

## Civil liability for Violating Electronic Privacy and Information Centers

Dr , Nabeel Zaid Magableh Dr , Naser Mohammad Saeed Balawi .  
Law Collage , Jadara University , Jordan

### Introduction

There is a civil and legal responsibility for electronic information and data collection centers and is often a contractual liability, unless it leads to a serious breach and harm to the user. Responsibility is transferred to a tort liability, and communication companies and social networking companies learn that and in their usage agreements electronically Unfair or incomprehensible to absolve itself of any liability you may expect, but the fact that these terms and employment agreements are similar in the compliance contracts and the conditions of compliance which the user can only accept in total Otherwise, the contract is not contracted, and it is forced to agree and sign (I agree). Does this contract or agreement absolve the truth of its responsibility for violating the privacy of the electronic user, and is it entitled to collect data and information available therein. The information filters were initially e-mail such as yahoo and then Google and then via social media such as face book, what is up and the information in it, then the search engines and then social information and finally the mobile numbers and the number of people in the world, Who are those? What will they use all this information ??? How to deal with programs, filtering, storage and programming websites for the future ??? All questions have one answer to those who own Internet resources, but really have we thought about this? We have provided an effective legal system to address it.

**Keywords:** Civil Law, Civil Liability, Electronic Privacy

**DOI:** 10.7176/JLPG/85-06

**Publication date:** May 31<sup>st</sup> 2019

Who controls the programming of information in the information centers, what are the powers of the engines and the information banks in their use and how they are used, what kind of information is this ??? What is individual privacy and how can it be violated in practice?

Questions to draw the answer and to determine the search, we ask what is privacy? What are Information Centers? How does this information affect the national security of the state internally? What information do these centers have? Legitimacy of the inheritance of information for children and grandchildren? Are there international laws and treaties to protect personal privacy? Are there laws to protect the privacy of the citizens of the state? How are electronic information sold and what are the means of maintaining it ?

Where are we to maintain our personal, societal and national characteristics? Did companies consult us to sell information about us and how to accept the sale of information mainly ?

First we must define the information centers and then we address the electronic privacy in the information and the nature and forms of information, and then review the civil responsibility.

### Chapter 1: Information and privacy centers for information and data.

Information Centers: are the modern electronic entities where information is collected and stored for the purposes of consumer knowledge, authentication of their means of communication and the confidence that the designated person has the authority of the sending networks requesting service from the provider to the service.

In short, the elements that make up the information center are the single provider and the multiple consumers (service seekers). For example, a company such as Microsoft is the provider of all products and electronic programs around the world and the rest of its users are consumers for its services. (Reciprocity), then there is the information that the consumer (applicant service) voluntarily approved to the provider, and this information is necessary and not for the submission of the service was provided to him.

If the information is given compulsorily and in a manner similar to the legally recognized compliance contracts, it is therefore part of the deal and only the transaction is concluded , and the employment agreements often provide for the protection and security of consumer information. Is this privacy maintained or changed and changed with the change of ownership These companies<sup>(1)</sup>, as was the case in the sales and acquisition transactions between many communication companies and information groups. The last of these transactions was the sale of what's up company to face book on 21/2/2014<sup>(2)</sup>, and will not be the last in light of the rapid growth of unlimited applications For communications .

<sup>1</sup> - See Article 1 of the Agreement for the provision of the What's up service at <http://www.whatsapp.com/legal>), which allows the service to be accepted only by accepting the preconditions that cannot be modified or negotiated by the consumer.

<sup>2</sup> - See Al-Quds Al-Arabi newspaper at <http://www.alquds.co.uk/?p=135903>.

What safeguards are the information that consumers have deposited with" what's up" <sup>(1)</sup>and what is their fate, and how a citizen of a country can make sure that personal information is not disclosed by numbers, photos, videos and other accounts .

