker
- Insurance Files
  - Created in case Julian Assange went missing or imprisoned
  - Password encrypted files would unlock within days revealing 100s of GB of unknown information



WikiLeaks Internal Controls

- Multiple servers to protect website from "DDOS" attacks
- Scattered servers across the world with military level secure encryption
  - Once ran on Amazon's servers (Broke terms of use)
- Main server in an old Swedish military bunker
- Insurance Files
  - Created in case Julian Assange went missing or imprisoned
  - Password encrypted files would unlock within days, revealing 100s of GB of unknown information



Popular Leaks

- Collateral Murder
- Diplomatic Cables
- Guantanamo Bay
- 1.2 Million leaks within first year

Conclusion/ Recommendation

WikiLeaks: Hero or betrayer?

- Personal Recommendation:
  - Continue operations
  - Stay aware of changing laws
  - Generates knowledge about unethical situations
  - Generates security advances

Exercise: Is whistleblowing ethical if company sells user data?
Solution: Ethical: Protect public → justified; Legal: May face retaliation

Mathematical Problem: Net_Ethical_Score = Benefit_public - Harm_organization = 9 - 6 = 3 (Justified)

Legal Considerations

- Introduction:
- - Laws governing hacking and whistleblowing

- Theoretical Principles:
- - CFAA: Unauthorized access illegal
- - Whistleblower Protection Act: Legal safeguards

- Practical Example: Employee hacking colleague’s account

- Exercise: Identify violations
- Solution: CFAA violation, company policy breach, unethical behavior

- Mathematical Problem: $ERS\_H = (Impact*Likelihood)/Mitigation = 7*0.6/3 = 1.4$

Digital Activism

- **Introduction:**
- **- Using technology for social/political change**

- **Theoretical Principles:**
- **- Civil disobedience, hacktivism ethics, utilitarian analysis**

- **Practical Examples: Arab Spring, Anonymous hacktivism**

- **Exercise: Evaluate ethical risks of hacktivism**
- **Solution: Utilitarian: Public good > harm → justified with caution**

- **Mathematical Problem: ERS_H = (Impact*Likelihood)/Mitigation = 9*0.5/3 = 1.5**

Tishk International University
Faculty of Applied Science
Cybersecurity Department

