



UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UTeM

BITS 2523

Cyberlaw & Security Policy

Lecture 10

By

Mohd Fairuz Iskandar Othman, Phd

mohdfairuz@utem.edu.my

Future Cyberlaws in Malaysia

Always A Pioneer, Always Ahead

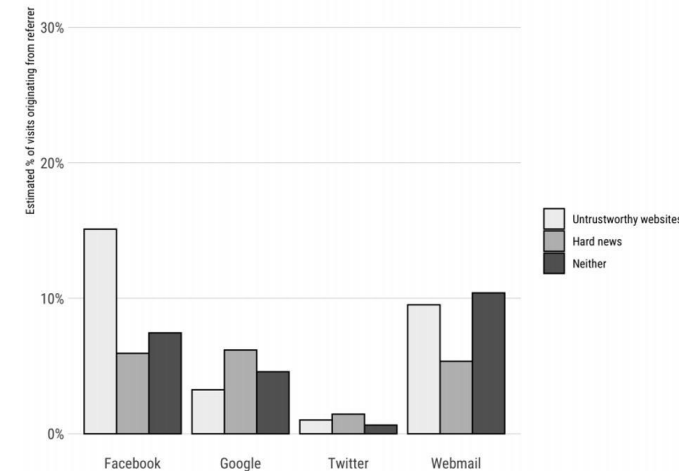
Topics covered:

- Fake news: Anti-Fake News Act 2018 (repealed)
- Cloud Computing
- Internet of Things (IoT)
- Blockchain
- Social media
- Spam
- Cybersecurity and related issues

Anti-Fake News Act 2018 (repealed)

Always A Pioneer, Always Ahead

- The Anti-Fake News Act (AFNA) was introduced to seek to deal with fake news by providing for certain offences and measures to curb the dissemination of fake news and to provide for related matters.
- As technology advances with time, the dissemination of fake news has become a global concern and is more serious in that it affects the public.
- Fake news may cause situations of anger, panic and unrest which affects the economy, and the people.



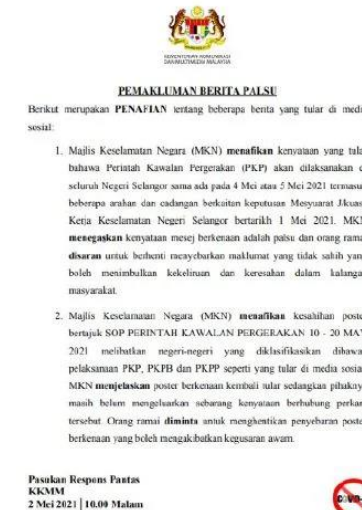
Facebook Spreads Fake News Faster Than Any Other Social Website, According To New Research*

*<https://www.forbes.com/sites/traversmark/2020/03/21/facebook-spreads-fake-news-faster-than-any-other-social-website-according-to-new-research/?sh=588fdf6e6e1a>

Anti-Fake News Act (repealed)

Always A Pioneer, Always Ahead

- The AFNA has now been repealed, but sought to safeguard the public against the proliferation of fake news while ensuring that the right to freedom of speech and expression under the Federal Constitution is respected.
- The Provision on the power of the court to make an order to remove any publications containing fake news served as a measure to deal with the misuse of the publication medium, in particular social media platforms.
- With the Act, it was hoped that the public will be more responsible and cautious in sharing news and information.



SOP PERINTAH KAWALAN PERGERAKAN 10-20 MAY 2021

KATEGORI	PKO Pulau Pinang Selangor Wilayah Persekutuan Melaka Johor Sabah	PKPB Pahang Perak Kedah Negeri Sembilan Terengganu Kelantan	PKPP Perlis Sarawak
Aktiviti sosial berbilang kumpulan (perkahwinan, sambutan perayaan, pertunjukan & sebagainya)	✗ Tidak dibenarkan	✗ Tidak dibenarkan	✓ Dibenarkan dengan SOP yang ketat
Rentas Negeri	✗ Tidak dibenarkan	✗ Tidak dibenarkan	✗ Tidak dibenarkan
Rentas Daerah	✗ Tidak dibenarkan	✓ Dibenarkan	✓ Dibenarkan
Jarak Pengerakan (dari 1000 jam negeri)	10 KM	Tiada	Tiada
Pembatasan Kumpulan (maksudnya pengurusan & skenarografi hadir ke pejabat)	2 orang sahaja termasuk ahli keluarga	Tiada	Tiada
Lidat Kadal Makan	✓ Dibenarkan secara peribadi dengan SOP yang ketat	✓ Dibenarkan dengan SOP yang ketat	✓ Dibenarkan dengan SOP yang ketat
Khidmat penghantaran makanan	✓ Dibenarkan	✓ Dibenarkan	✓ Dibenarkan
Pasraya, Perkhidmatan Kesihatan (Ginek/ Hospital, Farmasi) & Bank	✓ Dibenarkan	✓ Dibenarkan	✓ Dibenarkan

