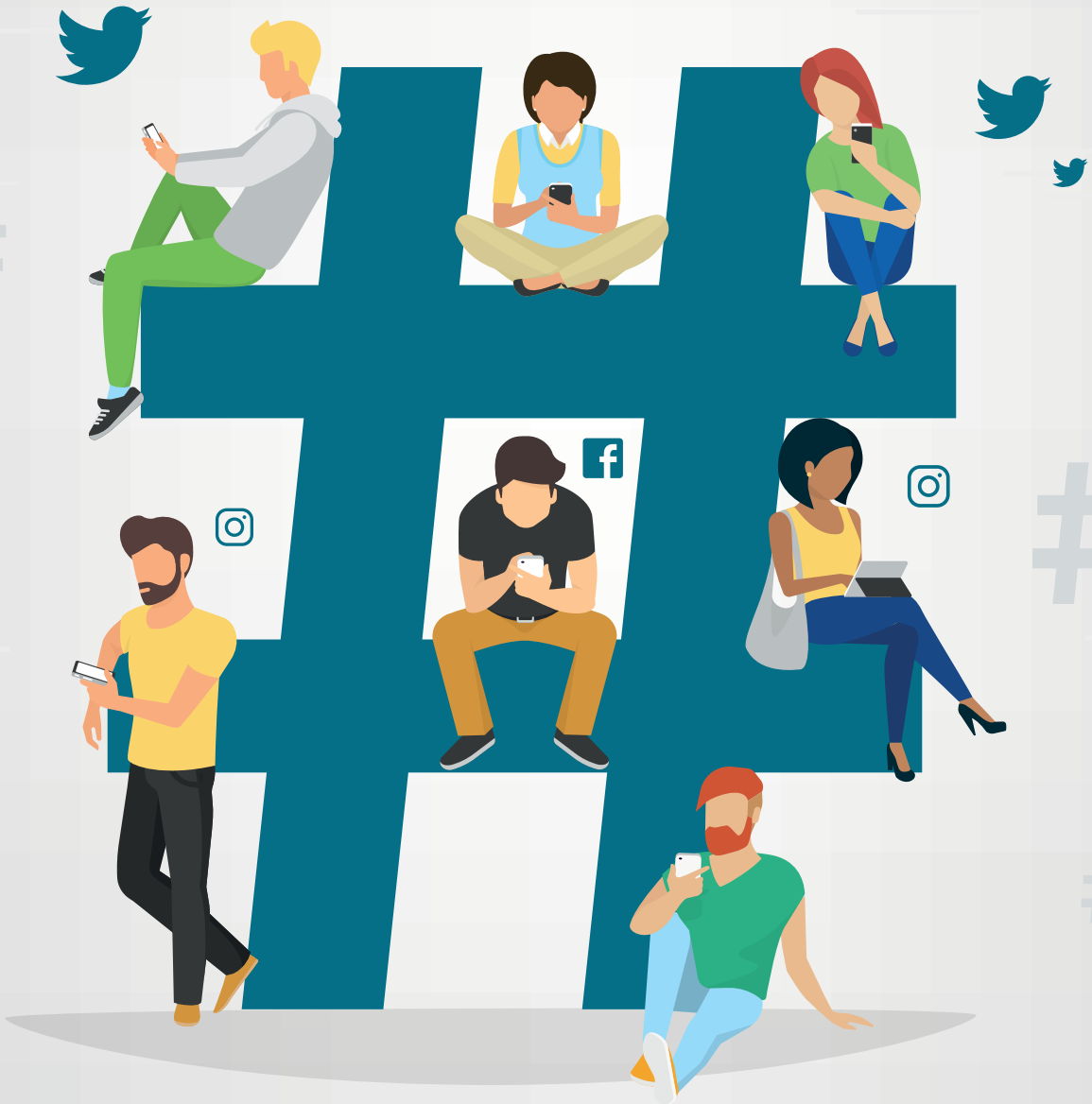
The Right to Freedom of Expression Online in Jordan



Kingdom of the Netherlands

ICNL
INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW

Index

Introduction

Social media has become a vital tool for individuals around the world to express themselves, communicate with others, obtain and share news, and explore areas of interest. In Jordan, seventy-five percent of adults use social media—primarily Facebook and Twitter—daily and for a variety of purposes, ranging from sharing personal photos to running a business or political campaign. Recognizing social media's growing reach, a number of countries have adopted regulatory frameworks to ensure safe and legal use of social media platforms and to prevent illicit online activities such as hacking and data theft.[1] In doing so, however, countries have adopted or are considering regulations on online activity that negatively impact freedom of expression.

Jordan is one such case. Since October 2017, the Government of Jordan has repeatedly attempted to amend the Kingdom's law on cybercrime to further regulate activity on social media in ways that would limit or chill expression online. In their most recent form,[2] the proposed amendments to Cybercrimes Law No. 27 of 2015 would newly criminalize and penalize broadly-defined expressive acts like spreading rumors or false information online.

In fact, Jordanians are already subject to a host of provisions and conditions stipulated in existing laws and within social media platforms that make the Government's efforts to expand the regulation of social media an unnecessary enterprise. Few among the public are aware of these laws, moreover, and their implications for individuals' online activity. The International Center for Not-for-Profit Law (ICNL) is therefore pleased to present this Guide to the existing legal instruments that currently govern expressive activity on social media platforms in Jordan. We hope the Guide will be a useful resource for the public, civil society organizations, activists, and anyone interested in the regulatory framework for online expression.[3]

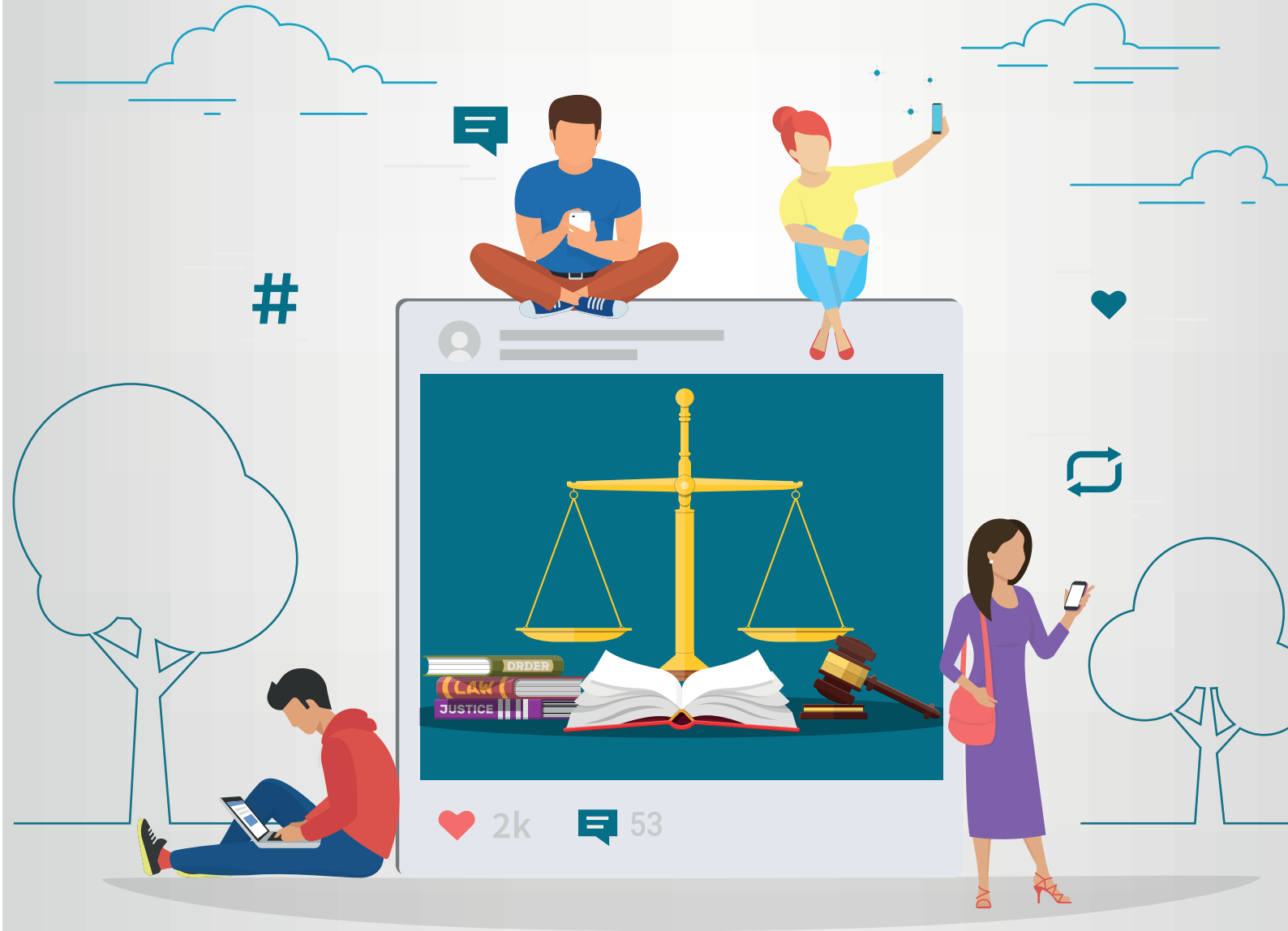
The content of the guide was developed in consultation with a focus group representing civil society organizations and media experts. We also collaborated with ICT Policy Specialist Issa Mahasneh, to provide technical information related to the Internet and social media use, focusing on Facebook and Twitter.