The British intelligence agency known as the (GCHQ) has collected images from the cameras of millions of users of the yahoo program for talks around the world<sup>(2)</sup>. The famous US company Yahoo has denied any prior knowledge of the intelligence program , Describing it as a violation of privacy "absolutely unacceptable " .

The report was based on information leaked by former CIA agent Edward Snowden, According to a leaked document, British intelligence gathered images of millions of Yahoo users on camera conversation, including sexually explicit images, although it was not targeted ,The work of the Authority is in accordance with the law.

The National Security Agency (NSA), according to the report, helped carry out the process, called "optic nerve", during which user images were stored between 2008 and 2010, and in just six months in 2008, Million users around the world.

"Unfortunately, it seems that a surprising number of people are using videoconferences to show intimate parts of their bodies to other people," says the leaked document.

The document adds that the yahoo chat program allows more than one person to watch a broadcast for the same camera without sending a reciprocal broadcast by these people, "which means that this is sometimes used to broadcast pornographic material."

"Completely new level," yahoo company said in a statement: "We were not aware of it, or to overlook such activity."

"This report, if true, represents a whole new level of violation of the privacy of our users and is absolutely unacceptable, and we strongly demand that the governments of the world work to reform the surveillance law to comply with the principles we set out in December," the statement said.

"We are committed to maintaining the confidence and security of our users, and continuing our efforts to expand encryption across all our services."

"All the work of the government communications headquarters is carried out in accordance with a strict legal and methodological framework that ensures that our activities are monitored, necessary and appropriate, and there is strong oversight including the State Department, intelligence commissioners, And the Parliamentary Intelligence and Security Committee <sup>(3)</sup>.

The privacy violation presents special challenges in cyberspace. Digital technology facilitates news gathering, In theory digital government records should create an unprecedented opportunity for citizens to access and supervise them, but many judges and legislators, fearful that access may facilitate identity theft, employment discrimination or other illegal behavior, decide to limit access to electronic files.

Judges also express concern that anyone from a remote location who does not have a "legitimate interest" in the community can browse the court records or land registry records and publish them on the Internet and fear that bloggers do little more than spread rumors, violate copyright laws, Identify the identities of victims of sexual abuse and do all this hidden behind the anonymity of the Internet. They are concerned that citizen journalists, mobile phones, cameras and registrars have invaded courtrooms and recorded what has happened in the online trial, Off its mean lacks dignity and support gatekeepers often access to government records and procedures as liberated in theory, but after becoming a low-cost access and easy, you may wonder about the wisdom. They think the information is too valuable or too dangerous to be online.

For example, in September 2008, a California trial judge prevented Arrange County Register from publishing "by all means and means of communication, whether personal or electronic, through audio or visual recording or any printed media "Any testimony given by any witness in a joint class action on salaries and hours filed by the newspaper's carriers against them, and concluded that such a prohibition was necessary to prevent subsequent witnesses from being affected by testimony given by others <sup>(4)</sup>.

In the end, the Appeals Chamber reversed this, and ruled that the risk that news reports might affect witnesses was insufficient to justify censorship. And that by using other alternatives, less intrusive, such as warning witnesses not to read the newspaper may accomplish the same goal. However, the widespread media on the Internet convinced the court judge to overlook some 70 years of legal precedents that preclude similar prior restrictions.

The problem is that the cautious (ISP )will choose to register the content and leave the subscriber and the copyright holder outlining their respective rights. The Digital Millennium Copyright Act (DMCA) allows copyright holders to use "certificates of attestation to perform an administrative certificate" to force an (ISP) to disclose the identity of the subscriber. Although such memos should only be issued to reduce the activity of the

<sup>1</sup> - See the service agreement for What's up on the website mentioned earlier, as Article 2 of the Convention does not assume responsibility for any damages such as leakage of information from the use of another site, what is the case after the merger with Face book will remain responsible for information or transfer responsibility Of the new site.

