UTeM

اونيۏرسيتي تيکنيکل مليسيا ملاک

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Always A Pioneer, Always Ahead

UTeM

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

MyUTeM

BITS 2523
Cyberlaw & Security Policy
Lecture 8

By

Mohd Fairuz Iskandar Othman, Phd

mohdfairuz@utem.edu.my

Ethical issues

Topics covered:

- Privacy
- Global issues of privacy in cyberspace
- Right to anonymity
- Right to be forgotten
- Defamation and cyber defamation
- Offensive content

Privacy

- Privacy is a fundamental human right. The right to privacy "constitutes an absolute imperative for…individual[s]" and is enshrined in international human rights treaties, such as Article 8 of the European Convention on Human Rights of 1950, Article 11 of the American Convention on Human Rights of 1969, Article 12 of the Universal Declaration on Human Rights of 1948, and Article 17 of the International Covenant on Civil and Political Rights of 1966.
- Conceptions of privacy vary and include the right to be free from observation; the right to be left alone; the capacity to keep one's thoughts, beliefs, identity, and behavior secret; and the right to choose and control when, what, why, where, how, and to whom information about oneself is revealed and to what extent information is revealed.
- In this modern society, right to privacy has been recognized both in the eye of law and in common parlance. The right to privacy refers to the specific right of an individual to control the collection, use and disclosure of personal information.

Privacy (cont...)

- Personal information could be in the form of personal interests, habits and activities, family records, education records, communication [including mail and telephone] records, medical records, to name a few.
- An individual could easily be harmed by the existence of computerized data about him/her which is inaccurate or misleading and which could be transferred for an unauthorized third party at high speed at very little cost. Innovative technologies make personal data easily accessible and communicable and there is inherent conflict between right to privacy and data protection.
- The latter understanding of privacy (i.e., the right to choose and control information about oneself) links privacy to information (or data) protection.

Privacy (cont...)

- Control and choice over disclosure of information is linked to an individuals' freedom to identify themselves and their actions at their own discretion and choosing and of their own volition. The right to privacy is, therefore, linked to freedom from identification.
- Anonymity enables users to engage in activities without revealing themselves and/or their actions to others. Online, anonymity "provide[s] individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks".
- In view of that, privacy affords users of information and communication technology with a space free from intimidation, retaliation, and other forms of coercion or sanction for the expression of thoughts, opinions, views, and ideas, without being forced to identify themselves.
- Accordingly, "technical solutions to secure and protect the confidentiality of digital communications, including [anonymity] measures…, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association".

Global issues of privacy in cyberspace

- This freedom from identification is believed to embolden some individuals to communicate cruel, discriminatory, racist, hateful, and/or other forms of harmful speech to others, which they would not otherwise have done if their identities were known.
- While this is true for some individuals, there are others who are emboldened by revealing their identities when making these comments. This identification occurs in order to be recognized by like-minded individuals and mobilize supporters to act.
- Milos Yiannopoulos, a former writer for a far-right sensationalist news source (Breitbart), is known for making racist, misogynist, anti-immigrant, and anti-Muslim remarks, as well as communicating other forms of hate speech, to gain popularity among those with similar views in the alt-right and far-right movements and/or supporters of these movements, and to mobilize others to engage in similar acts by targeting those who were the subject of his hate speech.

Global issues of privacy in cyberspace (cont...)

- The identity of the individual and their location can be difficult to ascertain due to anonymity and the use of privacy-enhancing technologies, such as Tor.
- Another example of a privacy-enhancing technology is encryption. Encryption blocks third party access to users' information and communications. Governments around the world have argued for the need to access encrypted communications and information in order to fight serious crimes, such as terrorism, organized crime, and child sexual exploitation. For these reasons, encrypted messaging services are considered illegal in certain countries.
- Telegram, an encrypted messaging app that has over 200 million users, has been blocked by judicial order in certain countries because the company refused to give these Governments decryption keys to monitor users' communications via the app

Global issues of privacy in cyberspace (cont...)

- Some countries have mandated the creation of backdoors and provision of decryption keys, while others, have requested the creation of backdoors and provision of decryption keys to fight serious crime, such as terrorism
- However, these backdoors and the provision of decryption keys could result in the abuse of access to data (e.g., data could be used by governments in unanticipated ways - above and beyond initial authorization in a specific case), and their use by criminals to gain access to this information for the purpose of viewing, copying, deleting, and/or altering it.
- Unsolicited commercial communications especially via unsolicited email or junk emails, generally referred to as spam, is a major cause of annoyance.

Privacy in Malaysia

- There is NO self-standing law on privacy in Malaysia, though there are several laws which provide limited rights to privacy such as the laws on data protection and criminal law. Up to 2009, the tort of invasion of privacy was not recognized in Malaysia. This basically means that no one can sue for invasion of his or her privacy.
- The right to privacy is provided by the Constitution. Article 5 of the Federal Constitution recognizes the right to privacy, according to the Federal Court case of Sivarasa Rasiah v. Badan Peguam Malaysia & Anor. Article 5(1) provides that "No person shall be deprived of his life or personal liberty save in accordance with law." Gopal Sri Ram FCJ (as then he was) said in the Sivarasa case, that the right to personal liberty includes the right to privacy. Nevertheless, it is not settled whether there is a tort of invasion of privacy rights in Malaysia.
- The Malaysian High Court case of Ultra Dimension Sdn Bhd v Kook Wei Kuan in 2009 had held that invasion or violation of privacy was not a recognized tort or a cause of action in Malaysia. In this case, the plaintiffs failed in their action for invasion of privacy against the defendant for taking a photograph of a group of kindergarten pupils, including the plaintiffs' child, at an open area outside the kindergarten and published it in two local newspapers.

Privacy in Malaysia

- A year later in 2010, the case of Lee Ewe Poh v. Dr. Lim Teik Man & *Anor became the first reported Malaysian case that recognizes the invasion of privacy as an actionable *tort.
- Maslinda Ishak v. Mohd Tahir Osman & Ors [2009] 6 CLJ 653 (impliedly recognised the tort); Lee Ewe Poh v. Dr. Lim Teik Man & Anor [2010] 1 LNS 1162; and Sherrina Nur Elena bt Abdullah v. Kent Well Edar Sdn Bhd (Sabah High Court Suit No. K22-187-2009-I (Unreported)), recognised the right to privacy and the tort of invasion of privacy in Malaysia.
- The High Court in Lew Cher Phow & Ors v. Pua Yong Yong & Anor [2011] MLJU 1195 observed that recent case law indicates that the Malaysian courts are leaning in favor of recognizing the right to privacy, especially given that the courts have to move with the change in times and the right to privacy is an unnamed right under the Federal Constitution.