The Guide consists of two sections. The first presents all laws that apply directly or indirectly to online expression, whether written or visual. The second section presents technical information on social media platforms and their policies. In developing the Guide, we sought to make the laws more easily accessible, in simplified language, and to illustrate practical examples where relevant.

We would like to thank ICNL staff and partners involved in the production of this Guide, as well as the Embassy of the Kingdom of the Netherlands in Jordan for the generous support that made the Guide possible.

-1 In the past five years, countries including Tanzania, Egypt, Bulgaria, Pakistan and Vietnam have adopted laws on cybersecurity crimes.
-2 This refers to the version of proposed amendments under consideration as of April 2019.
-3 The Guide is meant to share information about the laws and does not constitute legal opinion or legal advice.

Section One: Legal Framework of Freedom of Expression over the Internet



Section One: Legal Framework of Freedom of Expression over the Internet

Overview

Freedom of expression is a fundamental human right, as declared by Article 19 on the Universal Declaration of Human Rights.[4] In Jordan, expressive activity undertaken online is governed by a number of international and national legal instruments.

I. International Framework

The applicable international framework includes international conventions and treaties to which Jordan is a party.

i. International Covenant on Civil and Political Rights (ICCPR)

The International Covenant on Civil and Political Rights (ICCPR) is a key international human rights treaty, which Jordan ratified in May 1975. It is worth noting that while the drafting of the ICCPR predates the Internet, its provisions remain valid with regard to the right to freedom of expression and other rights exercised online.[5]

The ICCPR recognizes the right to freedom of expression in Article 19:

"Everyone shall have the right to hold opinions without interference and to freedom of expression."

According to Article 19, this right includes the
"...freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."
The UN Human Rights Committee has stated that "any restrictions on the operation of websites, blogs, or any other Internet-based electronic or other such information dissemination systems" must comply with Article 19 of the ICCPR.[7]

-4 Article 19 of the Universal Declaration of Human Rights states:
"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."
-5 The former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has emphasised, for instance, that Article 19 of the UDHR as well as Article 19 of the International Covenant on Civil and Political Rights (ICCPR) were "drafted with foresight to include and to accommodate future technological developments through which individuals can exercise their right to freedom of expression." Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (May 2011), para. 21, UN Doc. # A/HRC/27/17.
-6 International Covenant on Civil and Political Rights (ICCPR), Article 19.
-7 Human Rights Committee, General Comment No. 34: Article 19: Freedoms of opinion and expression (2011), para. 43, UN Doc. # CCPR/C/GC/34.

When are restrictions on freedom of expression permissible?

A restriction on freedom of expression as guaranteed by ICCPR Article 19 is only permissible if it can satisfy a three-part test. Namely,[8] the restriction must be:

1) Provided by law, which means that the restriction is clearly stated in the law and accessible to everyone. The restriction must also be conveyed in a way that allows individuals to predict whether the expression they wish to share may or may not violate the law.
2) Serving a legitimate interest, meaning the restriction must aim to serve one of the purposes set out in Article 19 of the ICCPR, namely to protect the rights or reputations of others, or to protect national security or public order, or public health or morals.
3) Necessary, which means that the restriction must be necessary to secure a legitimate interest, and that there is a "pressing social need" to serve that interest. The restriction must also be proportionate, such that it is the least restrictive means required to achieve the purported aim.

By law, the Jordanian legislative, executive, and judicial authorities must consider its commitments to protecting freedom of expression under Article 19 of the ICCPR when drafting, implementing, and adjudicating national laws affecting expressive activity in Jordan. Any restriction on freedom of expression included in national legislation must meet the criteria for permissible restrictions described above.

-8 See, e.g. Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, para. 69, UN Doc. # A/HRC/27/17 (May 2011).

II. National Framework

A number of Jordanian laws either directly or indirectly apply to individuals' expressive activity online.

ii. The Constitution

The Jordanian Constitution of 1952 sets forth the rights and freedoms enjoyed by Jordanians, including freedom of expression. According to the Constitution:

"The State shall guarantee freedom of opinion; and every Jordanian shall freely express his opinion by speech, writing, photography and the other means of expression, provided that he does not go beyond the limits of the law." [9]

Additionally, the Constitution states that:

"Every infringement on rights and public freedoms or the inviolability of the private life of Jordanians is a crime punishable by law." [10]

According to the Constitution, freedom of expression—like other rights and freedoms—is subject to limitations set forth in Jordan's national laws. [11] However, the Constitution states that any laws issued to regulate rights and freedoms must not affect the essence and core of such rights. [12]

-9 The Constitution of the Hashemite Kingdom of Jordan (1952), Article 15.
-10 Ibid. Article 2)7).
-11 Ibid. Article 15.
-12 Ibid. Article 1)128).

iii. Cybercrimes Law

ABOUT

Cybercrimes Law No. 27 of 2015 is the primary law that directly affects the right to freedom of expression online. Article 11 of the Law, in particular, regulates aspects of expressive activity on online platforms such as Facebook, Twitter, and blogs.

(Separate Information Box - Highlighted) As of April 2019, draft amendments to the Cybercrimes Law are currently under consideration by the Jordanian Senate. The draft amendments would newly criminalize acts such as spreading rumors and disseminating hate speech. The amendments would also extend the reach of the Law to "applications," including those used on mobile phone devices such as WhatsApp.

APPLICABILITY

This Law is applicable to any individual who commits any punishable act using information systems (applications) or the Internet.

CRIMINALIZED ACTS

Individuals can be criminally liable according to the provisions of the Cybercrime Law if they: "Send or resend or disseminate information through the Internet or website or any information system that includes defamation, slander or libel against any person." [13]

PENALTIES

If an individual is found guilty of online defamation, slander, or libel against another person, he can face jail time of at least three months and a fine of up to 2,000 Jordanian Dinars. [14]
In its current form, the Law does not set a ceiling on the penalty for online defamation. This allows authorities to detain an individual during investigation for up to one week, which can be extended to one month. [15]

EXAMPLE

If someone shares a post on Facebook that claims without evidence that a public official has abused his position to gain personal benefits, the person who makes the post as well as anyone who shares it could be sentenced to three months in prison and a fine of 2,000 Jordanian Dinars based on Article 11 of the Cybercrimes Law.

-13 Cybercrimes Law, Article 11.
-14 Ibid.
-15 Code of Criminal Procedures, Article 114

iv. Penal Code

ABOUT

The Penal Code No. 16 of 1960 includes a number of offenses that can implicate online freedom of expression. Under the Penal Code, one can be convicted of defamation or libel if disseminated or published. According to the law, publication includes via electronic means such as social media and other Internet forums. [16]

APPLICABILITY

This Law is applicable to anyone, Jordanian and non-Jordanian, who commits any of the crimes defined in the Law's provisions within the territory of Jordan, as well as any Jordanian who commits such a crime abroad. [17]

CRIMINALIZED ACTS

According to the Penal Code, the following expressive acts are prohibited and subject to sanction:

- Acts, writings, or speech that would subject Jordan to dangerous acts, upset its relations with another nation, or subject Jordanians to acts of revenge. [18]
- Acts that undermine Jordan's political system, or incite opposition, or that attempt to change Jordan's economic or social systems. [19]
- Acts, writings, or speech aimed at or that results in stirring up sectarian or racial strife, or inciting divisions between the nation's different groups. [20]
- Disseminating false facts or accusations in order to weaken the status of the national currency. [21]
- Insulting individuals or institutions including the Parliament or its members, courts, public administrations, army, and public officials. [22]
- Insulting or falsely attributing statements or acts to the King, the Queen, the Crown Prince, or other individuals affiliated with the Monarchy. [23]
- Any publication or public expression intended to insult the religious beliefs of others. [24]
- Insulting a foreign head of state, a foreign nation, its army, flag, national symbol, ministers, or its political representatives in Jordan. [25]
- Publishing news, information, or criticism that may influence a judge or witness or prevent anyone from disclosing information to parties of interest during a legal trial. [26]
- Engaging in acts as part of an "unlawful association," which is any group of people that form an association contrary to the applicable laws, including writings or speech that incite or encourage overturning the Constitution through illegal means, overturning the Kingdom's government through violence or force, or sabotaging the property of the government of Jordan. [27]
- Committing blasphemy by insulting Islam, the Prophet, or the feelings of any Muslim. [28]

PENALTIES

If an individual is convicted of any of the above crimes, he may face imprisonment ranging from three months to imprisonment with temporary hard labor, which can amount to twenty years, and/or a fine ranging from twenty to 200 Jordanian Dinars. [29]

EXAMPLE

If one shares a cartoon drawing on social media depicting a prophet with an offensive statement, he can be tried and face imprisonment for three months or a fine of twenty Jordanian Dinars.