<sup>2</sup> - <http://www.ammonnews.net/article.aspx?articulo=184578>

<sup>3</sup> - <http://www.ammonnews.net/article.aspx?articulo=184578#sthash.Cz0AqHE1.dpuf>

<sup>4</sup> - California court , Farouk alabasiri , Share contract of electronic information , dar aljameah , Alexandria Egypt, 2002 , page 152.

violation, the risk is that the birth certificates may be misused for the purpose of violating the established principles of protecting the right to privacy of information and electronic data.

The emergence of the Internet as important communication technology and as a platform for the deployment of journalists creates new legal complexities, but the governing principles must remain constant. It should not depend on whether The journalist acts as a "mainstream media" or publishes a blog. Judges and legislators must follow the principles that have long protected the press and people's right to know regardless of the media affiliation or media used.

## **Chapter 2 : The legal system for dealing with the means of social communication**

Information systems have developed rapidly and rapidly in recent years, This tremendous development has led to an evolution in the processing and transmission of data through computers and information networks, the so-called "information revolution". Information systems have become the basis of all aspects of life. Control aircraft to the bank and e-mail, and enables us to access people, information and libraries and access services quickly and without much effort or time.

On the other hand, the spread of the Internet has generated new types of crime, called cybercrime, and new means and tools have been created to commit traditional crimes, making it difficult to track crime and its perpetrators. Examples include theft with credit card information or unauthorized access to mail In particular, cyber crime has a broader scope than the traditional crime of lack of geographical boundaries and lack of restrictions on movement within the information network, and punitive legislation no longer exists Keeping in mind that the current legislation and the courts can not apply certain penalties for crimes committed using electronic means.

In many cases, the perpetrator remains unknown and can not be accessed for using fictitious names or sites or unregistered e-mail and other types of tricks using Technical means The proof of cybercrime is more difficult and more complex than conventional crime, where it is easy to destroy and wipe out electronic data and information immediately and thus erase the effects and means of committing the crime and the personality of the perpetrator. In addition, Attacks committed through or directed to or through an information system Electronic crime has acquired elements distinguishing it from conventional crime both in terms of the means used in the commission or the place of commission or the place of the attack. This creates difficulties in criminalizing acts committed by electronic means The availability of the required physical element in the legislation in force or the lack of a legal element which is to criminalize the act or not to address the legislation in force for acts aimed at the information system or the information network <sup>(7)</sup>.

Cybercrime is a major challenge for legal systems in both developed and developing countries. The process of legislation takes time to be an obstacle to combating cybercrime quickly. The direct effects of cybercrime are the violation of privacy and access to electronic data and information to individuals or countries. Of electronic media is always concerned about the fear of leaking data and private information and violating privacy.

In view of the laws of electronic transactions, we find that it aims to achieve specific objectives These objectives are:

- Establish uniform legal rules for the use of electronic transactions and signatures and facilitate their application in the public and private sectors through reliable electronic records.
- Trust in the authenticity, integrity and integrity of transactions, signatures and electronic records <sup>(1)</sup>.
- Facilitate the use of electronic transactions and signatures at the local and international levels to be used in all fields, such as government procedures, trade, medicine, education and electronic payment.
- Remove barriers to the use of electronic transactions and signatures.
- Preventing misuse and fraud in electronic transactions and signatures.
- Preserving privacy and criminalizing illegal access to electronic data and information.

It is clear from these objectives that the legislator is willing to keep pace with modern scientific progress in the management method and use the tools of scientific progress and impose a new culture through laws governing electronic transactions.

However, such violations can occur if they occur, it entails civil liability in addition to other legal responsibilities, and this civil liability is the compensation for the damage that resulted from them.