A World of Digital Activists

An Introduction to Digital Activism

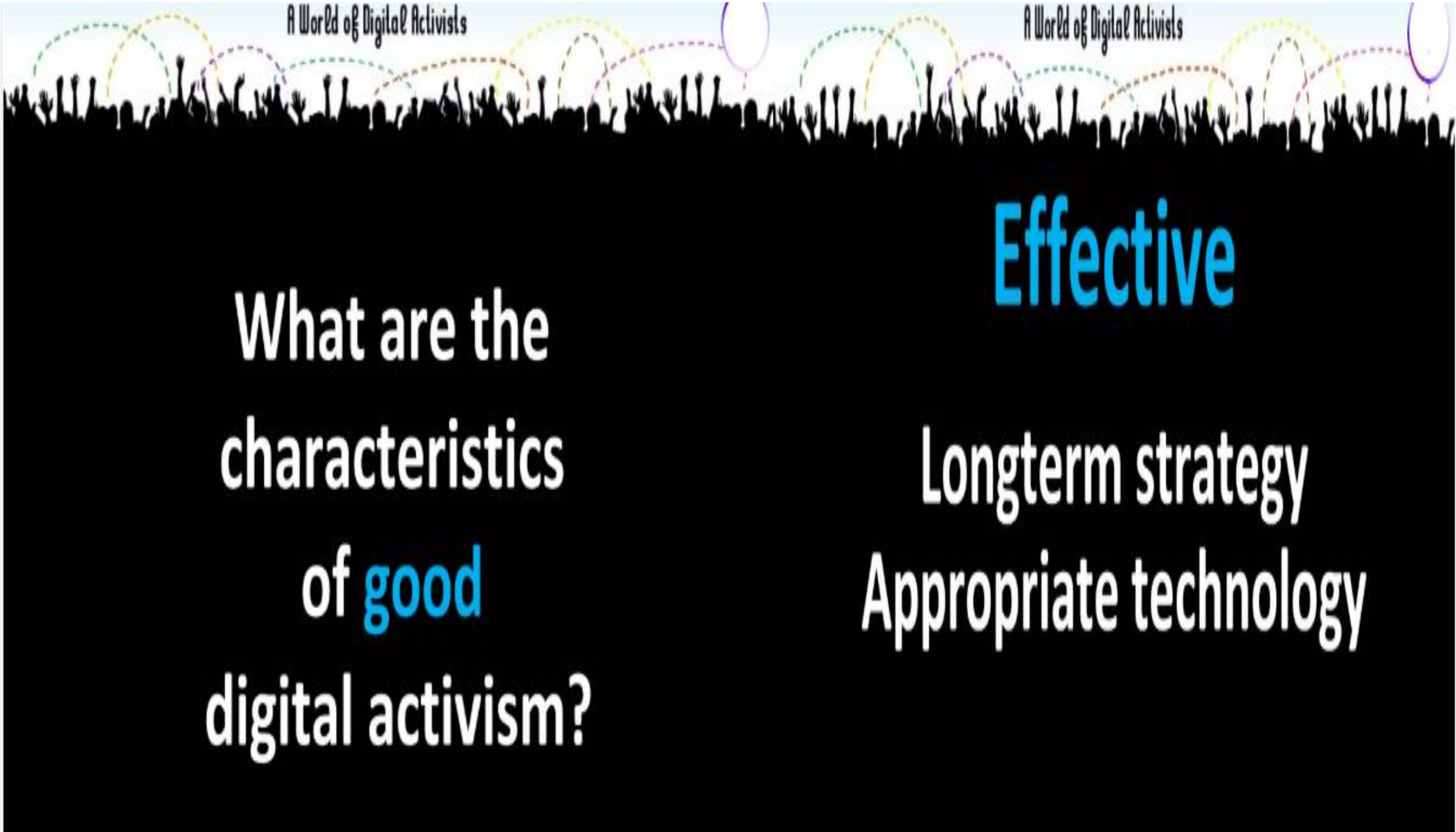
digital activism: grassroots activists using networked technologies for social & political change campaigns

Can you gimme an example?

international rallies organized through Facebook

Blogs and offline citizen journalists collect quake victim names

live SMS updates from protest march


A World of Digital Activists
A World of Digital Activists

What are the characteristics of good digital activism?