-16 Penal Code, Article 3) 73).
-17 Ibid., Articles 12 ,11 ,10 ,9 ,8 ,7 and 13.
-18 Ibid. Article 2) 118).
-19 Ibid. Article 1) 149).
-20 Ibid. Article 150.
-21 Ibid. Article 152 and 153.
-22 Ibid. Article 191.
-23 Ibid. Article 195.
24 Ibid. Article 278.
25 Ibid. Article 122
26 Ibid. Article 224
27 Ibid. Articles 161 ,159 and 163.
28 Ibid. Article 273.
29 Ibid. 273 ,224 ,195 ,191 ,163 ,161 ,160 ,153 ,152 ,150 ,149 ,122 ,118 and 278.

v. Audio-Visual Media Law

ABOUT

The Audio-Visual Media Law No. 26 of 2015 lists every visual and audio production recorded on any technical means as a production subject to the Law. Accordingly, the Law could apply to online broadcastings or productions.
The Law requires broadcasters to:
"respect human dignity, personal privacy, the freedoms and rights of others and pluralism of expression." [30]

APPLICABILITY

The Audio-Visual Media Law can be applicable to online broadcasters of any audiovisual media production, which is defined as:
"any television or radio broadcast that reaches public or targeted audience using signals, images, sounds or writings of any form, unless characterized as private correspondence, through channels, waves, transmitters, networks and other means and methods of broadcast or transmission." [31]
The Director of the Media Commission is entitled to:
• Shut down any unlicensed channel;[32]and
• Suspend the broadcasting of material or a program in cases where such material or program may hamper national security or societal peace or contain pornographic material. [33]

CRIMINALIZED ACTS

The Law prohibits broadcasting:
• Any content without obtaining a broadcasting permit according to the Law; [34]
• Materials that would violate public morals; incite hate, terrorism, or violence, or religious, sectarian, or ethnic hatred; damage the national economy or currency; or impede national or social security;[35]and
• Any false content that might harm Jordan's relations with other countries. [36]

PENALTIES

A person who broadcasts without a permit may face penalties including a fine of up to 30,000 Jordanian Dinars, which is doubled in case of continuation or repetition.

EXAMPLE

If one broadcasts a video encouraging terrorist acts through his personal website, he may be sentenced to pay a fine of 30,000 Jordanian Dinars as well as remedy the violation.

-30 Audio-Visual Media Law, Article 20 (l1-)
-31 Ibid. Article 2.
-32 Ibid. Article 8 (n).
-33 Ibid. Article 8 (o).
-34 Ibid. Article 15 (a).
-35 Ibid. Article 20 (l2-).
-36 Ibid. Article 20 (l3-).

vi. Press and Publications Law

ABOUT

Press and Publications Law No. 8 of 1998 governs everything related to press and printing, such as newspapers as well as news and media websites.
The Law includes an explicit guarantee of an individual's right to freedom of expression and speech:
"Press and printing are free and freedom of expression is guaranteed to every Jordanian, who is entitled to freely express his opinion verbally, in writing, photography, painting or any other form of expression and media." [37]
However, the Law also requires that in printing and publishing any materials, a person must be accurate, impartial, and objective. [38]
He must also refrain from including in the publication:
"Anything that conflicts with the principles of freedom, national responsibility, human rights, and values of the Arab and Islamic nation." [39]
A journalist should:
• Respect public freedoms and individuals' rights and privacy.
• Treat freedom of thought, opinion, expression, and information equally among both citizens and journalists;
• Maintain balance, objectivity, and integrity in the presentation of information;
• Refrain from publishing anything that may incite violence or call for division amongst citizens in any way;
• Adhere to the rules and principles of the journalism code of conduct issued by the Press Association. [40]
Content generated by electronic publication users, such as comments posted on news websites, must be monitored and preserved by the publication in a special record along with information provided by the user for at least six months.[41]The electronic publication has the right to approve, decline, or prevent user-generated content partially or entirely. Comments published on a website are considered media content that fall under the joint and equal liability of the electronic publication, its editor in chief, and owner. [42]

APPLICABILITY

The Law is applicable to journalists, who are members of and registered with the Press Association and practice journalism as their main profession. It also applies to publications in which ideas or words are disseminated by any means, including electronic publications.[43]
Accordingly, if you own a website that has a specific Internet address (URL) and that publishes content including news, investigations, articles, or comments then you are subject to the provisions of the Law. [44]

-37 Press and Publications Law, Article 3.
-38 Ibid. Article 5.
-39 Ibid.
-40 Ibid. Article 7.
-41 Ibid. Article 49 (e).
-42 Ibid. Article 49 (c).
-43Ibid. Article 2 (a3-).
-44 Ibid.

CRIMINALIZED ACTS

The Law states that journalists and publications should abstain from publishing anything that contains:
• Insults to religions that are protected by the Constitution; [45]
• Religious blasphemy;
• Incitement to sectarian or racial strife; and
• Content that includes defamation, slander or libel against individuals, or that affects their freedoms or includes false information or rumours about them. [46]

The Law also prohibits publications and reporters of foreign media from publishing details related to an investigation in a case before it is referred to the competent court, unless permitted by the prosecution. [47]

The Law specifically requires publications to abstain from publishing:
• Court hearings in which a gag order is issued for the purpose of protecting rights, public order, or public morals. [48]
• Comments that include inaccurate information or facts that are unrelated to the subject of the news, or that were not fact-checked, or that constitute a crime according to this Law or any other law. [49]

PENALTIES

With respect to online publications, if a publication violates the provisions of the Press and Publications Law or other laws in Jordan, the Jordanian Media Commission is authorized to block the website on which it is hosted.[50]In addition, a publication can be subject to a fine ranging from 500 to 5,000 Jordanian Dinars. [51] Additionally, any individual violator of the Law can face a fine ranging from 500 to 20,000 Jordanian Dinars. [52]

EXAMPLE

If an online journalist publishes a news story accusing a public official of corruption without fact-checking the published information, and the information is proven false, the journalist can be sentenced to pay a fine of 500 Jordanian Dinars under the Press and Publications Law, in addition to applicable penalties under the Cybercrimes Law and Penal Code.

-45 The Constitution does not explicitly stipulate a religion. Article 14 provides that: "The State shall safeguard the free exercise of all forms of worship and religious rites in accordance with the customs observed in the Kingdom, unless such is inconsistent with public order or morality."
-46 Ibid. Article 38.
-47 Ibid. Article 39 (a) and (c).
-48 Ibid. Article 39 (b).
-49 Ibid. Article 49 (d).
-50 Ibid. Article 49 (g).
-51 Ibid. Articles 45 (a) and 46 (c).
-52 Ibid. Articles 46 (d) and (e), 47 (b) and 49 (f).

vii. Press Association Law

ABOUT

Press Association Law No. 15 of 1998 regulates the affairs of its members, including online media journalists.
The Law defines a journalist as follows:
"A member of the Press Association who is listed in the practicing journalists record, and who undertakes journalism as his profession" [53]
The Law defines a media institution as:
"The natural or legal person that establishes news, broadcasting or television agency in Jordan, and that undertakes activities similar to journalism in the fields of media, and has news and editing divisions" [54]
According to the Press Association Law, Jordanian and non-Jordanian journalists must meet certain requirements to be eligible to work in journalism. The Law also prohibits press or media institutions from hiring journalists that are not registered with the Press Association. [55]
The Law affects the exercise of the right to freedom of expression online, as an individual who is not a registered journalist but who wishes to engage in the work of a journalist may not enjoy the same rights and protections stipulated in the Law for journalists. [56]

APPLICABILITY

The Law applies to practicing journalists, non-practicing journalists, journalists in training, and others who wish to practice journalism.

CRIMINALIZED ACTS

The Press Association Law prohibits:
• A press institution from hiring an individual to undertake journalistic work unless he or she is a registered, practicing member of the Press Association; [57]
• Corresponding with foreign press agencies under the false pretense of being a journalist, without having registered with the Press Association; [58]
• Practicing press work in a manner contrary to enacted laws or the journalists' Code of Ethics; [59] and
• Revealing the source of a journalist's information, or publishing information or news without confirming its veracity. [60]

PENALTIES

Journalists and journalists under training who violate provisions of the Press Association Law are subject to imprisonment from one to three months, and/or fines that vary from 500 to 2,000 Jordanian Dinars, to be duplicated in case of repetition. They may also be banned from practicing journalism. [61]

EXAMPLE

Unless duly registered with the Press Association, an individual who shares videos or press updates from a protest site with an international television channel, using communications apps on his mobile device, may be subject to a fine of 1,000 Jordanian Dinars and required to take measures to correct his action.

-53 Press Association Law, Article 2.
-54 Ibid.
-55 Ibid. Articles 9 ,6 , 5 and 16.
-56 Ibid. Article 44.
-57 Ibid. Article 16.
-58 Ibid. Article 18.
-59 Ibid. Article 42 (c)
-60 Ibid. Article 43.
-61 Ibid. Articles 18 (c), and 52 – 44.

viii. Counter-Terrorism Law

ABOUT

Counter-Terrorism Law No. 55 of 2006 lists forms of terrorism. Some prohibited acts in this Law apply to forms of expressive activity online.

APPLICABILITY

Any individual can be subject to Counter-Terrorism Law, and, if so, tried before the State Security Court, if he commits any acts of terrorism as defined therein.

CRIMINALIZED ACTS

With respect to online expression, the Counter-Terrorism Law explicitly prohibits using information systems or the Internet, or any means of publication or media, including websites, to facilitate or promote terrorist acts and ideas. The same applies to funding such actions online.[62]
According to the Law, a terrorist act is a deliberate act; an abstention of an act; or threat of an act, taken collectively or individually that could:
- Jeopardize the safety and security of society;
- Cause disorder by disturbing public order;
- Cause terror among people, intimidate them, or jeopardize their lives;
- Cause harm to the environment, or facilities, or public or private property, or facilities of international or diplomatic missions, or occupy any of them;
- Jeopardize national resources, or pose economic risk;
- Force a legitimate authority or an international or regional organization to do any work or abstain from it; or
- Disable the application of the constitution, laws, or regulations. [63]

This also includes committing any of the following acts:
- Any action that would jeopardize Jordanians or put their property at risk of hostile or revengeful acts;
- Acts that would subject the Kingdom of Jordan to hostile acts or harm its relations with a foreign country; and
- Any act that is deliberately committed with the intention of stirring insurrection against the current constitutional authority, or that prevents it from performing its constitutional duty, or amending the Constitution in illegitimate ways. [64]

All of the above-mentioned acts are prohibited under the Counter-Terrorism Law and subject to sanction, regardless of the motive—or lack thereof—underlying their execution.