Civil liability is required in accordance with the principles of civil law in general the availability of several conditions, including <sup>(2)</sup>:

1. The validity of the contract between the parties to judge the validity of the contract. The invalid contract shall not apply to this liability and the legal qualification required for the contractor or the entity that maintains the data or information such as the age of majority or authorized to sign the company, Such as telecommunications

<sup>1</sup> - For more information, see Osama Ahmed Badr, (2005) Consumer Protection in E-Contract, Al-Jama'a Publishing House, Egypt. And For further information, see Fawzi Hamad Khater (2001), International Information Technology Contracts, First Edition, Dar Al-Thaqafa Publishing, Amman, Jordan.

<sup>2</sup> - For more information see Abdul Razzaq al-Sanhouri (1934), The Theory of Contract, Cairo University Press, Cairo, Egypt.

companies, banks, shopping malls and even e-government employees such as civil and other security services in general, while this is not envisaged in tort.

2. Exemption from liability may be agreed upon, but this prior exemption is not in tort due to its nature as a general principle.

3 - The need to direct an excuse to claim compensation for damage to the violator of privacy before the lawsuit, unless it is exempted by agreement, and therefore do not hear the lawsuit only after this excuses, and this excuses is not required in tort, but only in the responsibility of the nodal.

4. In the value of compensation and warranty, the infringing entity, if proven, is committed to the direct or expected segregation at the time of conclusion of the contract, except for the serious damage that may occur. In this case, the damage is expected and significant in case of leakage of data and electronic information and violation of privacy.

5. Apply the liability rule of the contractor (contracting company) for the work of its employees directly in case of any deliberate or unintentional violations, while in tort liability there is no dependency.

6. Jurisdiction Where in contract liability the law of the place of conclusion of the contract is usually the law applicable or the law chosen by the parties, whereas in tort liability the law of the place of the incident is the applicable law and the competent court is the location of the incident.

There is no doubt that civil liability in such cases is either contractual or tortious . If the party that leaked, sold or transferred the information is contracted to the user, the liability is contractual in this case and is governed by the terms of the contractual liability and if there is no contract between them, Concise.

The victim must prove the contract, the fault and the damage in the liability contract, while in tort liability must prove the wrong and damage with minor differences in the civil laws of each country, and this leads us to the importance of the existence of international treaties governing such responsibility to have a specificity commensurate with the electronic violation and unite The legal rules of the majority of the world in these matters.

## Conclusion

We find through this research that the privacy of the electronic user especially needs its own laws because of the tools used and the nature of the potential violation and methods of proof in civil and criminal law and international jurisdiction, and therefore recommend the separation of the law that protects privacy from any legal rules scattered in the Constitution or the legal rules in the National laws, and we would like to have an international model law that protects this privacy, information and electronic data.

## References

- 1 - See Article 1 of the Agreement for the provision of the What's up service at <http://www.whatsapp.com/legal>), which allows the service to be accepted only by accepting the preconditions that cannot be modified or negotiated by the consumer.
- 2 - See Al-Quds Al-Arabi newspaper at <http://www.alquds.co.uk/?p=135903>.
- 3 - See the service agreement for What's up on the website mentioned earlier, as Article 2 of the Convention does not assume responsibility for any damages such as leakage of information from the use of another site, what is the case after the merger with Face book will remain responsible for information or transfer responsibility Of the new site.
- 4 - <http://www.ammonnews.net/article.aspx?articulo=184578>
- 5 - <http://www.ammonnews.net/article.aspx?articulo=184578#sthash.Cz0AqHE1.dpuf>
- 6 - California court , Farouk alabasiri, Share contract of electronic information , dar aljameah , Alexandria Egypt, 2002 , page 152.
- 7 - For more information, see Osama Ahmed Badr, (2005) Consumer Protection in E-Contract, Al-Jama'a Publishing House, Egypt. And For further information, see Fawzi Hamad Khater (2001), International Information Technology Contracts, First Edition, Dar Al-Thaqafa Publishing, Amman, Jordan.
- 8 - For more information see Abdul Razzaq al-Sanhouri (1934), The Theory of Contract, Cairo University Press, Cairo, Egypt.