Sumber: MAJLIS KESELAMATAN NEGARA

NSC denies viral info of MCO in Selangor either May 4 or 5

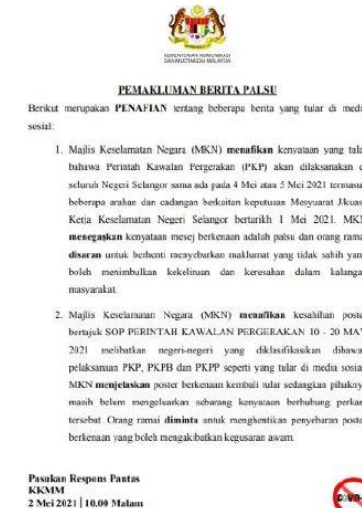
Anti-Fake News Act (repealed)

Always A Pioneer, Always Ahead

Creating, offering, publishing, etc fake news or a publication containing fake news

- Section 4 of the AFNA made it an offence for any person who, by any mean, maliciously created, offered, published, printed, distributed, circulated or disseminated any fake news or publication containing fake news.
- Fake news was defined in Section 2 as:

“fake news” included any news, information, data and reports, which is or are wholly or partly false, whether in the form of features, visuals or audio recordings or in any other form capable of suggesting words or ideas;
- Section 4 sets out some illustrations where the offence under Section 4 would apply:
 - A offers false information to B, for B to publish the information in B's blog. B not knowing that the information offered by A is false, publishes the information in his blog. A is guilty of an offence under this section. B is not guilty of an offence under this section.



SOP PERINTAH KAWALAN PERGERAKAN 10-20 MAY 2021

KATEGORI	PKO Pulau Pinang Selangor Wilayah Persekutuan Melaka Johor Sabah	PKPB Pahang Perak Kedah Negeri Sembilan Terengganu Kelantan	PKPP Perlis Sarawak
Aktiviti sosial berkumpulan (melainkan dengan perlesenan, perlesenan & keagamaan)	✗ Tidak dibenarkan	✗ Tidak dibenarkan	✓ Dibenarkan dengan syarat yang ditetapkan
Rentas Negeri	✗ Tidak dibenarkan	✗ Tidak dibenarkan	✗ Tidak dibenarkan
Rentas Daerah	✗ Tidak dibenarkan	✓ Dibenarkan	✓ Dibenarkan
Jarak Pergerakan (dari rumah ke lokasi lain)	10 KM	Tiada	Tiada
Pembatasan Kumpulan (penggunaan & sekiranya hadir ke pejabat)	2 orang sahaja dalam kumpulan dari 1 keluarga	Tiada	Tiada
Lidat Kadal Makan	✓ Dibenarkan secara peribadikan Taka away	✓ Dibenarkan dengan SOP yang ketat	✓ Dibenarkan dengan SOP yang ketat
Khidmat penghantaran makanan	✓ Dibenarkan	✓ Dibenarkan	✓ Dibenarkan
Pasaraya, Perkhidmatan Kesihatan (Glinik/ Hospital, Farmasi) & Bank	✓ Dibenarkan	✓ Dibenarkan	✓ Dibenarkan

Sumber: MAJLIS KESELAMATAN NEGARA

NSC denies viral info of MCO in Selangor either May 4 or 5

Anti-Fake News Act (repealed)