PENALTIES

Acts of terrorism are penalized by imprisonment that varies from temporary hard labor, which ranges from three to twenty years, to hard labor for life, and in some cases the death penalty.[65]

EXAMPLE

If an individual shares a post on social media criticizing the strategy or tactics of Jordan's military, such as its intervention in another country, he can be prosecuted before a State Security Court and face imprisonment with temporary hard labor for at least three years.

-62 Counter-Terrorism Law, Article 3.
-63 Ibid. Article 2.
-64 Ibid. Article 3.
-65 Ibid. Article 7 (c), (d) and (e).

ix. State Security Court Law

ABOUT

The State Security Court Law No. 17 of 1959 regulates the work of the State Security Court, which has the jurisdiction to adjudicate crimes of terrorism, espionage, treason, counterfeiting, and drug offenses.

APPLICABILITY

According to the Law, anyone can be prosecuted before the State Security Court if he commits any of the prohibited acts described below.[66] In addition, any person who conspires, incites, or assists in committing; attempts to commit; attempts to induce or incite others to commit; or otherwise assists in facilitating the commission of a prohibited act or has any connection to its commission, is subject to the Law and accordingly can be prosecuted before the State Security Court. [67]

CRIMINALIZED ACTS

An individual is subject to prosecution before a State Security Court if he commits or is connected to the commission of:

- Crimes of espionage in any form, committed in violation of the Protection of State Secrets and Documents Law; and
- Crimes of terrorism, including individual or group acts aiming at changing the economic or social identity of the state or fundamental status of the society, as described in the Penal Code. [68]

This applies to expressive activity online if it is considered to fall under any of the above-mentioned categories of offenses.

EXAMPLE

One posting a video on his Facebook page criticising security forces and encouraging the public to take collective certain action against them can be tried before the State Security Court for jeopardizing the safety and security of society and disturbing public order.

-66 State Security Court Law, Article 3 (a1- and 4).
-67 Ibid. Article 4.
-68 Ibid. Article 3 (a1- and 4).

x. Contempt of Court Law

ABOUT

The Contempt of Court Law No. 9 of 1959, amongst other things, defines and prohibits acts that are deemed to impede the judicial process.

APPLICABILITY

This Law is applicable to anyone who commits acts that are considered to impede or pervert the course of justice. With respect to online expression, this includes publishing matters that:
- Influence judges assigned to a case, prosecutors, or investigators;
- Influence witnesses testifying in a case or investigation;
- Prevent individuals from disclosing information to parties of interest; or
- Influence public opinion in favour of or against a party in a court case or investigation. [69]

CRIMINALIZED ACTS

Publication in any of the following cases is prohibited by the Contempt of Court Law and subject to penalty:
- Cases where courts have decided to hold secret sessions; [70]
- Cases involving crimes of the press;[71]
- Cases of defamation, slander, libel, and revealing secrets; [72]
- Cases concerning divorce, abandonment, and custody; [73]
- Public hearings of courts, if published with dishonesty or bad faith; [74]
- Broadcasts of ongoing criminal investigations;[75]or
- Criticism of a judge or court, or commentary on a court verdict, with the intention of doubting or defaming the course of justice. [76]

However, if an individual publishes news on the subject of a case or a court verdict, he or she is not in violation to the Law unless it was published without authorization or request from the relevant party in cases where evidence of published allegations is not established. [77]

PENALTIES

The Contempt of Court Law includes criminal penalties that vary from imprisonment for six months to one year, and a fine of twenty to 100 Jordanian Dinars.

EXAMPLE

If an individual posts on his Facebook page criticising the scrutiny of the court in a certain case, and questioning the neutrality of the judicial system in Jordan, she may be sentenced to prison for three months.

-69 Contempt of Court Law, Article 11.
-70Ibid. Article 12.
-71 Ibid.
-72 Ibid.
-73 Ibid.
-74 Ibid. Article 13.
-75 Ibid. Article 14.
-76 Ibid. Article 15.
-77 Ibid. Article 12.

xi. Telecommunication Law

ABOUT

While the Telecommunications Law No. 13 of 1995 focuses largely on the technical aspects of telecommunications, a few provisions implicate online expression.

APPLICABILITY

The Law applies to users and beneficiaries of public telecommunications services, such as Internet services. [78]

CRIMINALIZED ACTS

The Telecommunications Law prohibits the following:
• Using telecommunications services to direct threatening or insulting messages, or messages contrary to public morals; or
• Disseminating false news with the intent to spread panic. [79]
The authorities may order the blocking or denial of a user's access to telecommunication services if he:
"utilizes the services in a way that violates Jordanian legislation or public morals." [80]

PENALTIES

If a person commits any of the prohibited acts described in the Law, he or she may face imprisonment for at least a month and up to one year, or a fine ranging from 300 to 2,000 Jordanian Dinars, or both. [81]

EXAMPLE

If an individual sends threatening messages to another using a chat application, he may be prosecuted based on provisions of the Telecommunications Law, and consequently face either having his access to telecommunication services blocked, and/or being imprisoned for one month and/or paying a fine of 300 Jordanian Dinars.

-78 Telecommunications Law, Article 2.
-79 Ibid. Article 75 (a).
-80 Ibid. Article 58 (a).
-81 Ibid. Article 75 (a).

xii. Law on Access to Information

ABOUT

The Law on Access to Information No. 47 of 2007 regulates applications submitted to government agencies by Jordanians requesting information.
The Law grants every Jordanian the right to
"obtain information provided that she has a legitimate reason or a lawful interest in the information." [82]
According to the Law, public officials are obligated to facilitate access to the requested information without delay.[83]A decision on the request of information should be made within thirty days.[84]Denial should be justified, and along with unanswered requests within the timeframe, may be appealed before an administrative court.[85]
Requests that the government may legitimately refuse are those of discriminatory nature in relation to religion, race, ethnicity, sex or color. [86]
Public officials are authorized to refrain from disclosing certain information, such as:
• Secrets and documents protected under other laws;
• Secrets related to national defense, state security, or foreign policy;
• Information that would harm negotiations between Jordan and another nation if disclosed; and
• An individual's educational or medical files. [87]

APPLICABILITY

The Access to Information Law regulates a right for all Jordanians. The Law's provisions and government's implementation of the Law indirectly affect expressive activity online, as the absence of data and information has an impact on individuals' ability to be accurate in their communications, and may therefore expose them to greater liability under other laws described above.

CRIMINALIZED ACTS

There are no criminalized acts according to Access to Information Law, but one could be prosecuted under a number of the laws described in this Guide as a result of the government's refusal to disclose. For instance, an individual could be criminally liable for sharing information without evidence, even if the individual had attempted to request and obtain that evidence from the government and had been refused.

EXAMPLE

An online journalist who publishes an investigative piece, after officials refused to disclose information on a candidate's educational file, challenging a validity of the candidate's nomination for public office, could face imprisonment for three months and have to pay a fine of 2,000 Jordanian Dinars based provisions of the Cybercrimes Law.

-82 Access to Information Law, Article 7.
-83 Ibid. Article 8.
-84 Ibid. Article 9 (c).
-85 Ibid. Article 9 (d) and 17.
-86 Ibid. Article 10.
-87 Ibid. Article 13 (a, c, e and g).

xiii. Protection of State Secrets and Documents Law

ABOUT

The Protection of State Secrets & Documents Law No. 50 of 1971 allows officials to categorize information as state secrets, and imposes strict penalties on those who disclose such information.
The Law categorizes such documents into four types, according to the type of information they contain:
• Top secret: including but not limited to important political documents related to international relations;[88]
• Secret: including but not limited to information that could cause a threat to national security or harm its interests, or could be of a major benefit to a foreign state or any other entity; [89]
• Confidential: including but not limited to information that would demoralize citizens unless disclosure is authorised, and protected information that would harm the reputation of a public official or would impair the prestige of the state;[90]and
• Clearance: such information should only be disclosed to parties of interest, except in cases in which disclosure is endorsed.[91]

APPLICABILITY

This Law is applicable to officials with access to official and state documents, and individuals who may have access to such documents through legal or illegal means. Former public officials who once had access to such documents and information but who are no longer serving their official roles should not disclose such information or secrets. [92]

CRIMINALIZED ACTS

The Protection of State Secrets and Documents Law prohibits leaking classified documents except when necessary.[93] However, the Law does not identify cases of necessity.

PENALTIES

Penalties vary under this Law. A person violating its provisions can be subject to criminal penalties that range from ten to twenty years of temporary hard labor, and in some cases, he can be subject to the death penalty. [94]

EXAMPLE

If a journalist obtains access to classified information, and leaks the information through her Twitter account without establishing that the leak was necessary, she may face imprisonment with temporary hard labour for at least ten years.