* anor = another; ors = others ; tort = is a civil wrong that causes a claimant to suffer loss or harm, resulting in legal liability for the person who commits the tortious act.

Privacy in Malaysia

- Having said this, the existing laws are inadequate to protect private information and to protect against the intrusion of privacy. The importation of foreign principles through the reception of English Common Law offers only limited protection. Malaysia should, therefore, have a specific law to protect privacy.
- Existing privacy protections in Malaysia, which are only in limited circumstances such as in the Penal Code, Communications and Multimedia Act 1998 and the law of confidence. What we do not have, however, is a specific piece of legislation that expressly grants us the right to privacy.
- Calls for amending the Constitution to guarantee our right to privacy. Given the many digital surveillance and image-capturing gadgets available in the market, it will only be a matter of time before the use of such devices leads to abuse. As such, it is imperative that Malaysia should have a Privacy Act.
- The need to legislate a Privacy Act and its problem appear to lie in the issue of morality, the shifting standards of morality and the public's expectations of persons holding public office.

Privacy in Malaysia (cont...)

The effect of the recognition of the privacy rights in Malaysia is far reaching. It may, in no order, affect the following:

- Employees' rights especially when it comes to employee monitoring;
- Authorities' right to conduct searches such as strip searches or search of a premise or vehicle;
- Internet users' rights such as the right to remain anonymous;
- Details of relationships such as intimate details of partners including intimate pictures;
- The right of the media to report news regarding individuals;
- Rights of public figures such as politicians and celebrities; and
- The position of the admissibility in Court proceedings of illegally obtained evidence which infringes' an individual's right to privacy

Challenges enacting Privacy Law in Malaysia

- Challenge lies perhaps in Malaysia's multi-cultural and religious make-up whereby there are apparently different standards of morality being applied to Muslims and non-Muslims.
- There are potential conflicts between the Syariah law and any Privacy Act that clearly have to be addressed.

Removal of private information from the Internet

- Anything published on the internet will stay on the internet if no steps are taken to control its circulation – it will travel and be read by other people. Nothing is ever private on the internet. However, there may be circumstances where the content disappears from the internet. For example, when there is no longer any interest by anyone to preserve it.
- The leakage of private information on the internet does not necessarily destroy the quality of confidence in the information. Notwithstanding that such information can be downloaded online by anyone, it does not destroy the personal, private and confidential nature of the information. In AMP v Persons Unknown, the English High Court granted an interim injunction to prevent transmission, storage and indexing of any part or parts of stolen intimate pictures of a woman that were leaked online. The images were also uploaded to a Swedish website that hosts files known as "BitTorrent" files. The images have since been downloaded an unknown number of times by persons unknown. The images have been uploaded so that her name is appended to each of the images and can therefore readily be searched for when using online search engines.
- It is generally very difficult to remove anything from the internet, especially intimate photographs and videos. The best one can do is to limit the dissemination of the material by, among other things:
    1. If it is a user-generated website, the victim can report directly to the website operator to have it removed.
    2. If it is a self-published website, the victim can report to the operator directly to have it removed. However, they generally do not remove it. The victim may then consider filing a complaint to the web hosting service provider or even the domain name registrar.

Removal of private information from the Internet

- The victim should also assess the extent of the dissemination, that is, whether personal particulars such as full name have been published.
- If the search engine provider is showing the impugned / disputed materials based on a search of the personal particular, the victim should contact the search engine provider to request the removal of the link to the website. Most people would generally search for a person's name to obtain information about that person. Thus, it would be prudent to have links to the impugned materials removed from the search results.

Right to anonymity

- Many people don't want the things they say online to be connected with their offline identities. They may be concerned about political or economic retribution, harassment, or even threats to their lives. Whistleblowers report news that companies and governments would prefer to suppress; human rights workers struggle against repressive governments; parents try to create a safe way for children to explore; victims of domestic violence attempt to rebuild their lives where abusers cannot follow.
- Instead of using their true names to communicate, these people choose to speak using pseudonyms (assumed names) or anonymously (no name at all). For these individuals and the organizations that support them, secure anonymity is critical. It may literally save lives.
- There is no specific right to anonymity in Malaysia. One of the closest rights we have is under section 38 of the Personal Data Protection Act 2010, which allows a data subject to withdraw their consent to the processing of their personal data by a data user. However, this right is limited to matters concerning commercial transactions.

Right to anonymity

- Section 15(2) of the Courts of Judicature Act 1964 provides that a court may at any time order that no person shall publish the name, address or photograph of any witness in any cause or matter or any part thereof tried or held or to be tried or held before it or any evidence or any other thing likely to lead to the identification of any such witness; and any person who acts in contravention of any such order shall be guilty of an offence and shall, on conviction, be liable to a fine not exceeding RM5,000 or to imprisonment for a term not exceeding three years or to both.
- A blogger in Malaysia is unlikely to enjoy any right of anonymity. In the English case of The Author of A Blog v Times Newspapers Ltd,131 a blogger sought an interim injunction in the court to restrain Times Newspapers Ltd from publishing any information that would or might lead to his identification as the person responsible for a blog. The blogger argued that his anonymity protected him against any action being brought against him. His application failed. The High Court judge commented that blogging is a public activity and any right of privacy would likely be outweighed by public interest in revealing his activities.

Right to be forgotten

- The Right to be Forgotten is essentially the concept that individuals have the right to request that their data (collected by others) be deleted. This concept of "data deletion" has come to the forefront of many juridical discussions of the Right to be Forgotten.
- The Right to be Forgotten has risen to prominence alongside the rising importance of privacy law in general, particularly as understood in regulations like the European Regulation 679/2016 on Data Protection, (the "General Data Protection Regulation" or "GDPR").
- The issue has arisen from desires of individuals to "determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past."
- The legal history of the Right to be Forgotten can be said to have begun in 2010. That year, a Spanish citizen (together with the Spanish National Data Protection Agency) sued both a Spanish newspaper and Google, Inc. The Spanish citizen argued that Google was infringing on his right to privacy, because Google's search results included information relating to a past auction of the man's repossessed home. The plaintiff requested that his information be removed from both the newspaper and from Google's search engine results.
- Representatives for Google explained that even if the company could censor certain search results, as it had done in, for example, Google China, the censored information would remain in the original websites from which the Google results were created. Google effectively argued that they were data processors and not data controllers (two distinct classes with much different privacy obligations under E.U. privacy law).