Always A Pioneer, Always Ahead

- Section 4 sets out some illustrations where the offence under Section 4 would apply:
 - b) A fabricates an information by stating in an article published in his blog that Z, a well-known businessman has obtained a business contract by offering bribes. A is guilty of an offence under this section.
 - c) A fabricates an information by stating in an article published in his blog that Z, a well-known businessman has obtained a business contract by offering bribes. B, knowing that the information has been fabricated shares the article on his social media account. Both A and B are guilty of an offence under this section.
 - d) A publishes an advertisement containing a caricature of Z depicting Z as a successful investor is an investment scheme knowing that Z is not involved in the investment scheme. A is guilty of an offence under this section.
 - e) A publishes a statement in his social media account that a food product of Z's company contains harmful ingredients and is being sold to the public knowing that the production of the food product has been discontinued several years ago and the food product is no longer sold to the public. A is guilty of an offence under this section.
 - f) A creates a website impersonating a Government agency's website. In the website, A publishes a guideline purportedly issued by the Head of the Government agency which requires the public to apply for a license to carry out a particular activity. There is no such guideline issued by the Government agency. A is guilty of an offence under this section.

Anti-Fake News Act (repealed)

Always A Pioneer, Always Ahead

- Section 4 sets out some illustrations where the offence under Section 4 would apply:
 - g) A gives a speech during a public forum held at a public place. In his speech, A informs that Z has misappropriated moneys collected for charitable purposes knowing that the information is false. A is guilty of an offence under this section.
 - h) A holds a press conference where he claims that Z, an owner of a supermarket, will give out free gifts to the first one hundred customers of his supermarket on every first Saturday of the month knowing that Z has no intention to do as claimed by A. A is guilty of an offence under this section.
- A person found guilty would be liable to a fine not exceeding RM500,000 or to an imprisonment for a term not exceeding six years or to both, and in the case of a continuing offence, to a further fine not exceeding RM3,000 for every day during which the offence continued after conviction.
- The court may, in addition to any punishment specified in Section 4(1), order the person convicted of an offence under that subsection to make an apology to the person affected by the commission of the offence in the manner determined by the court. Failure to comply with such an order would be punishable as a contempt of court.

Anti-Fake News Act (repealed)

Always A Pioneer, Always Ahead

- It was reported that one Salah Salem Saleh Sulaiman was charged and punished under Section 4(1) of the AFNA, which carried a punishment of up to six years in prison and a fine of up to RM500,000, for maliciously publishing fake news in the form of a YouTube video under the user name “Salah Sulaiman”. He pleaded guilty and was sentenced to one week’s imprisonment and was fined RM10,000.



<https://www.reuters.com/article/us-malaysia-palestinian-fakenews-idUSKBN111019>

First person convicted under Malaysia's fake news law

Danish national wrongly accused police of slow response after Palestinian lecturer was killed



▲ Salah Salem Saleh Sulaiman, a Danish national, is escorted by police to a court in Kuala Lumpur. Photograph: AP

A Malaysian court has convicted a Danish citizen over inaccurate criticism of police on social media, the first person to be prosecuted under a new law

<https://www.theguardian.com/world/2018/apr/30/first-person-convicted-under-malaysias-fake-news-law>

Anti-Fake News Act (repealed)

Always A Pioneer, Always Ahead

KUALA LUMPUR: Royal College of Surgeons of Edinburgh (RCSEd) mengesahkan Tan Sri Dr Noor Hisham Abdullah menerima anugerah 'Fellowship Ad Hominem' daripada pihak mereka pada Oktober 2017.

Menerusi surat bertarikh semalam, RCSEd turut mengesahkan Ketua Pengarah Kesihatan itu menerima anugerah berkenaan daripada Presiden RCSEd, Mike Lavelle-Jones, pada 2 Februari 2018.

Salinan surat yang dimuat naik di Facebook Dr Noor Hisham hari ini sekali gus menafikan **dakwaannya menghadiri upacara Freemasons dan keagamaan** yang disifatkannya sebagai tidak benar serta fitnah.

"Penyebaran fitnah melalui media sosial dalam kalangan masyarakat masa kini semakin berleluasa dan sukar ditangani.

RCSEd sahkan Dr Noor Hisham terima anugerah 'Fellowship Ad Hominem'

Muhammad Yusri Muzamir - Mei 22, 2021 @ 1:50pm
yusri.muzamir@bh.com.my



AD HOMINEM FELLOWSHIP AWARD BY THE ROYAL COLLEGE OF SURGEONS OF EDINBURGH

The Royal College of Surgeons of Edinburgh is the oldest Surgical College in the world, with ca. 30,000 members in 100 countries. The College's primary role is to ensure the safety of patients by championing the highest standards of surgical and dental practice through the provision of courses, training, examinations, and Continuous Professional Development.