-88 Protection of State Secrets & Documents Law, Article 3.
-89 Ibid. Article 6.
-90 Ibid. Article 8.
-91 Ibid. Article 10.
-92 Ibid. Article 12.
-93 Ibid. Articles 13 and 16.
-94 Ibid. Article 16.

xiv. Public Assemblies Law

ABOUT

Public Assemblies Law No. 7 of 2004 regulates public meetings, assemblies and protests. The Law has been followed by a set of regulations and instructions in 2011, granting governors wide authority to control assemblies. The Law impacts online freedom of expression as it affects the ability of individuals to call online for public gatherings such as protests.
According to the Law, an individual is required to "submit a notification to the administrative governor at least 48 hours prior to an event."[95] However, in recent years, implementation of the Public Assembly Law has not been consistent with its provisions. For example, the government has required that individuals not only notify but obtain approval before holding events; in some cases it has cancelled organizations' events at the last minute despite of being duly notified according to the Law. Moreover, governors have asked organizations to provide detailed information about planned events, such as the names of participants, speakers, and agenda, and have required the organizers to disinvite certain participants and change certain content, or face cancellation of the event.

APPLICABILITY

The Public Assemblies Law applies to Jordanians as well as non-Jordanians, who are prohibited from holding public assemblies in Jordan per the Law's provisions. [96]

CRIMINALIZED ACTS

Any public assembly or rally organized contrary to the provisions of the Public Assembly Law and its instructions is considered illegal. [97]
An organizer of an assembly should not initiate any invitation or announcement before submitting a notification to the governor, forty-eight hours in advance of the assembly. [98]

PENALTIES

Violations of the Public Assemblies Law are punishable by criminal penalties ranging from imprisonment for one to three months, and/or a fine of 200 to 1,000 Jordanian Dinars. [99]

EXAMPLE

A person calling for a demonstration through social media, to protest a proposed law, may be held liable for violating the Public Assembly Law and consequently subject to imprisonment for a month or a fine of 200 Jordanian Dinars, or both, based on Article 10.

-95 Public Assemblies Law, Article 4.
-96 Ibid. Article 3 (a).
-97 Ibid. Article 5.
-98 Ibid. Article 4. Also refer to Article 2 (b) of the Instructions of 2011.
-99 Public Assemblies Law, Article 10.

xv. Law on Prevention of Crimes

ABOUT

The Law on Prevention of Crimes No.7 of 1954 grants governors wide discretionary powers to detain individuals based on suspicion that they might commit a crime. [100]

APPLICABILITY

The provisions of the Law on Prevention of Crimes can be used to prosecute individuals who practice their right to freedom of expression online, as potential violators of other laws.
The governor has the authority to determine whether an individual poses or might pose a threat. To verify the latter, the governor has the power to subpoena the individual and make him sign a declaration, pledging to maintain good conduct during a period that the governor determines.[101] The governor can also issue an arrest warrant in case the individual does not respond to the subpoena within a reasonable time. The detained individual should be tried before the competent court within a week of his arrest. [102]

CRIMINALIZED ACTS

The broad discretion granted to governors according to Law on Prevention of Crimes allows them to prevent possible violations or crimes committed online as described in any of laws described above.

PENALTIES

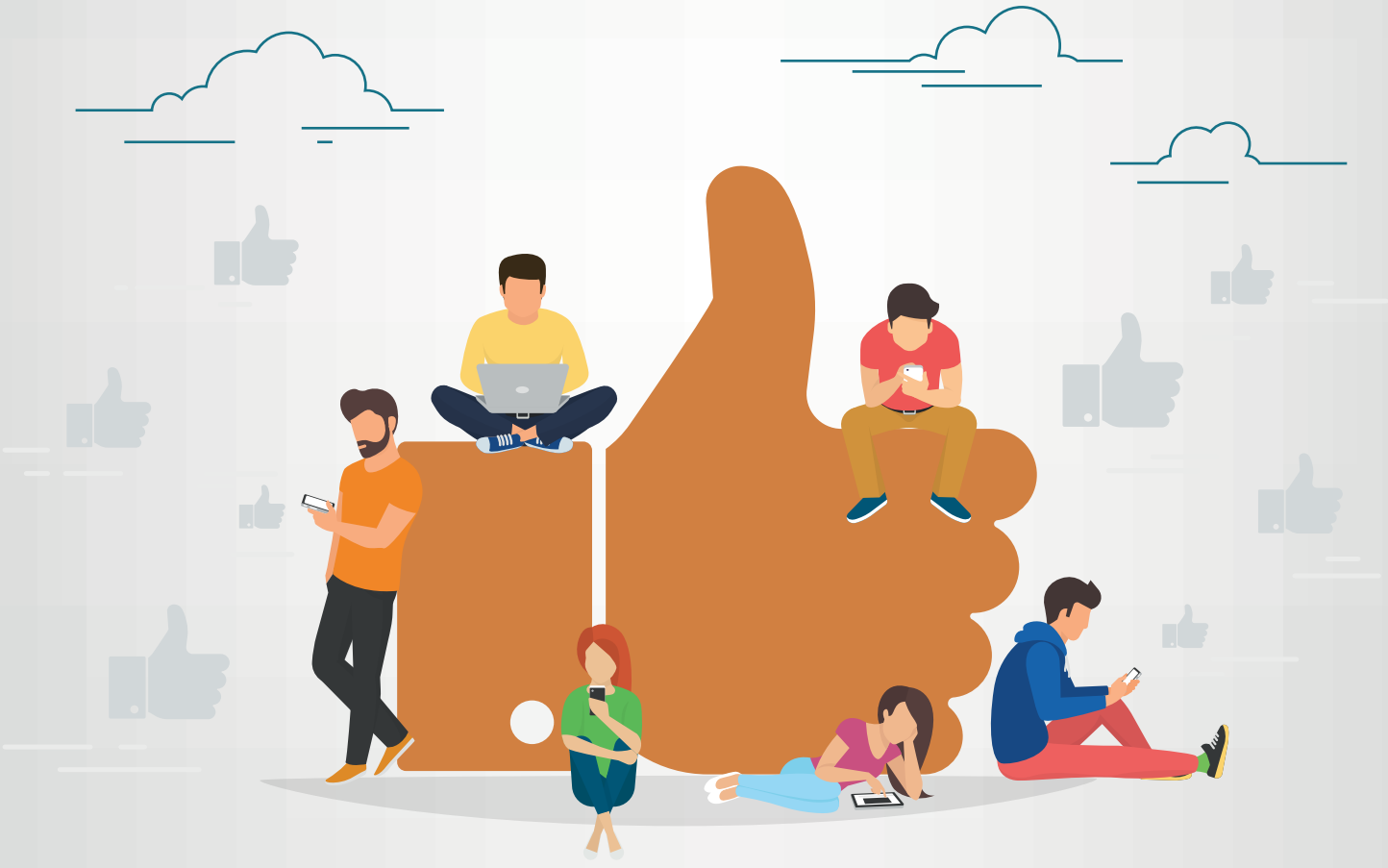
Suspected individuals must abide by several instructions, including but not limited to committing to house detention unless otherwise approved the governor, and allowing inspection visits from security forces.[103]If the individual violates the conditions determined in the surveillance order issued against them, they can also be subject to penalties including imprisonment for up to six months and/or a fine of fifty Jordanian Dinars. [104]

EXAMPLE

A governor can detain an individual that authorities suspect may commit a crime, in order to prevent him from Tweeting and sharing information that could be deemed contrary to public order, per applicable laws.

-100 Law on Prevention of Crimes, Article 3.
-101 Ibid. Article 3.
-102 Ibid. Article 4.
-103 Ibid. Articles 8 ,4 ,3 and 13.
-104 Ibid. Article 14.

Section Two
Social Media



Section Two: Social Media

During recent years, internet and social media platforms has become fundamental for exercising freedom of expression. Consequently, as a constantly developing means of communication amongst people all over the world, with each passing day, the internet and social media platforms are subjected to rules, regulations and laws, which are adopted on the national level by different countries. Not only that, social media platforms, run by private entities, include their own limitations on online freedom of expression based on policies, rules and regulations such entities have developed.

While the first section of this Guide focused on the legal framework governing online freedom of expression in Jordan, this section will provide guidance for internet and, more specifically, social media users. It will cover platform-specific policies and practical tips to know what to expect while specifically using Facebook and Twitter and how to deal with technical difficulties users may face. The section starts with an introductory part covering the history and governance of the Internet, and then moves to the current issues of social media in providing technical tips on privacy over social media, publicity of shared content, hate speech, and finally the protection of social media accounts.

I. The Internet

i. History of Internet Governance

If you want to understand how the Internet is managed today, it is necessary to understand a little of its history. The Internet was first created to allow researchers to collaborate remotely worldwide, and it was not opened to commercial entities until the 90s.
It was not until the World Summit on the Information Society (WSIS) in 2003 that the topic of how the Internet should be governed was first raised at a global level, not only technically, but legally, socially and politically. Governments around the world started to see the Internet, once created with few technical rules, as a medium that should be regulated and its governance to be discussed.

Freedom of expression and freedom of information have been long recognized as pillars of “Internet governance”, they were included in the 2003 Geneva Declaration and 2005 Tunis Commitment of the World Summit on the Information Society (WSIS). Based on the decentralized nature of the Internet and being an extra-national and cross-border network, global cooperation between governments, civil society, private sector and technical community and a shared respect for human rights are requirements to enable an environment for media freedom in the digital age.