Right to be forgotten

- Ultimately, the Division of Administrative Law of the Spanish National Court agreed to submit to the European Court of Justice (ECJ) a question of interpretation regarding certain provisions of the Data Protection Directive from 1995 on the protection of personal data. The questions were: 1) whether the Data Protection Directive applied to search engines; 2) whether the EU Law applied to Google Spain if the server was in the United States; 3) and whether a data subject could request to have his/her data removed from accessibility via search engines.
- In 2014, the ECJ ruled in favor of the Spanish citizen (C-131/12). The court stated that, according to the Art. 4.1 a) of the Data Protection Directive 95/46 EC , the European Data Protection Directive applies to search engine operators if one or more of the following three conditions are met: 1) if they have a branch/subsidiary in a Member State which promotes the selling of advertising space offered by the search engine to the inhabitants of that Member State; 2) if the parent company designates a subsidiary company in a Member State and it is responsible of two filling systems concerning data from the data subjects of such Member State; or 3) if the branch/subsidiary forwards to the non-EU parent company located outside the EU any requests and requirements from the data subjects or from authorities in charge of surveilling the data protection right even if these forwards are engaged in voluntarily.

Right to be forgotten

- As long as at least one of these conditions is met – in the aforementioned case, it was the first condition that the Court deemed Google to have met – the Court deemed this sufficient to qualify the search engine company as a data controller. As data controllers, the national laws that pursue the objectives of the directive 95/46/EC would fully applies to the search engine companies.
- For the Google Spain case, this meant that the Court affirmed the right of data subjects to ask search engine companies to remove links that contained personal information about the data subjects. The Court stated that: 1) the removal of data could be required under certain conditions, e.g., when the information is inaccurate, inadequate, irrelevant, or excessive for the purposes of the data processing; and 2) that the right was not absolute and needed to be balanced with other compelling rights such as the freedom of expression.

Right to be forgotten

- Under EU's GDPR, data subjects can exercise their rights to have businesses erase their personal information under specific circumstances – one of them being where they wish to withdraw consent on which the data processing was originally based. Another one being where the business no longer has any legal grounds or justification for processing personal data.
- With Malaysia PDPA, there is no equivalent provision. Under section 10, businesses can no longer keep their data subjects' data for "longer than necessary". This is in stark contrast with Article 17 of GDPR which states that data subjects can object to the processing of personal data and that the business in question has a maximum of 30 days to respond to such a request.

Legal controversies regarding Right to be forgotten

- There are already some notable concerns with the Right to be Forgotten – both in theory and in implementation:
- The main problem concerning the Right to be Forgotten (RTBF) lies in the clash between the good intentions of the regulators – written from an abstract point of view – and the actual complexity of real-life technical environments.
- The vagueness of the Article's definition, however, rubs the impossibility of its application: the Article seems to push towards the simple deletion of the personal data or the folder containing the personal data from the data controller's system, as if data on a computer was like a physical file that can simple be destroyed. Interestingly, the word "deletion" does not appear in the GDPR; and the word "remove" only appears twice but does not refer to the RTBF. The word used for the GDPR to refer to deletion is "erasure", and it is not explained throughout the text.

Legal controversies regarding Right to be forgotten

- In the light of the exceptions – for reasons of public interest in the area of public health, public interest, scientific, historical research or statistical purposes – some authors believe that the problem lies on determining what information may have value in the future.
- Ambrose argues that the immediate value and the remote value of the information play a major role in shaping the difficulties associated with the enforcement of this right, e.g., he claims that it can be dangerous in scenarios involving people running for political officers, for instance. Any misunderstanding concerning the RTBF might not matter in the light of a GDPR infringement. Penalties for non-compliance with the GDPR reach up to 4% of the undertaking annual revenue or include fines up to EUR 20 million. Moreover, those in the organization in charge of personal data protection can be criminally liable. Regulatory fines aside, one larger question that is somewhat outside the scope of this Article is whether the Right to be Forgotten matters – that is, whether there is a political, sociological, or moral need to protect the Right to be Forgotten. It seems so, according to the GDPR which is based on the fundamental right to data protection of the European Charter of Fundamental Rights.
- However, this assumption is not without defensible challenges, particularly from the free speech community. The United States, which could be considered by some to be an international free speech country, does not legally recognize the Right to be Forgotten. U.S. civil liberties advocates, and technology corporations have also fought against similar rulings. The legal discussion seems not to be of help either.

Legal controversies regarding Right to be forgotten

- In December 2015, the European Commission announced that while an individual that has given his/her consent to processing for a specific purpose has the right to get his/her data removed from the system when s/he does not want it processed anymore, still, “this does not mean that on each request of an individual all his personal data are to be deleted at once and forever”.
- The European Commission argues that retention of the data may be allowed for contract performance or for legal compliance reasons, and that data can be kept as long as it is necessary for that purpose. It is not surprising, therefore, that without any other clarification legal scholars and engineers are confused by the extent of such right.
- Some legal scholars see the main problem of the RTBF with the freedom of expression, of media and other compelling rights. Rosen believes that unless the right is defined more clearly, this right will make the gap between the understanding of privacy and freedom of speech between Europe and United States even wider, beyond the possibility that it will lead to a less open Internet.
- To that, the European Commission argues that, in theory, the Right to be Forgotten is about protecting the privacy of the individuals not about erasing past events or restricting freedom of press.

Defamation & cyber defamation

- The law presumes that a person is of good character, unless proven otherwise. If a statement about a person is defamatory and affects the reputation of that person in the eyes of the public, that person may have a claim for defamation against the maker of that defamatory statement.
- The term defamation is used to define the injury that is caused to the reputation of a person in the eyes of a third person. The injury can be done by words oral or written, or by signs or by visible representations. The intention of the person making the defamatory statement must be to lower the reputation of the person against whom the statement has been made in the eyes of the general public.
- The governing legislation for defamation in Malaysia is the Defamation Act 1957 ("Defamation Act"). The Defamation Act only applies to civil claims.
- The Malaysian law on criminal defamation is governed by the Penal Code (particularly, section 499) and will not be the focus of this topic.

Defamation

- Defamation is committed when the defendant publishes to a third person words or matters containing an untrue imputation against the reputation of the plaintiff. Liability for defamation is divided into two categories, that of libel and slander.
- Libel - If the publication is made in a permanent form or is broadcast or is part of a theatrical performance.
- Example: You are a member of your neighborhood committee. You receive a message through WhatsApp accusing you of being a troublemaker and a dishonest person, and that WhatsApp group includes many of your neighbors.
- Slander - If it is in some transient form or is conveyed by spoken words or gestures.
- Example: In an event attended by many of your colleagues, someone loudly exclaims that you are a lazy and incompetent worker. This person also said that you are only in your current position due to certain "favors" provided to your superiors.
- The plaintiff must prove three elements for the tort of defamation, which are:
  1. the plaintiff must show that the statement bears defamatory accusations;
  2. the statement must refer to or reflect upon the plaintiff's reputation; and
  3. the statement must have been published to a third person by the defendant.