The Fellowship Ad Hominem is one of the highest awards given by the College, granted to current or former medical practitioners or other individuals of distinction whose professional status is of a high order and who are deemed worthy of the honour. The distinction is formally awarded at a ceremony attended by members of the College. During the event, the recipients wear the College ceremonial gown and are presented with their diploma by the President.

Dr Noor Hisham Abdullah was awarded a Fellowship Ad Hominem by the Royal College of Surgeons of Edinburgh's Awards Committee on 12 October 2017. This award was subsequently presented to him by the President of the College, Mr Mike Lavelle-Jones, on 2 February 2018. He received this award in his capacity as Director-General of Health, Malaysia, in recognition of his achievements in the medical and surgical field, and of his support to the College for many years.

Thank you.

MARINETTE NAUO-BETTERIDGE
Head of International Engagement
For RCSEd International Office, Malaysia

21st May 2021

Tan Sri Dr Noor Hisham Abdullah menerima anugerah 'Fellowship Ad Hominem' daripada RCSEd pada Oktober 2017.

<https://www.bharian.com.my/berita/nasional/2021/05/819487/rcsed-sahkan-dr-noor-hisham-terima-anugerah-fellowship-ad-hominem>

Anti-Fake News Act (repealed)

Always A Pioneer, Always Ahead

Maliciously

- The Anti-Fake News Bill 2018 tabled for its first reading in Parliament used the word “knowingly” but that was later replaced with the word “maliciously”. The word “maliciously” was not defined in the Act. The Black’s Law Dictionary – Free Online Legal Dictionary defines malice as “carrying out intentionally of an injurious and harmful act with no cause or justification” and “malicious act” is defined as “a term referring to doing an intentionally wrong act”. While West’s Encyclopaedia of American Law defines “malicious” as “involving malice; characterized by wicked or mischievous motives or intentions; an act done maliciously is one that is wrongful and performed willfully or intentionally and without legal justification.”
- The word “maliciously” should not be equated with the word “maliciously” in section 8A of the Printing Presses and Publications Act 1984 (offence to publish false news). This is because section 8A(2) provides that “malice shall be presumed in default of evidence showing that, prior to publication, the accused took reasonable measures to verify the truth of the news”. The degree of proof under the Anti-Fake News Act 2018 was higher because the prosecution **had to prove that the act was done intentionally and had brought injuries or harm.**

Anti-Fake News Act (repealed)

Always A Pioneer, Always Ahead

Order for removal of publication containing fake news

- Under section 7 of the Anti-Fake News Act 2018, a person affected by any publication containing fake news could apply to the Sessions Court for an ex parte order declaring that the publication was fake news. The application had to be made in the form prescribed in the First Schedule of the Act and accompanied by a police report and other documents supporting such application. If the court was satisfied that the publication contained fake news, the court may make an order, in the form prescribed in the Second Schedule, for the removal of such publication.
- The order made under section 7 could contain the following particulars:
 1. the person who was required to remove the publication containing fake news;
 2. the manner of the removal of the publication containing fake news;
 3. the time within which the publication containing fake news shall be removed after the service of the order; and
 4. any other order as the court deemed fit.

Anti-Fake News Act (repealed)

Always A Pioneer, Always Ahead

Order for removal of publication containing fake news

- Any person who failed to comply with the order made under section 7 committed an offence and, on conviction, was liable to a fine not exceeding RM100,000. If the person against whom the order was made under section 7 failed to remove the publication containing fake news, the court could, on an application by the Public Prosecutor, make an order directing the police or an authorised officer under the CMA 1998, as the case may be, to take the necessary measures to remove such publication. **The word “remove” was not defined**; it could cover removal from access by the public, that is, blocked from access by members of the public.
- The outcome of an order to remove a publication containing fake news would be **unsatisfactory** if the person required to remove the fake news was outside Malaysia and ignored or refused to comply with the order on the ground that, among others, they were not subject to the laws of Malaysia.
- Section 9 of the Anti-Fake News Act 2018 gave power to the court, on an application by the Public Prosecutor, to direct a police officer or an authorised officer under the CMA 1998 to take the necessary measures to remove the publication. This **was also unsatisfactory** as the person affected by the fake news had to rely on the Public Prosecutor to take action. In this regard, such person **may have considered** filing a request with the MCMC to **request a blocking order under section 263** of the CMA 1998.

Anti-Fake News Act (repealed)

Always A Pioneer, Always Ahead

Setting aside the order for removal

- Under section 8 of the Anti-Fake News Act 2018, the person against whom an order under section 7 was made could apply to set aside the order within 14 days from the date the order was served on him. An application to set aside the order did not amount to a stay of the order for removal under section 7.
- If an order under section 7 was obtained by the government relating to a publication containing fake news which was prejudicial or likely to be prejudicial to public order or national security, there could not be an application for the setting aside of such order by the person against whom the order was made.

Repeal of the Anti-Fake News Act 2018

- After some opposition, the law was repealed via the Anti-Fake News (Repeal) Act 2020, with **effect from January 31, 2020**.
- Notwithstanding the repeal, **section 233 of the CMA 1998** and **section 505(b) of the Penal Code** may be used to combat online fake news. In 2020, section 505(b) was used to charge a journalist for posting alleged fake news relating to the spread of Covid-19 in Malaysia on her Facebook account.

Anti-Fake News Act (repealed)

Always A Pioneer, Always Ahead

Critique*

- “Fake news” is ambiguously defined. A person may be imprisoned or fined without the Government needing to prove that their expression caused harm to any legitimate interest, or that the person intended that harm to occur. It **essentially grants unfettered discretion to authorities to target expression they dispute the veracity of, or simply do not like**. As such, its content-based offences are much broader than those that already exist in legislation like the Sedition Act, Communications and Multimedia Act, or Penal Code.
- The Act also **co-opts online intermediaries**, such as search engines and social media platforms, in addition to administrators or owners of social media pages, into the Government’s censorship efforts. Criminal penalties **create strong incentives for the removal of content the Government may object to**, without regard to human rights, and without transparency or due process.
- Where a person is “in control of” so-called “fake news”, they **must remove so-called “fake news” on notice**, and **without a court order**. Failure to do so “immediately” is criminalised. In addition, the courts are given sweeping powers to demand private parties, on request of users or the executive, remove entire publications containing “fake news”, with severe fines for non-compliance.

Anti-Fake News Act (repealed)

Always A Pioneer, Always Ahead

Critique*

- These **ex-parte proceedings require no consideration of human rights**, and in many cases individuals' content will be removed without their being notified or having any opportunity to make representations, and with appeal rights limited only to the respondent to an order (and not necessarily available for authors or owners of offending content). **On matters pertaining to national security and public order, there is no right to appeal, giving the government broad powers to request removals without the possibility of challenge.**
- The **jurisdictional scope of the Act extends beyond Malaysia's territory**, allowing for the targeting of any person or entity if the expression concerns Malaysia or affects Malaysians. The potential impact of the Act on freedom of expression is therefore truly global.
- The **rapid enactment of the Act ahead of elections, without any effective public consultations**, raises significant concerns regarding the protection of freedom of expression in Malaysia in the months ahead. The criminal offences it contains, and the regime of intermediary liability it paves the way for, is likely to have a significant chilling effect on open debate, in particular on criticism of the government, and especially online. As Malaysians go to the polls, they are clearly being told that opposition and criticism will not be tolerated.

Anti-Fake News Act (repealed)

Always A Pioneer, Always Ahead

Recommendations*

- The Malaysian Government should comprehensively reform other laws that unjustifiably limit the right to freedom of expression, in particular by repealing the Sedition Act and reforming the Communications and Multimedia Act;
- The Malaysian Government should enact legislation to protect online intermediaries, such as search engines and social media companies, from criminal and civil liability for content that third parties create or share on or through their platforms;
- The Malaysian Government should ratify the International Covenant on Civil and Political Rights (ICCPR) without delay.

*<https://www.article19.org/resources/malaysia-anti-fake-news-act/>

Definition

Cloud Computing is defined as a large-scale distributed computing paradigm. It is becoming an important topic for businesses and organizations, where different types of services are provided in a competitive time frame over the internet, which accelerates operating the businesses to deliver faster and to scale up in a competitive timeframe. Cloud Computing offers Cost Reduction (pay-per-use), Maintenance, Enhance Productivity, Scalability, and Elasticity for Businesses.