Effective

Longterm strategy
Appropriate technology

A World of Digital Activists

Reproducible

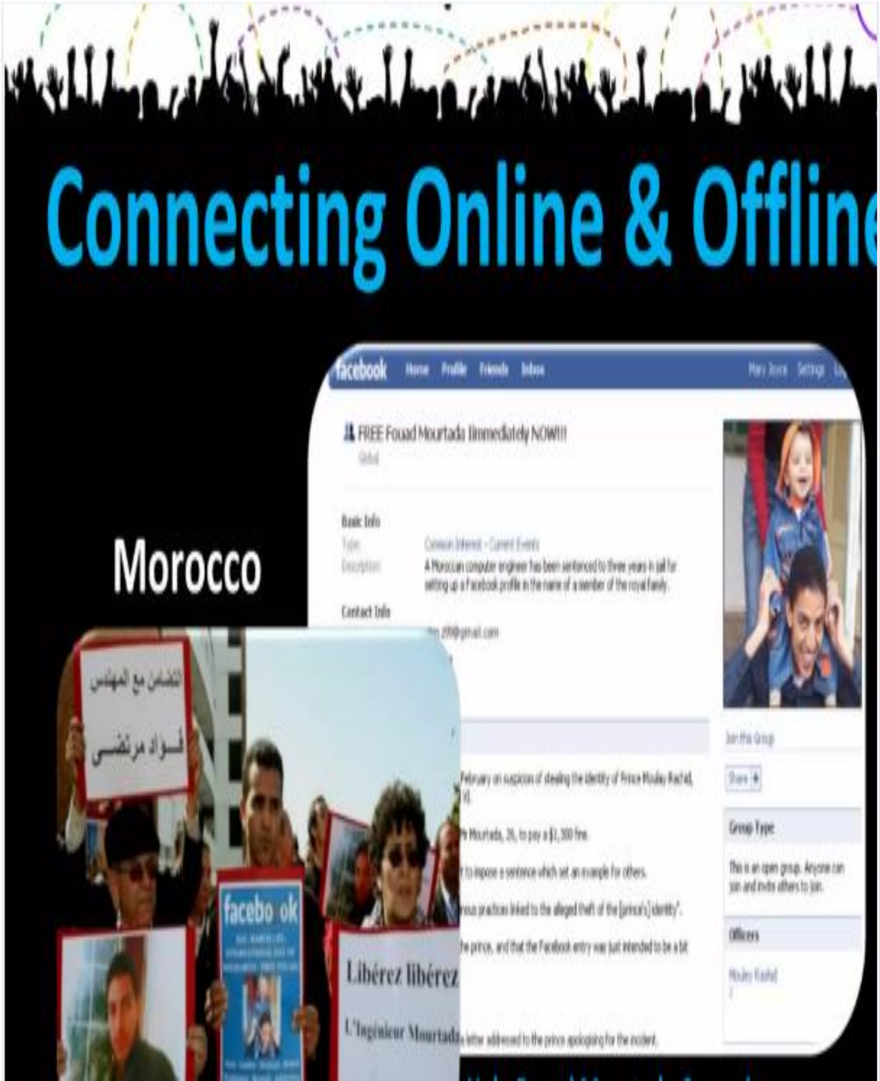
Other activists

Other countries

Other issues

A World of Digital Activists

What are the challenges to digital activism?



Connecting Online & Offline

Morocco

facebook Home Profile Friends Inbox Mary Joyce Settings

FREE Fouad Mourtada Immediately NOW!!!
Global

Basic Info
Type: Common Interest - Current Events