Timeline of the Internet	
1969	ARPANET was founded by the US Department of Defence, considered to be the first backbone of the Internet.
1984	The U.S. National Science Foundation (NSF) created NSFNET, a general-purpose research network.
1989	160,000 hosts in more than 9 countries were connected through the Internet.
1995	Restrictions on the commercial use of the Internet were terminated.
2003	The World Summit on the Information Society (WSIS) was held in Geneva.

ii. The Internet in Jordan

The first commercial Internet service was initiated in Jordan in 1996. For several years, access to the Internet remained open and free of any restrictions. In 2001, the Ministry of Interior issued new regulations for Cybercafés, enforcing filtering of content and keeping personal information of users. A year later, the first website was blocked in Jordan. It was not until 2010 that a legal framework to regulate online content started to form, first by the issuance of a temporary cybercrime law and then by the order of the highest appeal court, which later resulted in defining and including news websites as publications in the amended Press and Publications Law in 2012.

There are several stakeholders and actors that directly influence how the Internet is governed in Jordan, and, ultimately, have an impact on your use of the Internet and how online content is regulated.

Main Actors	
Telecommunication Regulatory Commission (TRC)	The TRC is an independent jurisdictional body that regulates the telecommunications and information technology sectors in Jordan according to the Telecommunications Law No. 13 of 1995. Why is it relevant to you? · The TRC is the entity that receives complaints from users in the case an issue with your telecom company is not resolved. · It is also the sole entity that regulates the operations of telecom companies, accordingly, all ban orders of online content are, ultimately, sent through the TRC to telecom companies.
National Information Technology Center (NITC)	The NITC is an independent government organization, which supports IT operations of the government and other public bodies. The NITC was established in accordance to Deployment of Information Technology Resources in Government Organization Law No. 81 of 2003. Why is it relevant to you? · If your website address (URL) ends with .jo, or you are willing to obtain one, the NITC is the entity that puts the regulations on the acquisition, use and termination of such address. · If you are using the Internet through a public body (like at one of the 'Knowledge Stations', government-run institutions that provide Internet to local communities), Internet service is provided by the NITC, which might apply specific filtering rules to block users from accessing content online.
The Media Commission (MC)	The MC is an independent government entity that regulates the audio-visual media. Based on the Press and Publications Law amendments in 2012, the MC administers the licensing of news websites. Why is it relevant to you? · If you want to run a website that provides news or reports about Jordan, you should obtain a license from the MC. · If you own any website that is not licensed, the MC will issue an order to block it in the case it breaches the law.
Anti-Cybercrime Unit	The Anti-Cybercrime Unit was established in 2008 under the Criminal Investigation Department of the Public Security Directorate. The unit's main duty is to investigate crimes committed through, or by, technological means. These comprise a wide range of acts that are considered illegal based on the Jordanian laws, from online abuse of children to electronic recruitment for terrorist organisations and hate speech. Why is it relevant to you? · If you are a victim of a cybercrime you should file a report with the Anti-Cybercrime Unit, the prosecutor's office will see what charges, if any, can be pursued.

II. Social Media

Information, ideas and messages were transmitted through the Internet since its early beginnings. Throughout the years, online behaviour evolved into more social and expressive forms, in the 90s and early 2000s via forums and blogs, and then by the appearance of online communities where social interactions were key, marking the start of social media as we know it. In 2004, Facebook was introduced, followed by Twitter in 2006.

Social media differ from 'traditional media' in a multitude of ways and not only by their means of transmission (digital/offline); while a newspaper or a blog is written by one entity and read by many, one distinguished characteristic of social media, is that they are platforms that allow many sources to reach many receivers.
The content on social media, including posts, comments, photos and videos, are user-generated and mixed with online interactions, for instance, what users like and the relationships between multiple users. The result is a 'social network' where ideas, expressions and actions of users are interconnected with others.

i. Facebook vs. Twitter

Facebook and Twitter are two social networks, founded in 2004 and 2006, respectively. They are both managed by U.S-based companies but accessible worldwide through any device with Internet access, such as personal computers and smartphones.
The major differences, including the platform-specific terminology, between Facebook and Twitter are shown in the table below:

Main Differences between Facebook and Twitter		
	Facebook	Twitter
Main method of publishing content	Users publish 'Posts', which may include: · Content in multiple forms, such text, photos, videos; and · Links to external content, such as websites, videos and photos published on another platform	Users publish 'Tweets', which may include: · Textual content, that is limited to 280 characters, in which photos and video can be added; and · Links to external content, such as websites, videos and photos published on another platform
Distribution of published content	Published posts formalize into a chain, called 'news feed'. Depending on the chosen privacy of the post by the user, it is visible to other authorized users upon registration	Published tweet formalize into a personalized list, visible for authorized users after registration. 'Public' tweets are shown to users even without registration
Interaction with published content	Users can 'like' posts. Posts are re-sharable. A user can share a post through clicking on the "share" button	Users can 'like' tweets. Tweets are retweet-able. A user can share a tweet through clicking on the "retweet" button
Relationship between users	A user can connect with other users by adding them as 'friends'. Friendship on Facebook is mutual, meaning that both users should accept this relationship in order for them to be on each other's friends list.	By default, a user can 'follow' other users in order to see their tweets, for this to happen, it does not require the followed user to 'follow back' the person requesting to follow him.
Private messaging	A user can send messages to other users through a Facebook platform called Messenger. Messages sent by those who are not on a user's list of 'friends' are separately received as 'message requests'.	A user can send a 'Direct Message' (abbreviated as DM) to other users. By default, the two users should 'follow' each other to be able to exchange direct messages.
Interaction between a group of users	Users can interact with each other in separate platforms from the news feed called 'groups'. Groups can be public, accessible and visible to all Facebook users, or private, only accessible and visible to its members.	A user can create a list of multiple users, to see their 'tweets' collectively.

ii. Current Issues

It would be difficult to limit our perspective of social media as merely Internet sites. They eventually became the main source of news as well as a democratic and accessible public space for socio-political change and free speech.

As the impact of social network is massive, individuals, organizations and states started using, and sometimes manipulate, online content to obtain economic or political gains, even by sharing false information (false news) online or by utilizing newer technologies like Artificial Intelligence (AI) and Big Data to affect freedom of expression online.

1) Fake News

Just like any public platform, social media can be an outlet for absurd actions and abuse such as populating fake news or false information. This can be done by publishers or spammers based on financial motivations, or by political entities for propagandistic reasons. How to stop such actions, especially fake news, is an open question, that has no one answer. However, some states adopted various mechanisms, such as adopting effective access to information laws that provide access to information and data that are necessary for informing the public, others provide support to digital media literacy and utilize techniques for explaining the flawed argumentation used in misinformation. Some of these state actions are highlighted in the table below.

Case studies of state actions to combat 'fake news'	
Germany	Germany adopted the Network Enforcement Act (NetzDG)[1] in September 2017. The law tackles what is considered 'fake news' according to the Criminal Code and requires social networks to maintain a procedure for handling complaints about unlawful content. Social networks are required to remove or block unlawful content within 24 hours of receiving a complaint, and in case of conviction, a fine can reach 5 million euros.
European Union	The European Commission issued a Code of Practice on Disinformation, to be signed by online platforms on voluntary basis, aiming to establish self-regulatory standards to fight disinformation. The code of practice covers five main areas[2]: 1. Disrupting advertising revenues of accounts and websites that spread disinformation 2. Making political advertising and issue based advertising more transparent 3. Addressing the issue of fake accounts and bots 4. Empowering consumers to report disinformation and access different news sources, while improving the visibility and findability of authoritative content 5. Empowering the research community to monitor online disinformation through privacy-compliant access to the platforms› data
France	In 2018, the French National Assembly approved the 'Law Against the Manipulation of Information'. Particular attention is given within this law to 'fake news' during election campaigns. The law stipulates several measures and obligations, including[3]: 1. Transparency obligation for digital platforms, which must report any sponsored content by publishing the name of the author and the amount paid 2. The creation of a legal injunction to halt the circulation of 'fake news'. A judge will determine what is 'fake news' according to three criteria; fake news must be manifest, must be disseminated deliberately on a massive scale, and must lead to a disturbance of the peace or compromise the outcome of an election. However, between elections, the law also establishes a 'duty of cooperation' for social networks and media platforms to force them to introduce measures to combat 'fake news'. Checking for compliance with this duty has been entrusted to the CSA (French Broadcasting Authority).
United Kingdom	The British Parliament set up a Board of Inquiry that issued a number of recommendations in regards to disinformation and fake news[4], including: 1. Compulsory Code of Ethics for tech companies overseen by an independent regulator that has powers to launch legal action against companies breaching code. 2. Social media companies obliged to take down known sources of harmful content, including proven sources of disinformation.