Service Models

- **Infrastructure as a Service (IaaS):** in this type, infrastructure is provided as a service to clients, where the client handles all software and application installed on the provided infrastructure. The usage time of CPU is measured, and the storage usage and data transfer are measured per gigabyte.
- **Platform as a Service (PaaS):** By Using PaaS, the clients develop their application on the provided platforms and toolkits that are hosted by the Cloud.
- **Software as a Service (SaaS):** The client in this model will be using the Software that is provided and hosted

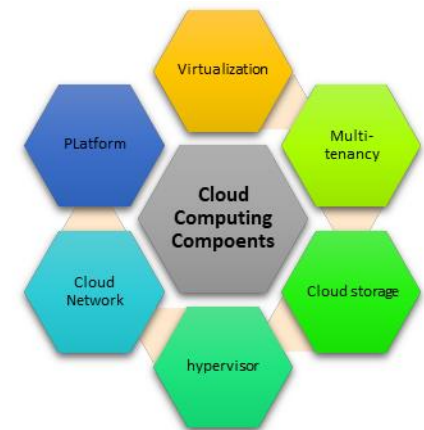
Cloud deployment

- **Private Cloud:** this Model delivers services from a business's data center to a specific organization and the organization members only. Other organization cannot access the services
- **Public Cloud:** in this Model, the services are given by specific provider and mostly being used on the basis of pay per use. In addition, the third party will manage the resources and services across organizations
- **Hybrid Cloud:** This model offers a combination of public cloud services and private cloud, with orchestration and automation between the two

Cloud computing components:

- 1) **Virtualization:** Creates the virtual instance of the resource such as operating system, servers,.etc.
- 2) **Multi-tenancy:** Shares multi customers and users resources or applications to optimal utilization.
- 3) **Cloud storage:** Maintained, managed, and backed up storage remotely

- 4) **The hypervisor:** Run on a single hardware host to manage and monitors the various operating systems.
- 5) **Cloud Network:** Provides the connectivity over the datacenters and the internet
- 6) **Platforms:** Environment setup and tools.



Legal and regulatory challenges

- **Applicable law and jurisdiction:** The issue is related to the identification of Cloud Computing applicable rules, policies, regulations and laws and competent jurisdictions for the provided services in the related counties and regions. This can be addressed mainly by the geographical location of the stakeholders involved, and the rights and obligations of each stakeholder are determined by applicable regulations in the relevant country. There might be also some special regulations or polices or rules to handle the data flow across borders and the different related jurisdictions to craft rules.
- **Handling disputes in the cloud:** This issue addresses the accountability between the different entities and how to handle the reinforce trust between customs and Cloud Computing services providers. Due to the nature and unique characteristics of Cloud Computing services, it might be difficult to identify the competent related jurisdiction between countries and regions. This issue has been handled in some regions like in Europe by assigning a specific regulator entity who can handle the disputes, but still, this is inside Europe and not comprehensive and not applicable outside Europe.



Legal and regulatory challenges

- **Politics and Governments Relationships:** This issue addresses the changes of the governments' relationships and politics between countries and the effect of the relationship changes on the Cloud Computing that serves the relevant countries and the scope of the regulation and the laws to govern these changes. An example for this: if the relationship between two counties has been suspended due to some political issues or others, and if the Cloud Computing Services Provider is in one of the counties and the client is in the other, what will happen and what regulations and law are there to protect the both client's and the service provider's rights? One of the solutions for this is to have an independent regulatory that govern the Cloud Computing worldwide, however this need a lot of efforts and international interference to establish this governance body and to craft the rules and regulations related to Cloud Computing services.



Internet of Things (IoT)

Always A Pioneer, Always Ahead

- Over the past few years, the Internet of Things (IoT) market has been experiencing explosive growth. According to Gartner, there will be 25 billion connected devices by 2021. Statista research suggests the total installed base of smart devices, such as smart TVs, smart locks, IP cameras, home assistants and their associated services, in homes around the world, **will reach 75 billion units by the end of 2025**, a five-fold increase in ten years. This rise in the number of IoT devices dramatically **increases potential vector points for cyberattacks and creates a massive security gap**.
- The challenge we all face is that **these devices have weak or no security controls and represent the fastest-growing attack landscape** for organizations all over the world, with attacks up 300% in 2019 alone. Cybercriminals exploit multiple vulnerabilities in smart devices and often use them to get access to entire networks. To strengthen the security of connected products, governments around the world are continuously working on the development of new legislation.
- Industry, in general, is feeling the **global push for robust IoT security standards**. Currently, the UK and Australia are world leaders when it comes to IoT security, with both nations **already enacting voluntary standards for consumer IoT devices**. In January 2020, in the USA, both California and Oregon introduced new legislation requiring “reasonable security features” to be added to IoT devices.

Fitness tracking app Strava gives away location of secret US army bases

Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities

- Latest: Strava suggests military users 'opt out' of heatmap as row deepens



▲ A military base in Helmand Province, Afghanistan with route taken by joggers highlighted by Strava. Photograph: Strava Heatmap



<https://www.news.com.au/technology/gadgets/wearables/fitness-tracking-apps-expose-activity-on-sensitive-military-bases/news-story/2e54eab1bb849fc49bf21b52fd1c22c8>

<https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>

California's IoT Security Law

- At its core, California's IoT security law mandates that all **connected devices** be equipped with "**reasonable security features**" to "protect the device and any information contained therein from **unauthorized access, destruction, use, modification, or disclosure.**"
- The **definition** of "**connected device**" is **extremely expansive**, as the law defines the term as "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address." This broad definition casts an extremely wide net; wide enough to encompass essentially all devices that are part of the IoT universe, including fitness trackers, connected cars, and smart home devices such as Google Home and Amazon Echo.
- **Reasonable security features** are defined as those that are:
 1. Appropriate to the nature and function of the device;
 2. Appropriate to the information the device may collect, contain, or transmit; and
 3. Designed to protect the device, and any information contained therein, from
 4. unauthorized access, destruction, use, modification, or disclosure.

California's IoT Security Law

- Although the law does not provide any discussion of what constitutes “reasonable security features,” it does provide that if a device can be accessed outside a local area network with a password, it will be deemed to have a “reasonable security feature” if the device is equipped with a unique password for each device, or requires users to generate their own password before they can access the device. As such, the California IoT law marks the end of generic default credentials. Importantly, however, the scope of the law is limited to the issue of authentication. Outside of that, the law merely mandates undefined, indeterminate “reasonable security features” as it relates to IoT devices.
- The California IoT security law is also short on specifics around enforcement, providing only that it does not provide a basis for a private right of action and that enforcement authority is possessed exclusively by the California attorney general, as well as city, county, and district attorneys. Yet despite the lack of a statutory private right of action, it is expected that the Plaintiff's bar will nevertheless point to the California IoT law as a basis to bring consumer class actions in which the law is deemed to set the industry standard for “reasonableness” in a suit alleging negligence.

California's IoT Security Law

- Although the ultimate impact of the law remains uncertain, enforcement of California's IoT security law has the potential to significantly expand IoT manufacturers' scope of liability exposure, including precluding certain IoT makers from operating in some of the largest markets.
- Please refer to The Rise of Internet of Things Security Laws Part 1 & 2 for more discussion.

UK's IoT Cybersecurity Law

- In January 2020, the UK government announced it is going to introduce new mandatory requirements for IoT device manufacturers in an effort to improve consumer data security. The aim is **to move the responsibility away from consumers** to secure their own devices by ensuring strong cybersecurity is built into these products by design.
- According to the proposed law, **all consumer smart devices sold in the UK** should adhere to a **basic level of security**. This includes **three main requirements**: passwords for all connected devices must be unique, manufacturers must provide a public point of contact to report vulnerabilities, and a minimum period of security updates must be specified when sold.