Description: A Moroccan computer engineer has been sentenced to three years in jail for setting up a Facebook profile in the name of a member of the royal family.

Contact Info
zfl0@gmail.com

February on suspicion of stealing the identity of Prince Moulay Rachid, 34.

Mourtada, 26, to pay a $1,300 fine.

to impose a sentence which set an example for others.

practices linked to the alleged theft of the [prince's] identity".

he prince, and that the Facebook entry was just intended to be a bit

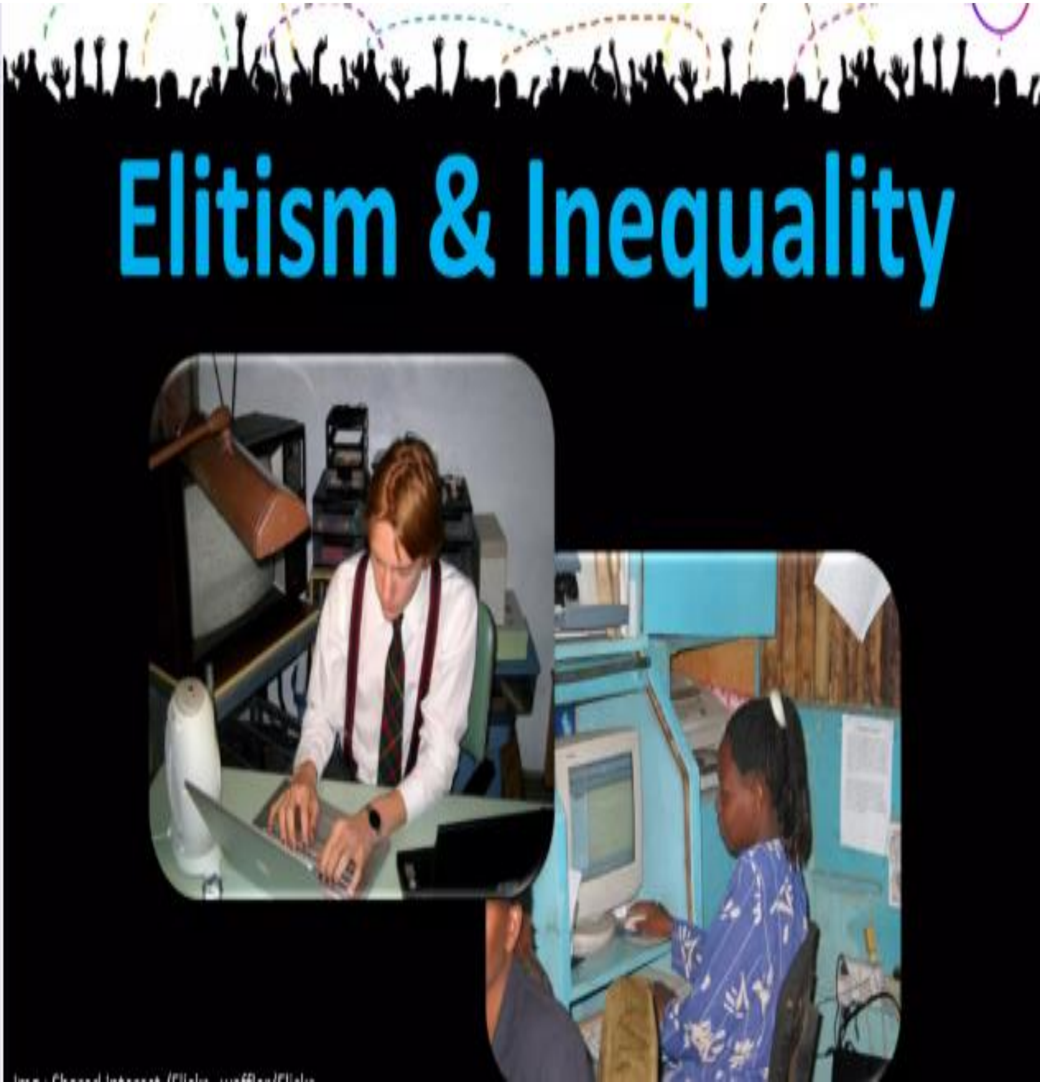
a letter addressed to the prince apologising for the incident.