Who to sue?

- Under Section 114A of the Evidence Act 1950, the following three categories of persons are presumed to have published a defamatory statement unless the contrary is proved:
  1. A person whose name, photograph or pseudonym appears on any publication depicting himself as the owner, host, administrator, editor or sub-editor, or who in any manner facilitates to publish or republish.
  2. A person who is registered as a subscriber of a network service.
  3. A person who has in his custody or control any computer on which any publication originates.
- Section 114A operates as a presumption in law, there is no need for the person suing to prove who published the defamatory statement. For example, if B used C's Facebook account to post something defamatory about D, D can now rely on this presumption in order to sue C. D does not have to prove on a balance of probabilities that C posted the defamatory post on his Facebook account. However, C bears the burden of proving that C did not publish the defamatory post on Facebook.
- In the case of Thong King Chai V. Ho Khar Fun [2018] 1 LNS 374, the High Court held that an email was presumed to have been published by the defendant since it originated from his email address. Thong's case further held that there was also a presumption of fact that a Facebook post was published by the defendant since it was published using his Facebook account.

Who to sue?

- Alternatively, it is possible to bring an action for a pre-action discovery under Order 24 Rule 7A of the Rules of Court 2012 to discover the identities of the person who posted the defamatory post. In the case of Kopitiam Asia Pacific Sdn Bhd v Modern Outlook Sdn Bhd & Ors [2019] 10 MLJ 243, the plaintiff discovered that an article allegedly defaming him was circulating on certain websites. The plaintiff contended that he had insufficient information on those responsible for posting the defamatory article. Hence, he commenced an action against the defendants who were the administrators of the websites for an order that the defendants disclose all relevant information on the identities of the relevant parties.
- The High Court held that under the Data Protection Act 2010, the Court is empowered to direct persons in possession of relevant data to disclose it to a third party. Consequently, the High Court allowed the plaintiff's pre-action discovery having been satisfied that the plaintiff's intended action against the persons responsible for posting the defamatory article can only be fairly disposed of once the plaintiff obtained the necessary information from the defendants.

Defamation

- The test involved in determining whether or not the words complained of are defamatory is a two-stage process:
    1. First, it must be considered what meaning the words would convey to an ordinary person; and
    2. second, it must be considered whether, under the circumstances in which the words were published, a reasonable man would be likely to understand that in a defamatory way
- However, there is no precise test to be applied to determine whether or not any given words are defamatory.
- A defamatory accusation is one to a man's discredit, or which tends to lower him in the estimation of others, or to expose him to hatred, contempt or ridicule, or to injure his reputation in his office, trade or profession, or to injure his financial credit. The standard of opinion is that of right-thinking person's generally. To be defamatory an accusation need have no actual effect on a person's reputation; the law looks only to its tendency.
- Whether the words are defamatory lies in the nature of the statement in that it must have the tendency to affect the reputation of a person. Therefore, the question arises in whose eyes the words complained of must have the tendency to affect the plaintiff's reputation.

Defamation

- There are two methods of interpreting the words in an allegedly defamatory statement:
  - By their natural and ordinary meaning; or
  - By innuendo.
- The natural and ordinary meaning of words may be:
  - The literal meaning of the words;
  - An implied or inferred or an indirect meaning;
  - Any meaning based on general knowledge.
- In most defamation cases, the court will only be concerned with the natural and ordinary meaning of the words claimed to be defamatory. This is the meaning that an ordinary, reasonable person would derive from the words, without any special knowledge beyond that which is known to ordinary people generally.

Defamation

- Alternatively, it is how the words would be understood by “the man in the street”. This means that the plaintiff must identify what he claims to be the natural and ordinary meaning of the words as understood by the ordinary reader. In this context, the natural and ordinary meaning includes innuendos, that is, something which is insinuated in or inferred from the words.
- Innuendo is used to describe words which have special meaning only to persons who have knowledge of some special background or facts.
- For example, the statement that “Kenny recently purchased a luxurious bungalow worth RM10 million” may not be defamatory under its natural and ordinary meaning. Without knowing more about Kenny, it can be taken to mean that Kenny is a wealthy man who recently made another property investment.
- However, for those who know that Kenny is employed as a civil servant, the statement can be understood to mean that Kenny may be engaging in corrupt activities. This is because it is usually difficult for a civil servant to be able to afford such a lavish home.

Defamation

- The determination of the meaning of the disputed words involves both a question of fact and law. The actual meaning of the publication is a question of fact. However, the court has a preliminary power to hold that the words are not capable of bearing a particular meaning, which is a question of law. In short, where the words are not capable of bearing the pleaded meaning, that meaning will be struck out.
- The determination of the meaning of the disputed words involves both a question of fact and law. The actual meaning of the publication is a question of fact. However, the court has a preliminary power to hold that the words are not capable of bearing a particular meaning, which is a question of law. In short, where the words are not capable of bearing the pleaded meaning, that meaning will be struck out.

Proving that a Defamatory Statement was Published

- "Publication" means making the defamatory statement known to some other person other than to whom it is written or spoken. The statement must be published to a third party. The uttering of a libel to the party libeled is not publication for the purpose of a civil action. The fundamental principle is that the statement must be communicated to a third party in such manner as to be capable of conveying the defamatory imputation about the plaintiff.
- Publication includes electronic publication, and it may be in various forms. Facebook postings, tweets, online forum messages or instant messages, electronic voice messages, domain names, text on hyperlink or even a Wi-Fi name are some forms of electronic publication.
- It is easy to prove that the defamatory statement was published once it is posted on the internet. The case of Datuk May Phng @ Cho Mai Sum & Ors v Tan Pei Pei [2018] 11 MLJ 741 concerned defamatory statements circulated by email. The High Court held that the email in question is not an ordinary email directed to one person but rather one "written in the context to address the public, to have the said email widely circulated among the public". As such, there is "a presumption by law that such circulation over the internet is presumed to be wide publication and the onus is on the defendant to prove the limited publication as alleged".
- Similarly in the case of Datuk Seri Anwar bin Ibrahim v Wan Muhammad Azri bin Wan Deris [2014] 9 MLJ 605, the High Court took judicial notice that the internet is used worldwide. In this case, the blogger known as 'Papa Gomo' had published defamatory statements with the intention to discredit Datuk Seri Anwar bin Ibrahim "to show that he is an immoral person, not dignified, ineligible to hold public office, not eligible to become political leader, not fit to be Prime Minister and a leader who is not responsible and cannot be trusted". As such, the High Court held that given that the defamatory statements were published on the internet and "people all over the world can get access to the website …there was a wide publication of the defamatory statements".

