

MAKERERE UNIVERSITY BUSINESS SCHOOL
FACULTY OF COMPUTING AND INFORMATICS
DEPARTMENT OF INFORMATION SYSTEMS

E-COMMERCE

BENT III

TOPIC VI: Environment of electronic commerce: legal and ethical issues

Ethics is a set of moral principles or rules of how people are expected to conduct themselves. It specifies what is considered by society to be right or wrong.

Issues of privacy, ownership, control, and security must be confronted in implementing and understanding the ethical challenges of EC.

Business ethics (also known as *corporate* or *enterprise ethics*) is a code of values, behaviors, and rules, written or unwritten, for how people should behave in the business world. These ethics dictate the operations of organizations

INTELLECTUAL PROPERTY LAW AND COPYRIGHT INFRINGEMENT

The legal system is faced with the task of maintaining a delicate balance between preserving social order and protecting individual rights.

Intellectual Property in E-Commerce

Intellectual property (IP) refers to property that derives from the creative work of an individual, such as literary or artistic work. Intellectual property can be viewed as the ownership of intangible assets, including inventions, ideas, and creative works. It is a legal concept protected by patents, copyrights, trademarks, and trade secret law (known as **Intellectual property law**).

There are various intellectual property law specialties. Those specialty laws are interrelated and may even overlap.

Recording Movies, Shows, and Other Events

A common method of infringement is to bring video cameras and smartphone cameras to movie theaters, stadiums, etc. and record the performances. Pirate Eye (pirateeye.com) is one of the companies that manufactures devices that discover and identify the presence of any digital recording device, monitor remotely in real time, and much more.

A common problem is the illegal copying of e-books, which, is damaging not only to authors

and publishers but also to our culture. This situation requires international collaboration.

Copyright Infringement and Protection

Numerous high-profile lawsuits already have been filed regarding online copyright infringement related to EC and the Web.

A **copyright** is an exclusive legal right of an author or creator of intellectual property to publish, sell, license, distribute, or use such work in any desired way. In the United States, content is automatically protected by federal copyright laws as soon as a work is produced in a tangible shape or form. A copyright does not last forever; it is good for a set number of years after the death of the author or creator (e.g., 50 years in the United Kingdom). After the copyright expires, the work reverts to the public domain (or becomes publicly available). See fairuse.stanford.edu/overview/public-domain and thepublicdomain.org.

In many cases, corporations own copyrights. In such a case, the copyrights will last up to 120 years, or even longer. The legal term for the use of a work without permission or contracting for payment of a royalty is **copyright infringement**.

File Sharing

One of the major methods of violating copyrights is *file sharing*. File sharing became popular in the late 1990s through facilitating companies such as Napster. One of the players in this area is The Pirate Bay. The loss to copyright holders is estimated to be several billion dollars annually.

Privacy in E-Commerce

The reason for privacy concerns stems from the fact that in using the Internet, users are asked to provide some personal data in exchange for access to information (such as getting coupons, allowing downloads, etc.). Data and Web mining companies receive and gather the collected data. As a result, users' privacy may be violated. Privacy concerns limit EC. Privacy rights protection is one of the most debated and frequently emotional issues in EC and social commerce. Many EC activities involve privacy issues ranging from collection of information by Facebook to the use of RFID.

Illegal Visits to Torrent, Streaming, and Download Sites (i.e., Piracy)

There are billions of visits to websites that provide free videos, music, books, and other media to people that do not pay for the legal versions. Known as piracy, this phenomenon is performed worldwide. In some countries (e.g., Latvia), almost half of the population visit pirate sites

Digital ethics, trust and security

A website that sells products or services is built on trust. When buying online, buyers disclose their physical (shipping) addresses and other personal information. They share, through a trusted payment provider, their financial details and allow their money to change hands once a product is shipped. With no physical contact between buyers and sellers and without a physical exchange of money for products or services, the issue of trust and strengthening the brand's credibility becomes ever so important.

Publish reliable information about products and services

Furthermore, with no possibility of touching, feeling and looking in person at products or services, buyers need to ascertain products meets their expectations. That is why it is so important that contents disclosed online inspire trust. This is key to help costumers building trust. To be trustworthy, information about products or services offered by the business should have the following characteristics:

Be accurate: the information must disclose valid and verifiable details. It cannot be designed to deliberately confuse clients or contain false information

Be relevant: a product description should be about the given product

Be informative: it should provide enough details for the buyer to build a full picture about the product, describing its key features in sufficient detail

Contain mandatory disclosure: any mandatory information (such as health hazards, child warnings or other information prescribed by law in a specific jurisdiction) should be provided in full.

Whilst there is some flexibility (except for mandatory disclosure items defined by law), sellers must strive to provide as much of the above information as possible, to earn the trust of buyers and not to lose potential customers.

Nevertheless, providing full information about the product is not enough. In addition to the above, the seller is required to assure buyers that they are dealing with a reputable business, a business that will not disappear with their money.

How to provide such an assurance to buyers? Particularly through payment providers. **Payment providers** require that certain amount of valid information is shown, accessible on a company's website and validated. This information includes legal address, several legal documents (user agreement, privacy policy, terms and conditions, etc.) and other mandatory disclosure information. This list may be different depending on the jurisdiction of both the business and the payment provider. There is also other confidential information that the payment provider asks before accepting the opening of an e-commerce payment account. This confidential information includes business owner's details, identification, bank account information for the business, etc.

The institution verifies the data provided against the Interpol lists, other databases to ensure business owners are not known for money laundry, financing terrorism, etc. These checks, as intrusive as they may seem, protect buyers, sellers, and the institution itself by reducing the probability of fraud. In addition, in certain industries (such as medical, financial, and legal services), regulators oversee and mandate the publication of specific information on corporate websites, including medical diplomas, licenses, and bar membership for lawyers.