Join this Group

Share +

Group Type
This is an open group. Anyone can join and invite others to join.

Officers
Moulay Rachid



Elitism & Inequality

Img : Shared Internet /Flickr, wuffles/Flickr

A World of Digital Activists

Hype & Tool Transience

A World of Digital Activists

New Casualties

Ethical Decision-Making Framework

- Introduction:
- - Guides ethical decisions

- Theoretical Principles:
- - Recognize → Judge → Intend → Act
- - Decision analysis using risk and benefit quantification

- Practical Example: Reporting a system vulnerability

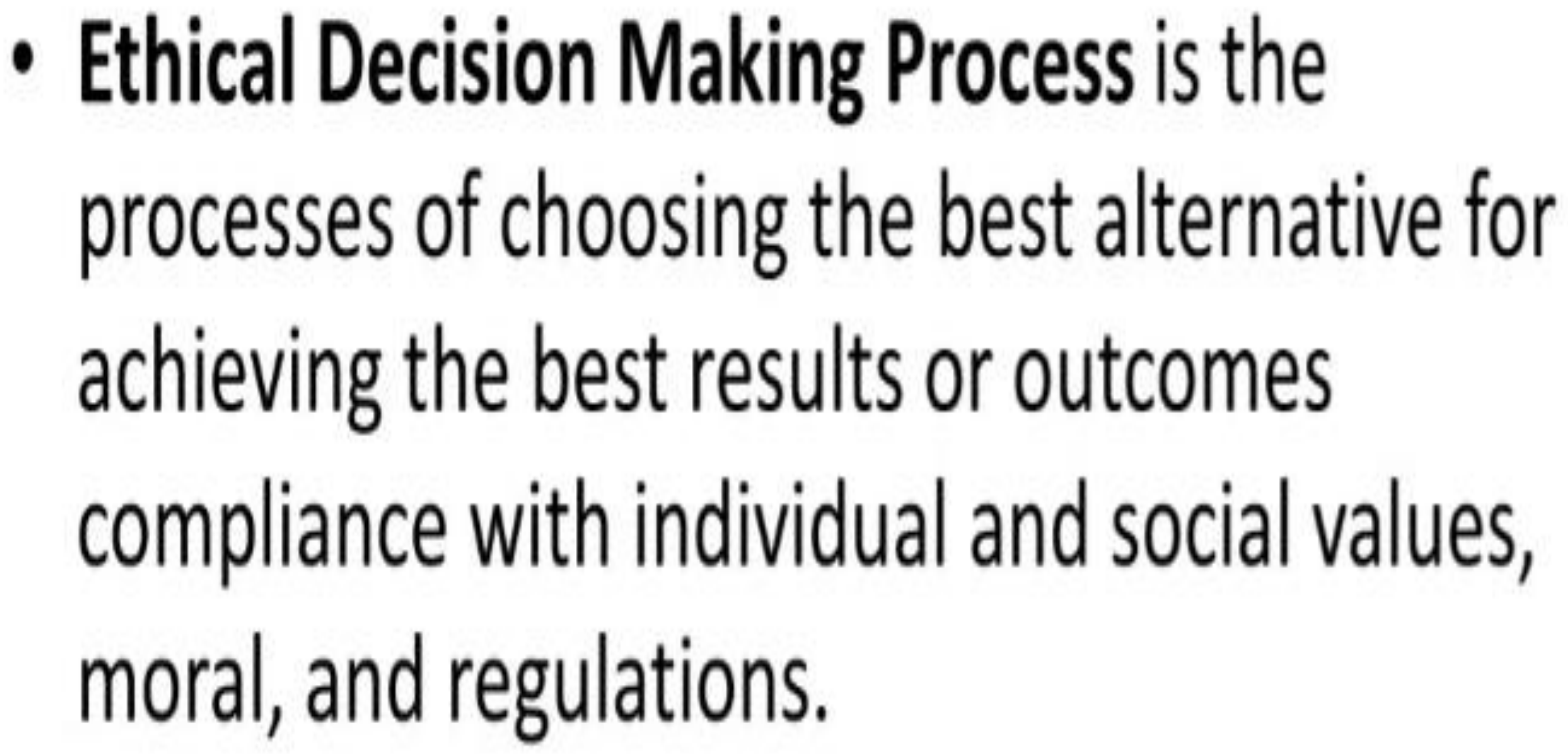
- Exercise: Apply Rest’s Model
- Solution: Recognize → Judge → Intend → Act → ethical action

- Mathematical Problem: Decision Score = (Benefits_public - Harm_individual)/(Legal Risk+Ethical Risk) = (8-2)/(1+1)=3

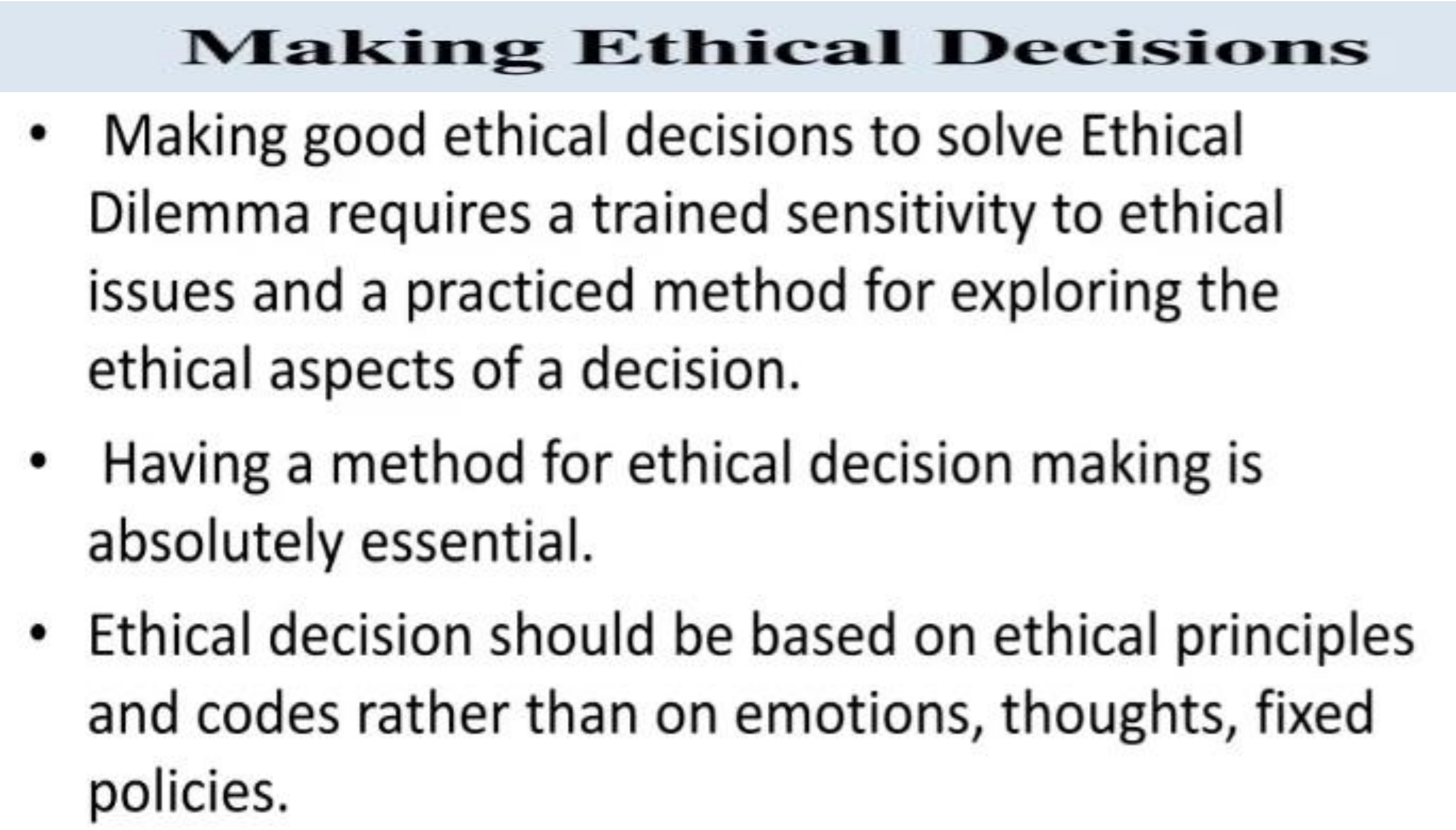
Ethical Decision-Making Framework: A Guide for Resolving Dilemmas

Learn to navigate ethical dilemmas with a systematic framework for decision-making. Understand the steps involved in identifying, analyzing, and resolving ethical issues effectively. Gain insights into prioritizing values and principles to make sound decisions. Evaluate outcomes and ensure compliance with ethical standards and codes.

Ethical Decision

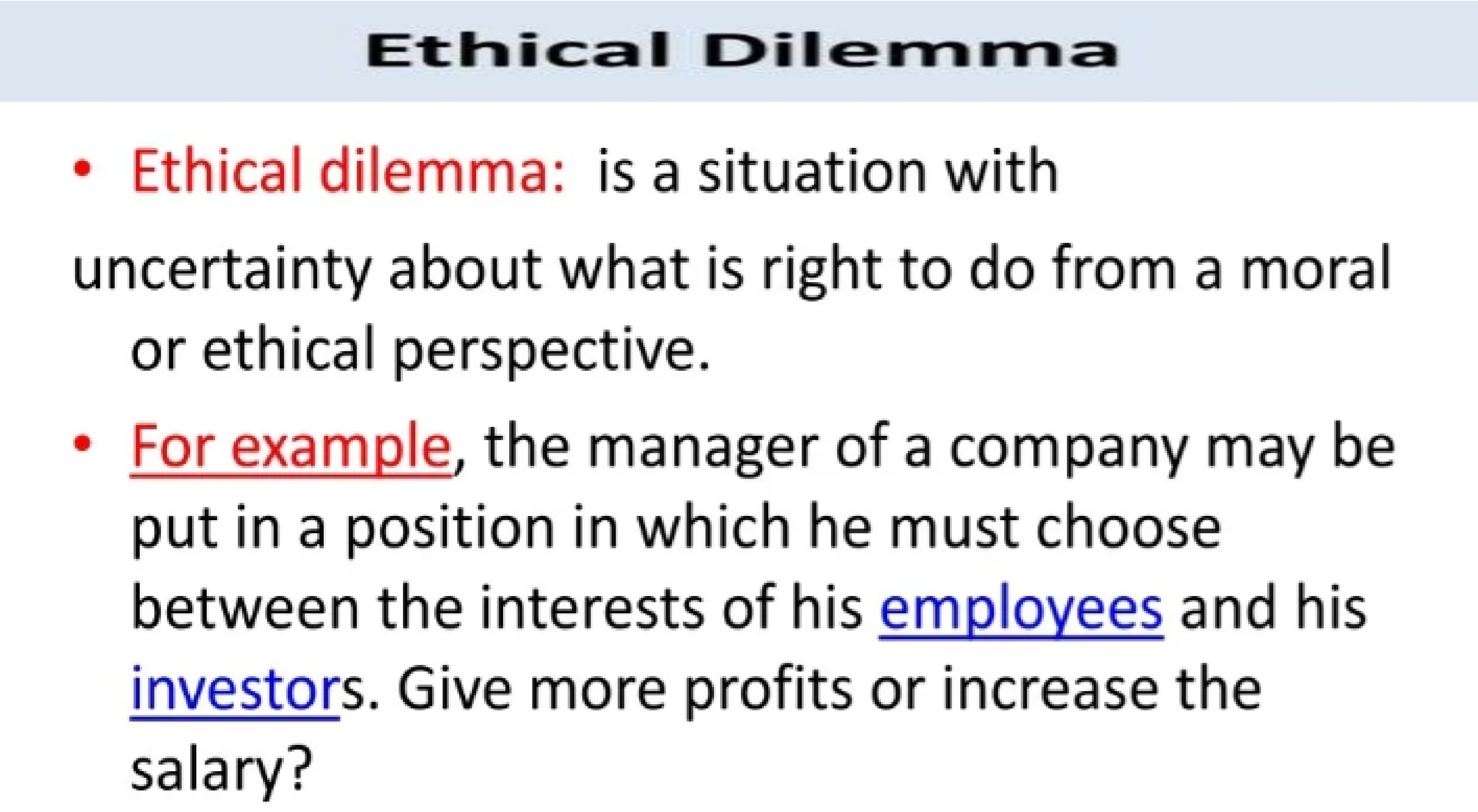


- **Ethical Decision Making Process** is the processes of choosing the best alternative for achieving the best results or outcomes compliance with individual and social values, moral, and regulations.



Making Ethical Decisions

- Making good ethical decisions to solve Ethical Dilemma requires a trained sensitivity to ethical issues and a practiced method for exploring the ethical aspects of a decision.
- Having a method for ethical decision making is absolutely essential.
- Ethical decision should be based on ethical principles and codes rather than on emotions, thoughts, fixed policies.