Cyber defamation

- Cyber defamation is publishing of defamatory material against another person with the help of computers or internet.

Example:

- Someone publishes some defamatory statement about some other person on a website or send emails containing defamatory material to other persons with the intention to defame the other person about whom the statement has been made would amount to cyber defamation.
- The same laws for defamation apply to online defamation. This can be seen in the cases which involve the liability of intermediaries. Our courts have applied principles applicable to traditional intermediaries to cases involving Facebook pages or group owners and online forum operators, rules on the publication of defamatory materials via the Internet (for example, single and multiple publication rules and the presumption of publication to third parties).
- However, there are some notable differences when dealing with online defamation. Requirements of pleadings for cyber defamation is slightly different, for example, the URL and time and date of publication of the impugned website should be pleaded.

Cyber defamation

Example:

- Under the general law of tort, everyone who knowingly takes part in the publication of a libel, or authorizes or ratifies it, are jointly and severally liable. In relation to a Facebook page, other users of Facebook may publish his or her comments on the Facebook page of another provided that the owner of the latter has allowed that to be done. The Facebook page owner has the option to delete or hide the comment. A question would be whether the Facebook page owner is liable for the comments made by third parties on their Facebook page.
- The High Court in GS Realty Sdn Bhd v Lee Kong Seng dealt with the liability of a Facebook page owner over third-party statements. The plaintiff, a company carrying on business as a property agent, sued the defendant, a former agent of the plaintiff, for defamation after the latter posted certain comments on his Facebook page. His Facebook posting containing the defamatory statements were commented on by other parties known to the plaintiff. These comments were found to be defamatory by the High Court. The court found the defendant liable for defamation over his Facebook posting and responsible for the postings of others on his Facebook page.

Cyber defamation

- A republication of a defamatory statement is also still be defamatory. In the case of YB Hj Khalid bin Abdul Samad v Datuk Aziz bin Isham & Anor [2012] 7 MLJ 301, the High Court quoted Gatley on Libel and Slander (8th Ed), at p 117 which states that "every republication of a libel is a new libel and each publisher is answerable for his act to the same extent as if the calumny originated with him".
- Accordingly, every repost or share of a defamatory statement is considered a new publication because those who do so are deemed to have approved, endorsed or repeated the same. This position was reiterated in the recent Court of Appeal case of Raja Syahrir bin Abu Bakar & Anor v Manjeet Singh Dhillon and other appeals [2019] MLJU 75.
- Unlike Facebook, an administrator of an instant messaging application (for example, WhatsApp) group may not have the option to delete messages of their group members. An administrator generally has the power to add or remove members. The power to control a group depends on the instant messaging application. For example, a Telegram group administration may mute the group and disallow other users to post any comments.
- There is currently no Malaysian case decided on this point.

Responding to Cyber Defamation

- Businesses have a variety of potential responses available when faced with defamatory online statements, each of which offers its own potential risks. These options range from doing nothing to filing a lawsuit:

  - Ignoring the statement
  - Seeking removal of the statement
  - Rebutting the statement
  - Filing a legal action

Damages

- Defamatory statements made on social media are regarded as libel (as per the case of Tony Pua Kiam Wee v Dato' Sri Mohd Najib bin Tun Haji Abdul Razak [2018] 3 CLJ 522). Libel is actionable per se, so there is no need to prove actual damage suffered due to the defamatory statement.
- Case laws have shown that the Court may consider the following factors in assessing damages:
  - The gravity of the allegation;
  - The size and influence of the circulation;
  - The extent and nature of the claimant's reputation; and
  - The effect of the publication.

Damages

- In the case of Sociedad Limitada & Ors v Drive M7 Sdn Bhd [2018] MLJU 1614, the court held that the factors above are not exhaustive. The more important point to note is that “the tort of defamation exists to protect, not the person or the pocket, but reputation of the person defamed”.
- Given the above, it is strongly advisable to exercise more caution when we publish or republish statements on social media to prevent the allegation of defamation.
- Should you wish to publish statements for corporate or business purposes such as advertisements, public journal and so on, it will be prudent to first consult a legal advisor for risk management purposes.

Offensive content

- Offensive content is defined as “any published or broadcast content (such as articles, photographs, films, or websites) that is likely to be upsetting, insulting, or objectionable to some or most people”.
- In Malaysia, as far as offensive content on the Internet is concerned, section 211 and section 233 of the CMA are the main provisions that enable legal action to be taken against providers of offensive content on the Internet. Section 211 CMA provides that:

  “(1) No content applications service provider, or other person using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person.

  (2) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of one thousand ringgit for every day or part of a day during which the offence is continued after conviction.”
- Regarding the term “offensive content”, the CMA does not provide a specific definition. Nonetheless, the term ‘content’ is defined in section 6 of the CMA as: "any sound, text, still picture, moving a picture or other audio-visual representation, tactile representation or any combination of the preceding which is capable of being created, manipulated, stored, retrieved or communicated electronically."

Offensive content: indecent content

- Accordingly, S 211 of the CMA sets out five categories for the internet content to be offence which are; indecent content, obscene content, false content, menacing content and offensive in character, also no definitions for these types of offensive content on the internet is provided under s 211. However, the Malaysian Communications and Multimedia Content Code has classified the offensive content into nine categories; they are; Indecent Content, Obscene Content, Violence, Menacing Content, Bad language, False Content, Children's Content, Family Values, People with Disabilities (The content code, 2001).
- Indecent content is defined as "a material which is offensive, morally improper and against current standards of acceptable behaviour. This includes nudity and sex." (Malaysian, n.d). While the second category of offensive content on the internet under s 211 CMA is obscene content; no definition is provided for the term "obscene" in the CMA.

Offensive content: indecent content

Example:

Astro has been fined by the Malaysian Communications and Multimedia Commission (MCMC) for airing in 2015 an Al Jazeera documentary on the controversial murder of Mongolian Altantuya Shaariibuu. The news portal cited the MCMC as saying it fined the satellite television provider as its investigations concluded the content of the document to be indecent and the firm to be in violation of Section 211 of the Communications and Multimedia Act 1998.Section 211 handles "provision of offensive content", which prohibits content that is "indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person". "In its letter to Measat, MCMC said the company was found guilty of airing the episode, which was indecent, with the intention to offend related parties. "As such, the company was fined RM1,000 for each time the episode was aired, totalling RM4,000. The company has 30 days to appeal against the compound," said the report.