-1 [German] Federal Ministry of Justice and Consumer Protection, "Network Enforcement Act - NetzDG", in German, available at: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html
-2 [European Commission] Digital Single Market, "Code of Practice on Disinformation", available at: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation
-3 Gouvernement.fr, "Combating the manipulation of information", available at: https://www.gouvernement.fr/en/combating-the-manipulation-of-information
-4 UK Parliament, "Disinformation and 'fake news': Final Report published", available at: https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-report-published19-17-

On the technical level, different social media platforms are experimenting new features to alleviate these issues, like cooperating with fact-checking organizations to show their findings, providing users with more information about the media outlet whose article has been posted, or by allowing users to mark stories as inaccurate.
While social media platforms might remove accounts and content that violate their policies, many social media companies believe that governments, except in narrowly defined circumstances based on internationally recognized standards, should not restrict the right to freedom of expression. For example, some of the major IT companies including Facebook, Microsoft and Google, have agreed to

"Respect and work to protect the freedom of expression rights of users when confronted with government demands, laws and regulations to suppress freedom of expression, remove content or otherwise limit access to communications, ideas and information in a manner inconsistent with internationally recognized laws and standards" [5]

2) Artificial Intelligence and 'Big Data'

As the size of discussions and information shared online has increased dramatically, new technologies were created to better handle, utilize and benefit from this huge mass of information. These technologies could be applied in different ways, mainly by utilizing Artificial Intelligence (AI), i.e. the ability of a computer program or a machine to think and learn, which is currently employed to discover inauthentic content like fake news or spam. There is also a feeling between activists and civil society organizations, that the same technologies could be used against free speech, for example, to automatically report content or users without human judgement or reasonable decisions.
Entities could also collect data of users, their published content, online relationships and activities. These huge amounts of data, also known as 'big data', are analysed by using sophisticated computer tools, valuable information could be obtained and utilized for economic and political reasons. In fact, states and political entities are making use of these data to scan users' comments and posts in order to monitor public opinion or to promote a specific political agenda. Some of these entities could deploy methods that are not always seen as ethical, like targeting genuine free speech by utilizing bots (software that appear as humans) to share counter-debates, or to fuel online harassment against activists and human rights defenders.

iii. Privacy

While in the physical world individuals expect to have their physical spaces, like their homes, and their personal life be protected, in the Internet, privacy concerns with respect to their personal information persist. Additionally, information on the Internet could be permanent or remain available for long periods of time, and they can be retrieved and shared by other Internet users.
Your personal information can be collected by a myriad of entities for different uses.

-5 Global Network Initiative, "The GNI Principles", available at: https://globalnetworkinitiative.org/gni-principles

Entities could use this information for 'social profiling'; creating a profile of you based on your data and online behaviour, to better target you in advertisement. Other information about your personal life could be inferred from that, including your health status, sexual behaviour and political and religious views.
Malicious actors can invade your privacy, for example, by taking your picture without your consent and releasing it on social media, or by threatening to release private communications or private videos and photos of you. In such case, there are different potential online and offline solutions that you can resort to in order to solve stop and eventually remove the violation. For more information on how to resolve privacy violation issues, check Box No. 3 herein.

The main difference between Twitter and Facebook in terms of privacy is that Twitter is by default public, except when choose to have a private account, and Tweets can be seen immediately by anyone around the world, while Facebook, being a social media platform that promotes real interactions with your 'friends', allows more options for the user to select what could be seen by others.
Facebook does not allow users with fake or anonymous identities, while on Twitter, you can create and operate an account without exposing your real identity.

1 - Do: Check privacy settings on Social Media

Both Facebook and Twitter have privacy policies that specify how they handle your private information, for example, they collect information about the devices you use, your IP address (a unique address that identifies your device on the Internet), and other additional information you share with them, like phone number or location. These information are used for marketing or to populate relevant content. To know more about how Facebook and Twitter collect, process and use your data, you can refer to these links:
Facebook: https://facebook.com/about/privacy
Twitter: https://twitter.com/en/privacy

Both Facebook and Twitter give you control through your settings to limit the data they collect from you and how they use it.

On Facebook, you can select how people find and contact you, whether to allow Facebook to be able to recognize you in photos and videos (face recognition), if others can share your stories as well to other settings related to your timeline, tags and their approval before they got published.
You can change these settings on: https://www.facebook.com/settings?tab=privacy

On Twitter, you can select whether to share your location with the tweets you post, or whether others can find you using your phone number or email or whether, you get personalized content, through which Twitter presents you with more relevant Tweets, suggestions about who you might enjoy following, and better ads based on your online activity, or by allowing Twitter to use certain information, like your current location, to help show you more relevant content.
You can change these settings on: https://twitter.com/settings/safety

2 - Do: Understand visibility of content

When you post something on Facebook, you can choose who will able to see it, i.e. the 'audience' of your post. You can change the audience before posting or update previous posts' audience as well.

Public: Everyone on the Internet can see your post.
Friends: Only persons on your list of friends will be able to see.
Custom: You can select specific persons (or lists of persons) that can see (or not see) your post.

You can change who can see your future posts from here: https://web.facebook.com/settings?tab=privacy&section=composer

On Twitter, you can select whether to publish your tweets to the public, or to 'protect' them, making them available only to users you select. However, the tweets you posted previously may stay publicly visible.
You can protect your tweets on this page: https://twitter.com/settings/safety

3 - Do: What to do in case your privacy has been violated?

Definitions of private information may vary depending on local laws, social media platform comply with these laws based on where you reside. Jordan has not yet adopted a specific definition of privacy, or privacy and personal data protection law.

1. If you think a photo or video violates your privacy, and you want to request its removal, you can fill a removal request at:

Facebook: https://facebook.com/help/contact/144059062408922
You will be asked to specify the photo or video, its link or to describe where it can be found.

Twitter: https://help.twitter.com/forms/private_information
You can use the form provided by Twitter to request the removal of other personal information that are shared without your consent, like contact information, financial account information or ID card information.

2. If someone is threatening to share your private and intimate photos, videos or messages on Facebook, you can:
a. Contact the Anti-Cybercrime Unit at the Public Security Directorate.
b. Report the person to Facebook, by filling the form at: https://facebook.com/help/contact/567360146613371
c. Block the person on Facebook. A blocked person can no longer start conversations with you or see things you post on your profile.

iv. Hate Speech

As described earlier, social media brought many opportunities by providing an open space in which people can express their views freely, but opened the door for additional challenges, including how to protect the people most at risk from online attacks. The nature of social media, characterized by the enormous penetration and the control of users on the selection of information they send and receive, made balancing between freedom of expression and protecting human dignity even more complex.

Article 2)20) of the International Covenant of Civic and Political Rights (ICCPR) enforces State Parties to prohibit "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence", however, the use of the term hate speech could be seen as vague and widely contested. Therefore, international best practices have set criteria on how to prevent hate speech without restricting civic space.

Social media platforms have proposed their own definitions –and policies– to tackle the issue. Generally, these definitions incorporate references to direct attacks against protected categories of people, based on specific attributes. For example, Facebook defines hate speech as:

"A direct attack on people based on what we call protected characteristics — race, ethnicity, national origin, religious affiliation, sexual orientation, caste, sex, gender, gender identity, and serious disease or disability. We also provide some protections for immigration status".

While Twitter defines hateful conduct as:

"[Promotion of] violence against or directly attack or threaten other people on the basis of race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease".

The definitions of attack or violence themselves may vary from a platform to another, and could be tackled differently when some content is moderated. The box shows which online activity Facebook and Twitter consider as hate speech, violence and attacks. .

What are attacks and violence according to Facebook and Twitter?

Facebook

Facebook divides hate speech into 3 different tiers, from the most severe to the least, and defines 'attack' distinctly on each tier:

- Tier 1: Any violent speech or promotion thereto in written or visual form, in addition to dehumanizing speech, such as reference or comparison to insects and other animals perceived as inferior, filth, disease or violent criminals.

- Tier 2: Statements of inferiority or an image implying a person›s or a group›s physical, mental, or moral deficiency, or expressions of contempt or disgust or their visual equivalent.
These include wordings like 'ugly' or 'undeveloped' (physical deficiency), "stupid" or "idiot" (mental deficiency), "fraud" or "cheap" (moral deficiency), or expressions like "I hate" or "I don't like" (contempt) and "gross" or "disgusting" (disgust).

- Tier 3: Calls to exclude or segregate a person or group of people.

In all tiers, to be identified as hate speech, the attacks should target people based on the previously mentioned protected characteristics. Tier 1 takes into account immigration status as well.

Twitter

A set of online behaviour could constitute hateful conduct, representing either violence or attacks to people:
- Violent threats: declarative statements of intent to inflict injuries that would result in serious and lasting bodily harm.
- Wishing, hoping or calling for serious harm on a person or group of people.
- References to mass murder, violent events, or specific means of violence where protected groups have been the primary targets or victims.
- Inciting fear about a protected category, based on race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease.
- Repeated and/or non-consensual slurs, epithets, racist and sexist tropes, or other content that degrades someone.
- Hateful imagery.

Both Facebook and Twitter confirm they remove hateful content, however they are both criticized for the inconsistency in enforcing their policies, and for the protected categories of people in their definitions, which some see controversial or not inclusive. In all the cases, take into consideration that what you can see as a hateful statement might not actually represent a violation of the rules and policies of a social media platform, and might not be eventually removed. The following table presents the practice of removing content considered as hate speech by social networks.

Hate Speech Removal in Practice: Facebook and Twitter	
Facebook	Facebook removed a massive quantity of content categorized as 'hate speech' during the first quarter of 2018 alone; Facebook removed 2.5 million pieces [6] , either reported by users or detected through utilized technologies developed by the company. Real-life examples include: • In 2019, Facebook removed the account of the British journalist and activist, Tommy Robinson, after he posted material that included dehumanizing language and called for violence targeting Muslims. •In 2019, Facebook banned several Myanmar pages that included incendiary posts aimed against the country's Rohingya Muslims. •In 2015, Facebook started to automatically ban posts with the word 'moskal', a slang term seen offensive to Russians. •In 2018, Facebook temporarily banned the account of the Israeli prime minister's son after posting a series of anti-Muslim and anti-Palestinian posts.
Twitter	Twitter may suspend accounts, temporarily or permanently, if tweets include content that can be considered 'hateful'. However, Twitter does not inform users who are permanently suspended of the tweet behind the decision, or of the company's rules which were violated. Real-life examples include: • In 2016, a rapper's account was suspended after making racist and homophobic posts towards a singer, while in 2017, the account of a blogger was suspended after the use of homophobic language regarding a Teen Vogue›s article. •In 2016, the account of an American social media personality was suspended after publishing neo-Nazi tweets, including a photo of herself rendering a Nazi salute at a white nationalist event. •In 2018, the account of a religious figure was suspended after the use of a term of considered pejorative and racist towards black people. · In 2018, the account of a far-right political activist was suspended after violating «rules against hateful conduct» in a tweet targeting a Somali-American congresswoman.