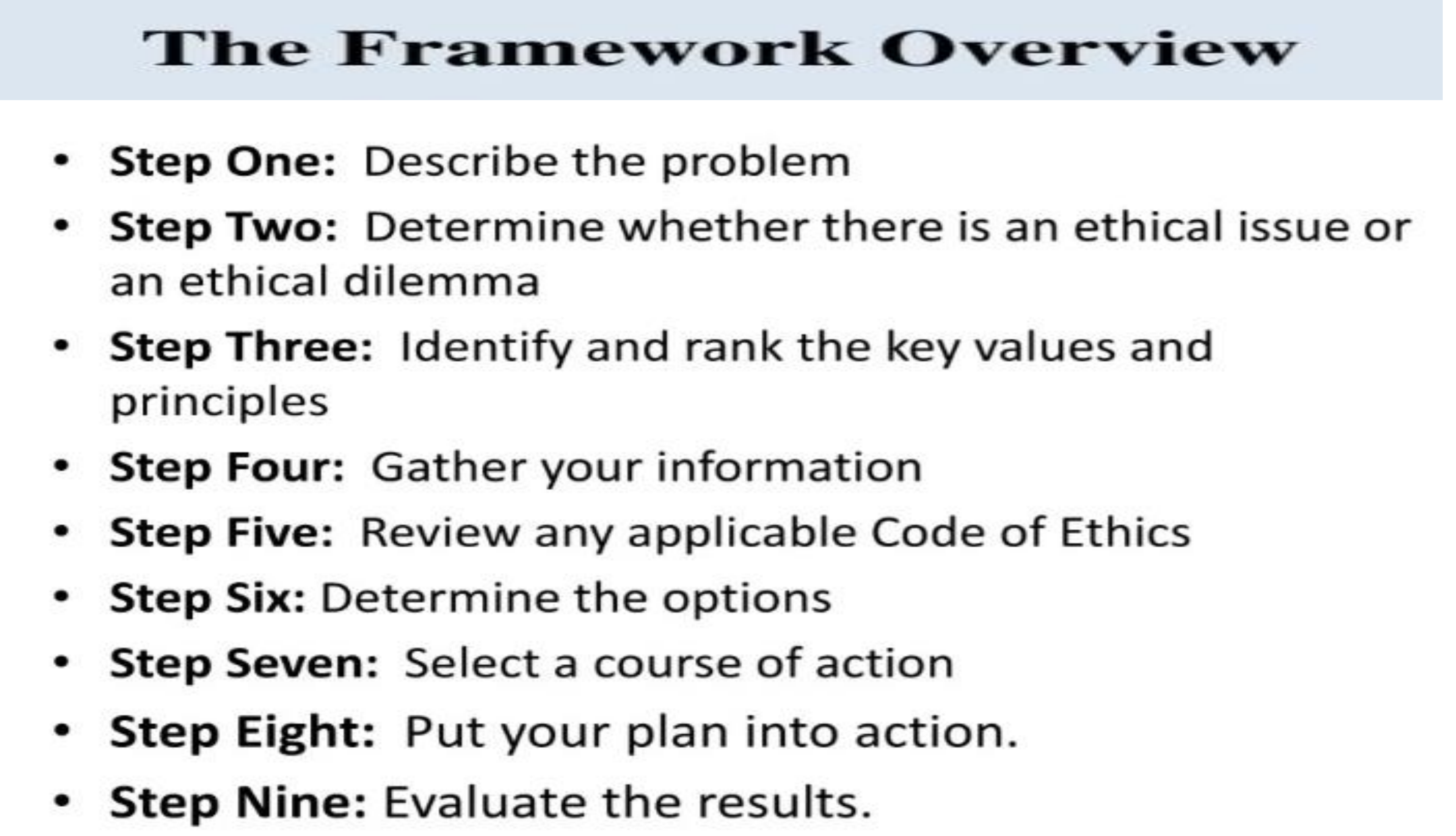


Ethical Dilemma

- Ethical dilemma: is a situation with uncertainty about what is right to do from a moral or ethical perspective.
- For example, the manager of a company may be put in a position in which he must choose between the interests of his employees and his investors. Give more profits or increase the salary?

Ethical Dilemma Defined

- **Example 2 :**
- A new technology is being launched which is good for the company as well as the customers. But, if this is brought into use, a lesser man-power is required for the organization.
- The entrepreneur is now in an ethical dilemma whether he wants to better his clients with good services or be loyal to his employees who have helped the company grow.
- The unpleasantness of the situation arises when neither the clients nor the employees deserve to suffer and it is the entrepreneur's call to take.



The Framework Overview

- **Step One:** Describe the problem
- **Step Two:** Determine whether there is an ethical issue or an ethical dilemma
- **Step Three:** Identify and rank the key values and principles
- **Step Four:** Gather your information
- **Step Five:** Review any applicable Code of Ethics
- **Step Six:** Determine the options
- **Step Seven:** Select a course of action
- **Step Eight:** Put your plan into action.
- **Step Nine:** Evaluate the results.

Case Studies & Discussion

- **Introduction:**
- **- Apply theoretical principles to real-world scenarios**

- **Practical Examples: Sony Pictures Hack, Chelsea Manning leaks**

- **Exercise: Identify ethical/legal breaches; propose mitigation**
- **Solution: Unauthorized access → illegal/unethical; Mitigation: stronger controls, reporting**

Homework & References

- Homework:
- - Essay: Ethical dilemmas in whistleblowing and hacking: Snowden vs WikiLeaks
- - Problem Set: Five scenarios; calculate ERS_H; provide ethical/legal solutions

- References:

- - Tavani, H. T. (2016). Ethics and Technology. Wiley.
- - Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. Cengage Learning.
- - IEEE Code of Ethics: https://www.ieee.org/about/corporate/governance/p7-8.html

Thank you for your listening