Report: MCMC fines Astro for airing Al Jazeera documentary on Altantuya murder five years ago | Malaysia | Malay Mail

Offensive content: obscene content

- Similarly, the term “obscene” is not defined in the Malaysian Penal Code as what may be obscene at present may not be in the future. It also differs and varies from age to age, region to region, from culture to culture and perhaps religion to religion (ASM, n.d). In Pandurangan v State, the court stated that the word ‘obscene’ means ‘offensive to chastity or modesty; expressing or presenting to the mind or view something that delicacy, purity and decency forbid to be expressed; impure, as obscene language, obscene pictures anything ‘expressing or suggesting unchaste and lustful ideas, impure, indecent, lewd (ASM, n.d).
- In 2013, Fila Syahida Zulkipli was charged under section 292 of the Penal Code by the Mukah Magistrates Court. She pleaded guilty to recording an obscene video of a 15-year-old girl using her mobile phone and was fined for producing the obscene video (Malaysia, n.d).

Offensive content: obscene content

- In this context, obscene content has been described as “content that gives rise to a feeling of disgust because of its lewd portrayal and is essentially offensive to one’s prevailing notion of decency and modesty, such as content may have a negative influence and corrupting the mind
- Three obscenity standards in Miller v. California has been based on what is offensive in a particular community and not all over the world.
- For example, what's offensive to someone in a specific society may not be in another society, this could create legal challenges on the applicable law that governs the obscene, also different cultures may have different standers of obscenity. Moreover, nowadays, the Internet has made the obscenity much more complicated. Today obscenity materials can be sent from a computer in a specific country to someone else in another country by the click of a button. As a result, the three obscenity standards in Miller v. California, may not be adequate to describe obscene content (Eze, 2018).

Offensive content: obscene content

Example:

From 2015 to 2018, the Malaysian Communications and Multimedia Commission (MCMC) blocked more than 400 websites that contained child sexual abuse content through collaborations and information-sharing with Interpol and the Royal Malaysia Police. MCMC's chief compliance officer Zulkarnain Mohd Yassin said the action was taken under Section 211 of the Communications and Multimedia Act which prohibits the content application service provider or other persons using the service to provide, produce or solicit indecent, obscene, false, menacing or offensive content with intent to annoy, abuse, threaten or harass any person.

MCMC: Over 400 websites with child sexual abuse content blocked | Malaysia | Malay Mail

Offensive content:menacing content

- The second offence of offensive content under s211 CMA is menacing content which is described by the Malaysian Communications and Multimedia Content Code as, the content that annoys, threatens harm or evil, encourages or incites crime, or leads to public disorder.
- Also, hate propaganda and information which may be a threat to national security or public health and safety are considered as a menacing content, and it shall not be presented (Communications, n.d).
- Creating a false or misleading impression on the internet is also an offence under s 211 CMA. False content has been described as content that contains dishonest material which may mislead; this might be because of incomplete information.
- However, there are two exceptions for false content which are; satire and parody; and where it is clear to an ordinary user that the content is fiction. Nevertheless, it is evident that s 211 CMA required mens rea for the offensive content offences, which is the intent to annoy, abuse, threaten or harass any person.

Offensive content: False content

Example:

Yesterday, MCMC issued a statement saying that sharing false news or altered images related to the investigation on the state-owned fund on social media or on mobile messaging app WhatsApp could be a violation of Section 211 or Section 233 of the Communications and Multimedia Act 1998. Sections 211 and 233 of the law concern state it is an offence for people to provide electronic content that is indecent, obscene, false, menacing or offensive with the intent to annoy, abuse, threaten or harass any person, punishable by a fine of not more than RM50,000 or imprisonment of not more than one year.Lim said MCMC did not do anything when false news alleging his teenage son of a sexual offence were spread online several years ago. "All they did was advised us to lodge a police report and after we lodge a police report, the matter ended there but in this case, MCMC immediately issues a warning," he said. “This clearly showed that there is a political motive behind MCMC's warning, he added.

MCMC warning a bid to curb public attention on 1MDB, Guan Eng claims | Malaysia | Malay Mail

Improper use of network facilities or network services

- In Malaysia, the second provision that prohibits offensive content on the Internet is section 233 of the CMA, that provides: “Improper use of network facilities or network service, etc.

(1) A person who

(a) By means of any network facilities or network service or applications service knowingly:
(i) Makes, creates or solicits; and
(ii) Initiates the transmission of, any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person; or

(b) initiates communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address, commits an offence.

(2) A person who knowingly

(a) by means of a network service or applications service provides any obscene communication for commercial purposes to any person; or

(b) permits a network service or applications service under the person’s control to be used for an activity described in paragraph (a), commits an offence.

(3) A person who commits an offence under this section shall, on conviction, be liable to a fine not exceeding RM50,000 or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of RM1,000 for every day during which the offence is continued after conviction.”

Improper use of network facilities or network services

- Some would argue that illegal and harmful content seems different in a sense; the first is criminalized by national laws, while the second could be considered as disgusting or offensive by some people and not criminalized by national laws. This means that harmful content on the Internet is legal content, but it may offend some Internet users or could be thought to the harm of others, for example, access to sexually explicit content by children, sexually explicit content, religious beliefs, political opinions, views on racial matters and sexuality; but child pornography is the most common example of illegal content on the Internet (Yaman, 2001).
- PP v Rutinin Bin Suhaimin 2015 established three ingredients that must be proven to be an offence under s. 233 CMA 1998 (Rutinin, 2015):

  I. The accused person-initiated communication in question.

  II. The communication in question is either indecent, obscene, false, menacing, or offensive in character; and

  III. The accused had the intention to annoy, abuse, threaten or harass any person

The Balance between Freedom of Expression and S 211, 233 CMA 1998

- Freedom of expression refers to “the right of individuals and communities to express their opinions or ideas without fear of reprisals or censorship or sanctions”. Mendel (2010). The right of freedom of expression has been generated by article 19 of the Universal Declaration of Human Rights (UDHR) which provides that " 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" (The Universal Declaration of Human Rights, n.d). Similarly, article 19 (2) of the International Covenant on Civil and Political Rights (ICCPR) affirmed the right of freedom of expression (ICCPR, n.d).
- The UNHRC noted that the exercise of the right to freedom of expression on the Internet is "increasing interest and importance as the rapid pace of technological development enables individuals all over the world to use new information and communications technologies." However, the UNHRC affirmed that article 19 could be applied to the freedom of expression on the Internet (Acharya, 2015).
- In this regard, s 233(1) of the CMA has been criticized as a serious encroachment on freedom of expression, as it is broad in scope, with vague and ambiguous terms that can easily be misused to stifle speech and expression (Steven, n.d)