-6 Facebook Newsroom, "Facebook Publishes Enforcement Numbers for the First Time", available at: https://newsroom.fb.com/news/05/2018/enforcement-numbers

Do: Check the rules.

Platforms define hate speech in different ways in their terms of use and policies, accordingly, they might take different enforcement actions on the user's account or their content. You are encouraged to have a look at these policies, as they represent the main guidelines on when these platforms can remove your online content.

On Facebook, you can read the Community Standards, a set of rules that outline what is and is not allowed on Facebook, at: https://facebook.com/communitystandards
On Twitter, you can access the rules and policies at: https://help.twitter.com/en/rules-and-policies

What to do in case you see violations or content that you do not like?

On different platforms, you can hide content that you do not like, or report content that constitutes violation of the rules and policies.
When reporting content, please keep in mind that:

- Reporting something does not guarantee that it will be removed.
- Reporting is confidential; your personal information are not shared with the person who published the reported content.

Facebook

- For posts and photos, the easiest way to report, is by clicking the down arrow (√) next to the post itself, then select Report post or Report photo.

- For photos and videos, click them and put your mouse's cursor on the content, once the Options link is visible in the bottom part, click it and select Give feedback on this photo or Give feedback on this video.

After that, in all cases, you have to select the option that best describes the issue and follow the instructions.

Twitter

For tweets, the easiest way to report, is by clicking the down arrow (√) next to the tweet itself, then select Report. You will be asked to select one of the options that better describe the violation, in case you select "It directs hate against a protected category (e.g., race, religion, gender, orientation, disability)" you will be asked to select if it targets you, an individual or a group, you might be asked to select some tweets from the user, in order to provide context.

v. Trust and Protection

When people interact on the Internet they want to feel safe; a trusted environment is crucial to allow people to express their views and opinions, but, like any other human community, social media is only as accurate as the people using it and encompasses actions that can undermine yours and others' ability to express freely.

To Trust or not to Trust?

No one appreciates interacting with imposters at work, class, and other spaces. The same applies to your virtual ones, not all the profiles on social media are real ones, fake profiles are profiles that do not impersonate their owners.

Specifically on Twitter, not all the tweets you see are written by humans! Recently, technologies that emulates human language are utilized to create profiles that can automatically publish content, colloquially knowns as 'bots'. These computer applications can write content, share other posts and even interact with you. The level of sophistication of such applications may vary, but their power in assimilating normal human behaviour should not be underestimated. Additionally, some of these bots run with the actual help and input of real people making them even more realistic.

Remember that when you post anything online, or take part in any social media conversations, you might deal with all the aforementioned phenomena, understanding existence of bots, and decide your actions accordingly could definitely help you in having a more pleasant social media experience.

Do: Check security settings

Facebook

Facebook provides extra security settings for your account, you can:

- Receive alerts about logins on your account by devices or web browsers Facebook does not recognize.
- Set up two-factor authentication, which allows to use another security code in addition to your password. It is a wise decision to use an Authentication Application, like Google Authenticator, rather than SMS for this feature; SMS are not encrypted and can be potentially read by anyone trying to unlawfully access your account.
- Choose friends to be your 'trusted contacts', this will be useful in case you are unable to access your Facebook account anymore. 'Trusted contacts' will be able to send you a recovery code with a special link you can click to access your account again.

You can access and enable these options at: https://web.facebook.com/settings?tab=security

Twitter

On Twitter you can enable 'login verification' (i.e. two-factor authentication) in a manner similar to Facebook, this option is available at your account's settings: https://twitter.com/settings/account

What to do in case your account got hacked?

Your account could have been hacked if you notice changes you have not committed yourself. If your contact information, like email address or telephone number, or other account information changed, or if your account send requests or messages to people you do not know, or published content you have not created, there is a possibility your account is hacked.

Facebook

Facebook provides a step-by-step process to recover hacked accounts, and can also automatically scan any recent changes to your account. Facebook will require from you to change your current password, and would allow removing any friends or posts that have been added recently from your account.
Visit: https://facebook.com/hacked

Twitter

Twitter provides a password reset form, that will send a temporary password to the email address linked to your account, you can access it from here: https://help.twitter.com/forms/signin
In the unfortunate case you have no access to your email, but you are still logged in on your Twitter app on a mobile device, you can update your email address from your app settings, if that is not possible, you can contact your email service provider to try and regain access.

What to do in case you have been mistakenly/ falsely reported?

In case your account is reported, social media platforms might take different actions based on reports. Your account features could be temporarily limited or your account could be disabled or suspended.
Facebook may limit you to send messages or friend requests if you posted or shared content that seems suspicious or abusive, in that case, these features should be restored after a few days. However, in the case you have done something that does not follow Facebook's Community Standards, the block of your account features can last up to 30 days.
Twitter may limit some of the account features for a limited period of time, if that happens, you will receive a message when you log in. Click or tap Continue to Twitter to initiate the countdown to restore your account features.

In the case your account on Facebook or Twitter is suspended or locked, you can initiate an appeal process whether you think your account was disabled by mistake. Before that, check that you have not violated any rules of the terms of use, as these terms represent a legally-binding contract between you and the social media platform, and, in case of violation, they have the right to disable your account.

The latest version of Facebook's terms of service is available at: https://www.facebook.com/terms.php, while the latest version of Twitter's Rules is available at: https://help.twitter.com/rules-and-policies/twitter-rules

Facebook

1. In the case you believe your account was disabled by mistake, visit the page at: https://www.facebook.com/help/contact/260749603972907, you should not be logged in any account.
2. Fill the form, you should insert your email address or mobile phone number and your full name as it›s listed on the account.
3. You will be asked to provide a photo of your ID, like your passport or any other government-issued document with your personal details. Facebook will store your ID for up to one year to be used in 'detecting fake IDs through automated systems'.
4. If you don›t want Facebook to use your ID, turn that option off on the Identity Confirmation page, available at https://www.facebook.com/id?id_settings=true. In that case, the copy of your ID will be deleted within 30 days of submission.

Twitter

1. In the case you believe your account was suspended or locked by mistake, login to your account, then visit the page at: https://help.twitter.com/forms/general?subtopic=suspended
2. Fill the form, you will be asked to identify the device in which you are facing the problem; i.e. mobile or desktop.
3. You should describe the nature of your appeal, for example, why you do not believe your account violated the Twitter Rules.
4. Add your personal details, including your full name, email and Twitter user name, optionally, you can add your phone number.

Moving forward...

It is evident, through their impact, that social media platforms are not detached from the real world. Therefore, it is important for an individual to remember that if he joins a social media platform, he is joining a community, and, like any other community in the real world, there are rules and regulations governing discussion, expression of opinions amongst other interactions. Individuals need to make sure that they abide by community standards, represented in the rules and policies of social media platforms, and provisions of the law while practicing their right to freedom of expression online.
Even with such standards and provisions, misconduct still occurs, but as represented in this guide, social media platforms provide fast, easy and non-punitive remedies. The different tools and mechanisms for protecting privacy, preventing hate speech and reporting of abusive content can be considered practical and cheaper alternatives to penalties, which are set in laws.
In preparing this Guide, and to ensure its responsiveness to a wider group of stakeholders, we conducted focus group discussion with local experts in media, journalism, and freedom of expression. We discussed alternative options and recommendations for overcoming ill practices over the internet and social media while protecting online expression, and the following is suggested:

- The State should develop and adopt alternative penalties for cybercrimes such as administrative penalties and community service.
- Civil society organizations and other relevant stakeholders should develop and adopt their own policies and practices for their online platforms and interactions to demonstrate best practices and proper expression.
- Activists, civil society organizations and other relevant stakeholders should undertake advocacy initiatives and campaigns to raise public awareness with forms of cybercrimes, and highlight any challenges they face such as online harassment, blocking the content of their websites, etc.
- The Press Association should revise its adopted code of conduct and amend it as deemed necessary to encourage ethics and professional conduct, such as avoiding publication of fake news. the Association should also engage in awareness activities to ensure capacity among journalists with conform with the technical developments including the use of the internet and advanced technology
- Promote knowledge of cybercrimes within the young generations through alternative educational courses.
- Promote values of tolerance, human rights, dialogue, constructive criticism, etc. among the public.

As presented in the first section of this Guide, online freedom of expression in Jordan is governed by a collection of laws, but as technology is an ever-evolving creation, which provides numerous tools to deal with day-to-day challenges, a law can be considered as one of many ways to deal with such challenges. A law, with its punitive deterring measurements, is not always the only or best means to deal with violations that occur online, because with a fast-moving technology development, a law will remain behind, and finally any legal framework cannot be seen in isolation to public policy and implementation.

ICNL

INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW