

## **Defn**

Whistle-blowing can be defined as the release of information by a member or former member of an organization that is evidence of illegal and/or immoral conduct in the organization or conduct in the organization that is not in the public interest.

## **Loyal Agent Argument**

According to one argument, an employee is an agent of an employer. An agent is a person who is engaged to act in the interests of another person (called a principal) and is authorized to act on that person's behalf. This relationship is typical of professionals, such as lawyers and accountants.

The loyal agent argument receives considerable support from the law, where the concept of agency and the obligations of agents are well developed.

The main obligation of an agent is to act in the interest of the principal. We expect a lawyer, for example, to act as we would ourselves, if we had the same ability. This obligation is expressed in the Second Restatement of Agency as follows: "an agent is subject to a duty to his principal to act solely for the benefit of the principal in all matters connected with his agency."

## **Are Whistle-Blowers Disloyal Agents?**

Although employees have an obligation of loyalty that is not shared by a person outside the organization, the obligation is not without its limits. Whistle-blowing is not something to be done without adequate justification, but at the same time, it is not something that can never be justified.

Second Restatement, to obey all reasonable directives of the principal. This is interpreted to exclude illegal or immoral acts; that is, employees are not obligated as agents to do anything illegal or immoral—even if specifically instructed by a superior to do so.

The law of agency further excludes an obligation to keep confidential any information about the commission of a crime. Section 395 of the Second Restatement of Agency reads in part: "An agent is privileged to reveal information confidentially acquired . . . in the protection of a superior interest of himself or a third person."

## **Conditions for Justified Whistle-Blowing**

1. Is the situation of sufficient moral importance to justify whistle-blowing?  
A cover-up of lethal side effects in a newly marketed drug, for example, is an appropriate situation for disclosure because people's lives are at stake. But situations are not always this clear.
2. Do you have all the facts and have you properly understood their significance? Whistle-blowing usually involves very serious charges that can cause irreparable harm if they turn out to be unfounded or misinterpreted.

3. Have all internal channels and steps short of whistle-blowing been exhausted? Whistle-blowing should be a last rather than a first resort. It is justified only when there are no morally preferable alternatives. Virtually every organization requires employees to take up any matter of concern with an immediate superior before proceeding further—unless that person is part of the problem.
4. What is the best way to blow the whistle? Once a decision is made to “go public,” a host of other questions have to be answered. To whom should the information be revealed? How much information should be revealed? Should the information be revealed anonymously or accompanied by the identity of the whistle-blower? Often an anonymous complaint to a regulatory body, such as the Environmental Protection Agency or the Securities and Exchange Commission, is sufficient to spark an investigation. The situation might also be handled by contacting the FBI or a local prosecuting attorney or by leaking information to the local press.
5. What is my responsibility in view of my role in the organization? The justification for blowing the whistle depends not only on the wrongdoing of others but also on the particular role that a whistle-blower occupies in an organization. Thus, an employee is more justified in blowing the whistle—and may even have an obligation to do so—when the wrongdoing concerns matters over which the employee has direct responsibility.
6. What are the chances for success? Insofar as whistle-blowing is justified because of some good to the public, it is important to blow the whistle only when there is a reasonable chance of achieving that good. ## Employee Privacy

Government is not the only collector of information. Great amounts of data are required by corporations for the hiring and placement of workers, etc..

### **Workplace Monitoring**

Monitoring the work of employees is an essential part of the supervisory role of management, and new technologies enable employers to watch more closely than ever before, especially when the work is done on telephones or computer terminals. Even the activities of truck drivers can be monitored by a small computerized device attached to a vehicle that registers speed, shifting, and the time spent idling or stopped. In addition, employers are increasingly concerned about the use of drugs by workers and the high cost of employee theft, including the stealing of trade secrets. Employers also claim to be acting on a moral and a legal obligation to provide a safe workplace in which employees are free from the risk of being injured by drug-impaired coworkers.

Even efforts to improve employees' well-being can undermine their privacy. Wellness programs that offer medical checkups along with exercise sessions result in the collection of medical data that can be used to terminate employees or defend against workplace injury claims. Although the use of an EAP is usually voluntary, employees are often required to gain approval from an EAP counselor

before seeking company- paid mental healthcare. Some employees thus face the choice of revealing their mental health condition to their company or paying for mental health care out of pocket.

### **Psychological Testing**

Tests that measure job-related abilities and aptitudes have raised little opposition. However, employers have increasingly come to recognize that an employee's psychological traits are important, not only for predicting successful job performance but also for identifying potentially dishonest and troublesome employees. Some critics have charged that no one can pass an integrity test without a little dishonesty. Ironically, the highly honest may be among the most frequent victims of mistakes because they are more forthcoming in their answers.

### **Consumer Privacy**

Businesses have discovered that it pays to know their customers. For example, grocery stores that issue identification cards that are scanned along with the universal product code on each product are able to construct detailed profiles of each customer's purchasing preferences.

If a company can identify the characteristics of potential customers by age, income, lifestyle, or other measures, then a mailing list of people with these characteristics would enable the seller to reach these customers at relatively low cost. Such targeted selling, known as direct mail, is also potentially beneficial to consumers. Another eg: Youtube, facebook, google adsense suggestions.. Companies that specialize in data collection can provide direct marketers with customized mailing lists that target groups with the desired characteristics.

### **Issues in Consumer privacy**

One issue in the use of databases to generate mailing lists is the right of control over information. If we reveal some information about ourselves to a company, does that company "own" the information? For example, does a magazine have a right to sell a list of its subscribers to a direct marketer? Some privacy advocates hold that there should be no secondary use of information without a person's knowledge and consent. Thus, some magazines inform subscribers that they make their list available for direct mail and allow subscribers to "opt out" by removing their name and address from the list.

### **Definitions of privacy**

- Brandeis -> privacy is the right to be left alone.

Many critics have pointed out that the phrase "to be let alone" is overly broad. Individuals have a right "to be let alone" in matters of religion and politics, for example, but legal restrictions on religious practices, such as snake handling, or

on political activities, such as the making of political contributions, do not involve violations of privacy. At the same time, the Warren and Brandeis definition is too narrow, because some violations of privacy occur in situations where there is no right to be let alone. Workers have no right to be free of supervision, for example, even though it can be claimed that their privacy is invaded by the use of hidden cameras to monitor their activity secretly.

- Alan -> “Privacy is the claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others.”
- A third, more adequate definition of privacy: “the condition of not having undocumented personal knowledge about one possessed by others.
  - . A person does not suffer a loss of privacy, for example, when a conviction for a crime becomes known to others, because court records are public documents. Similarly, there is no loss of privacy when an easily observable fact, such as a person’s baldness, is known to others, even if the person is sensitive about it and prefers that others not be aware of it.

## Utilitarian Arguments (Value of privacy)

Some arguments are needed, therefore, to establish the value of privacy and the claim that we have a right to it. One category consists of utilitarian arguments that appeal to consequences, and the second is Kantian arguments that link privacy to being a person or having respect for persons.

One of the consequences cited by utilitarians is that great harm is done to individuals when inaccurate or incomplete information collected by an employer is used as the basis for making important personnel decisions. (like results of improperly administered drug tests)

A drawback to this argument is that it rests on an unproved assumption that could turn out to be false. It assumes that on balance more harm than good will result when employers amass files of personal information, use polygraph machines, conduct drug tests, and so on. Whatever harm is done to employees by invading their privacy has to be balanced, in a utilitarian calculation, against the undeniable benefits that these practices produce for both employers and employees.

Similarly some practices, such as observing workers with hidden cameras and eavesdropping on business conducted over the telephone, are generally considered to be morally objectionable in themselves, regardless of their consequences.

## Kantian Arguments

Two Kantian themes that figure prominently in defense of a right to privacy are those of autonomy and respect for persons.

“But respect for persons,” Benn claims, “will sustain an objection even to secret watching, which may do no actual harm at all.” The reason, he explains, is that covert spying “deliberately deceives a person about his world,” which hinders his ability to make a rational choice.

Fried argues that privacy is of value because it provides a “rational context” for some of our most significant ends, such as love, friendship, trust, and respect, so that invasions of privacy destroy our very integrity as a person. The reason that privacy is essential for respect, love, trust, and so on is that these are intimate relations, and intimacy is created by the sharing of personal information about ourselves that is not known by other people. In a society without privacy, we could not share information with other people (because they would already know it), and hence we could not establish intimate relations with them. Thus, monitoring, in Fried’s view, “destroys the possibility of bestowing the gift of intimacy, and makes impossible the essential dimension of love and friendship.” Similarly, trust cannot exist where there is monitoring or surveillance, because trust is the expectation that others will behave in a certain way without the need to check up on them.

### **Drawbacks**

- It is too strong to assert that all instances of people being watched unknowingly result in deceiving people and depriving them of a free choice. Otherwise, we would be violating people’s right of privacy by observing them strolling down a street or riding a bus.
- Intimate relations such as love and friendship do not consist solely in the sharing of information but involve, as one writer says, “the sharing of one’s total self—one’s experiences, aspirations, weaknesses, and values.” Consequently, these relations can exist and even flourish in the absence of an exclusive sharing of information.

### **Privacy on the internet**

Imagine that most of the stores you entered created a record of your visit including not only your purchases but also what merchandise you looked at, how long you took, what route you followed through the store, what other stores you had visited, and what you bought there.

The most common method for obtaining information covertly is the installation of a “cookie,” which is a file placed on a user’s hard drive that recognizes a repeat user and stores information from past visits. Cookies benefit users by eliminating the need to enter information each time, but they can also provide the site owner with “clickstream” data about what pages are visited and how much time is spent on each one.

The explosive growth of the Internet as a consumer marketplace is a benefit to consumers and businesses alike. sites that offer free content depend on

advertising, and advertising space is much more valuable if it can be tailored to individual users.

### **What's wrong with information collection**

Store owners, if they wish, could follow consumers around to see what merchandise they examined. Computers do not observe us without our knowledge or intrude into our private lives the way psychological tests or hidden cameras do. The Internet is arguably a public arena

“Collecting data cheaply and efficiently will take us back to the past (where people are divided by rank).” For example, by means of frequent flyer programs, airlines identify their better customers and offer them special treatment.

### **Principles for protecting privacy**

The Federal Trade Commission list of five principles is representative of the many documents on Internet privacy. 1. Notice/Awareness. 2. Choice/Consent. 3. Access/Participation. Allow consumers access to the information collected about them and the opportunity to contest the accuracy or completeness of the data. 4. Integrity/Security. Inform users of the steps taken to protect against the alteration, misappropriation, or destruction of data 5. Enforcement/Redress. Assure consumers that the company follows responsible information practices and that there are consequences for failing to do so.

### **Implementing internet privacy**

Its decentralized, democratic structure makes centralized, authoritarian approaches ineffective, as does its global reach.

The main approach to date has focused on government regulation and self-regulation by the industry

We can protect privacy through both formal and material means. Although we need laws against theft (formal), we also protect property with locks (material). A material solution consists in the development of various privacy enhancing technologies (PETs). Among such means are services that permit “proxy surfing” by hiding the identity of the user’s computer and remailers that forward e-mail stripped of any identifying markers. Cookie-management software exists that can block or disable cookies.