The Balance between Freedom of Expression and S 211, 233 CMA 1998

- However, it has been argued that s 211 and s233 of the CMA intend to protect individuals who have been hurt by any negative remarks, photos, signs on the internet or derogatory materials. This would be a deterrent measure that is necessary to prevent offensive content on the internet.
- However, the only problem is related to the interpretation and how to use these sections, for example "what constitutes indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass'"? Therefore, s 211 and 233 can be used to silence the critics and comments on political issues (Shahrin, 1998).
- The freedom of expression right is not absolute, this is can be seen in the international law, whereby Article 19(3) of the ICCPR provides two limitations on the rights recognized in article 19(2), which are: the rights must be provided by law and must respect the right of reputations, national security, public order, or public health or morals. (ICCPR, n.d) Furthermore, Article 20 of the ICCPR restricts freedom of expression to protect the other rights, for instance, propaganda for war, advocacy of national, racial or religious hates that could lead to discrimination, hostility or violence (Prohibited, n.d). In addition to this, Article 17 of ICCPR protects any acts against arbitrary or unlawful interference and unlawful attacks on reputation (Subjected, n.d).

The Balance between Freedom of Expression and S 211, 233 CMA 1998

- Consequently, according to the above illustration, it could be submitted that:
  1. It cannot be said that s 211 and s233 of the CMA violates freedom of expression, because freedom of expression is not an absolute right, it has limits and as determined by the constitution and the law. In addition, freedom of expression mustn't offend others, it must be within the law.
  2. Due to the seriousness of cybercrime, which has no geographical limits with broad effects that may not be remedied, s 211 and s 233 CMA are suitable to deter people who have criminal tendencies.
  3. Offensive content cannot be limited to specific acts, since the offensive content may be different from one community to another. Further, the Malaysian Communications and Multimedia Content Code describes the offensive content into categories. Fourthly, s 211 and s 233 of the CMA is designed to protect the rights with broad interpretation to consist of any offensive content on the Internet (Elad, Ngan & Bongbee,2017)

Improper use of network facilities or network services

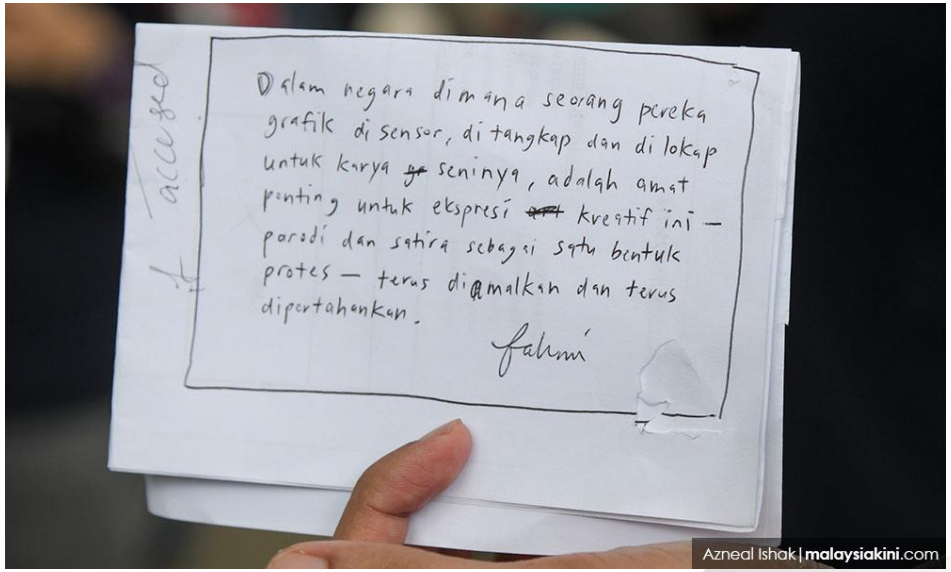
- In PP v Muslim bin Ahmad 2013 (Muslim, 2013) The accused was charged under s 233(1) of the CMA for three offences of posting offensive comments, on the Perak State Government's official portal. He denied the charges and claimed that he had been at work when the offensive comments were posted, this was proven by two witnesses. He also called one Krishnan a/l Raja Gopal ("DW4") as his expert witness to show that IP spoofing was done, but his conclusions were without a real examination of any exhibits or the server. The accused was fined of RM10,000 in respect of each charge, and in default of each fine, to six months' imprisonment.
- It is clear that a person who posts any offensive materials on the Internet may be prosecuted under section 233 of the CMA, but the prosecutor must prove that the post has been disseminated with an intent to annoy, abuse, threaten or harass others.

Improper use of network facilities or network services

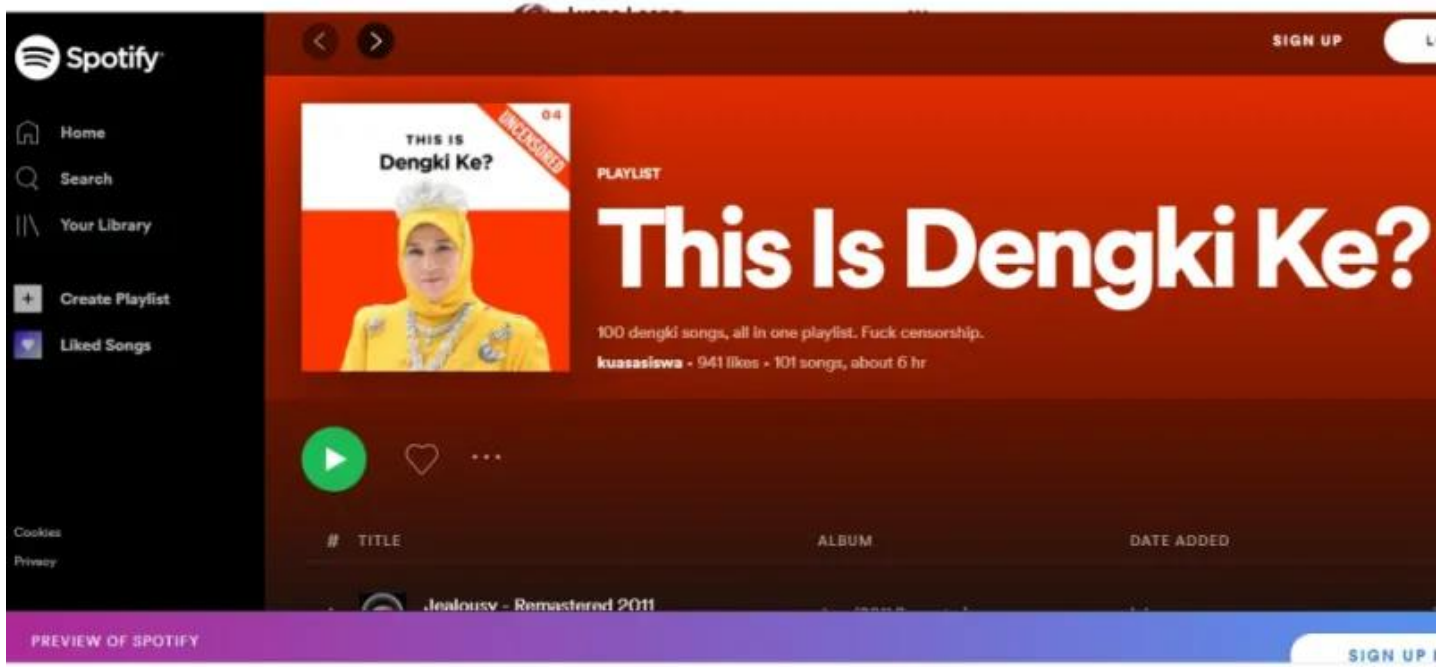
Example:

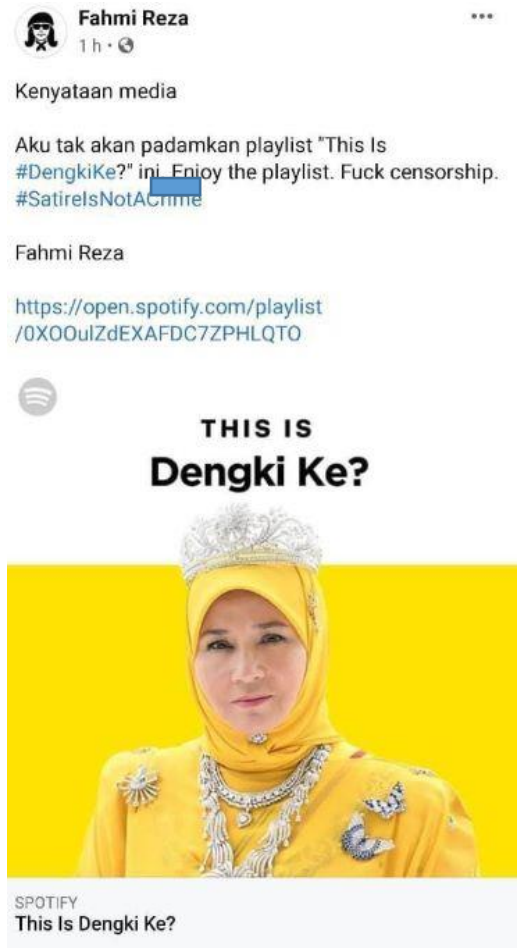
Graphic artist Fahmi Reza Mohd Zarin has been called by the police to give his statement on two different social media postings. Fahmi said that the probe is being carried out under Section 504 of the Penal Code and Section 233 (1) of the Communications and Multimedia Act 1998. Section 504 of the Penal Code deals with deliberate attempts to humiliate with the intention of breaching the peace and carries a prison sentence of up to two years, or a fine, or both.The other charge involves Section 233 (1) of the Communications and Multimedia Act 1998, whereby a person who uses the internet or telephone to spread false news may be subject to legal action.

[Fahmi Reza under police probe again over two other social media postings | Malaysia | Malay Mail]



Improper use of network facilities or network services





[Fahmi Reza under police probe again over two other social media postings | Malaysia | Malay Mail]

[Communications Ministry will not interfere, leaving it to police to investigate Fahmi Reza, says minister | Malaysia | Malay Mail]

Improper use of network facilities or network services

Example:

Opposition Leader Datuk Seri Anwar Ibrahim had his statement recorded by the police today over a leaked phone conversation allegedly between him and Umno president, Datuk Seri Ahmad Zahid Hamidi. In a statement today, Bukit Aman Criminal Investigation Department (CID) director Datuk Huzir Mohamed said that this was done after 18 police reports were lodged over the voice recording.“Investigation is being carried out under Section 505(b) of the Penal Code, that is over statements which cause or which is likely to cause, fear or alarm to the public, and Section 233 of the Communication and Multimedia Act (CMA) 1998, that is for improper use of network facility or network service, after an order to investigate was obtained according to provisions under Section 108 (2) of the Criminal Procedure Code, from the public prosecutor,” Huzir said. He added that the four minutes and 17 seconds voice clip which went viral early this month, has caused public fear and alarm, which led to police reports being lodged.

Cops say recorded Anwar’s statement over audio clip purportedly with Zahid, after 18 reports lodged | Malaysia | Malay Mail

Improper use of network facilities or network services

Example:

Federal police have opened an investigation paper into the case of a newsreader who had allegedly made slanderous remarks on television. Berita Harian reported Deputy Inspector-General of Police Datuk Seri Acryl Sani Abdullah Sani as saying that the case will be investigated under Section 504 of the Penal Code for intentionally insulting any person with the likelihood that such provocation will break the public peace. The reader was presenting news on the RM50,000 fine imposed upon a burger seller in Kelantan, after it was found that he violated existing standard operating procedures for Covid-19. At the start, the reader used a Malay idiom to imply that the authorities are foolish to impose such fines upon members of the public seeking to earn a living and raise their families during the ongoing pandemic. The incident will also be investigated under Section 233 of the Communications and Multimedia Act for the improper use of network facilities or network service, which is punishable with a RM50,000 fine, one year imprisonment, or both.

Deputy IGP: Police open investigation paper on news anchor who made offensive remarks on air | Malaysia | Malay Mail

Summary

- In summary s.211 of the CMA describes that content on the internet is offensive if the content is: indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person.
- The content could be sound, text, or picture. In fact, it's really difficult to draw out a comprehensive definition, because what shall be deemed offensive content in a specific country, custom, or peoples may not be for others. It also differs and varies from age to age, region to region, from culture to culture and perhaps religion to religion.
- Also, it seems that the offensive content on the internet under s.211 and s.233 of the CMA is very broad but, in the end, it's subject to the court's assessment whether the content falls under the types of offensive content described in s.211 and s.233 of the CMA.
- Finally, it could be submitted that s.211 and s.233 of the CMA does not breach the right to freedom of expression, as there is a limitation on freedom of speech and this principle is not an absolute right; freedom of speech does not mean a right to offend others.
- Additionally, s.211 and s.233 of the CMA is designed to protect people's rights with a broad interpretation to consist of any offensive content on the Internet in the future, as evaluated by the court.
- Section 233 deals with the improper use of network facilities or network service, while Section 211 prohibits the publication of offensive content on the Internet.

Thank You

MyUTeM

www.utem.edu.my