Malaysia Case

- Blockchain technology is commonly used today in cryptocurrencies. The distributed ledger and proof-of-work system behind blockchain **allow remittance of cryptocurrencies across international jurisdiction without reliance on an intermediary such as bank** at a much faster rate and cheaper fees than conventional inter-bank transfer and without the need for the parties to divulge personal details except for their respective unique alphanumeric public keys.
- The multiple independent nodes in the blockchain system ensure a self-sustaining environment for the digital currencies and **eliminate meddling from the government** where such meddling may sometimes lead to devaluation in currencies as documented by history.
- However, beyond the blockchain ecosystem, cryptocurrencies are **susceptible to certain drawbacks**. As an open source technology, **anyone who is savvy enough can create and deploy his/her own version of cryptocurrencies**. Ever since the launch of Bitcoin by the elusive Satoshi Nakamoto, there are numerous other cryptocurrencies being launched with **aggregate market capitalisation averaging between USD 120 to 140 billion as of February 2019**.
- New launches of cryptocurrencies in the form of initial coin offering (“ICO”) **allows investors from all over the world (with internet connection, of course) to purchase newly minted currencies** with either fiat or existing cryptocurrencies in hope of appreciation in value of such new currencies upon implementation of the underlying project and listing on the cryptocurrencies exchange.

Malaysia Case

- Unfortunately, more often than not, **these ICO projects fail and abandoned, together with all monies raised from the investors. The fact that the company behind these ICO projects does not have physical presence in the country of the respective investors hinders the recovery of the money lost by the respective investors.** Even if the ICO projects may be promising and legit, investors could lose their investment when such cryptocurrencies traded on digital cryptocurrencies exchange is compromised by hackers as seen in the case of Mt. Gox or in a more absurd scenario, the death of the CEO as seen in the case of QuadrigaCX who purportedly being the only person with access to its customers' cryptocurrencies stored in cold storage.
- Against this backdrop, **it is paramount to have blockchain law in Malaysia regulate activities relating to cryptocurrencies** particularly issuance of cryptocurrencies and establishment of cryptocurrencies exchange in the interest of general investing public.

Malaysia Regulatory Framework

- The Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 (“**POS Order**”) which is in force with effect from 15 January 2019 widens the scope of “securities” under the **Capital Markets and Services Act 2007** (“CMSA”) to cover digital currencies and digital tokens. This effectively means that **issuance of blockchain based digital currencies and digital tokens which are not issued or guaranteed by any government body or central bank, and fulfils the prescribed criteria, are subject to approval by the Securities Commission Malaysia (“SC”).**
- As at the time of writing, the SC has announced that in view of the POS Order, **no person shall conduct an ICO without the prior authorisation of the SC and the guidelines for ICOs will be issued by the end of Q1 2019.** Until issuance of such guidelines for ICOs, ongoing ICOs should cease all activities and return all monies or digital assets collected from investors.
- Pursuant to the CMSA, **any person who make available, offer for subscription or purchase, or issue an invitation to subscribe for or purchase unlisted capital market products** (which includes securities and by virtue of the POS Order includes digital currency and digital token) and **fails to obtain authorization from the SC commits an offence and shall on conviction, be punished with imprisonment for a term not exceeding ten (10) years and be liable to a fine not exceeding RM3,000,000.**

Malaysia Case

HOME / MALAYSIA

Securities Commission: All LaVida Coin promotional activities must cease immediately

Wednesday, 05 Sep 2018 08:42 PM MYT



The cryptocurrency was launched by cosmetic queen Datuk Seri Hasmizah Othman, also known as Datuk Seri Vida. — Picture by Choo Choy May

Subscribe to our [Telegram](#) channel for the latest updates on news you need to know.

<https://www.malaymail.com/amp/news/malaysia/2018/09/05/securities-commission-all-lavida-coin-promotional-activities-must-cease-imm/1669696>

Lavida Coin masuk senarai Amaran Pengguna Kewangan Bank Negara



Azzman Abdul Jamal - Ogos 29, 2018 @ 6:20pm
azzman@nstp.com.my



KUALA LUMPUR: Bank Negara Malaysia menyenaraikan pengendali terbitan mata wang kripto Lavida Coin, VI Profit Galaxy (DSV Cryptoclub & LUX Galaxies) dalam senarai Amaran Pengguna Kewangan bank

<https://www.bharian.com.my/bisnes/lain-lain/2018/08/467521/lavida-coin-masuk-senarai-amaran-pengguna-kewangan-bank-negara>

Malaysia Regulatory Framework

- The enactment of the POS Order therefore restricts the establishment and operation of cryptocurrencies exchange in Malaysia as section 7 of the CMSA prohibits the operation of a stock markets other than (amongst other) a stock market of a stock exchange or a recognized market. Approximately 15 days later after the enactment of the POS Order, the SC then revised the Guidelines on Recognized Markets to include digital assets exchanges (being electronic platform which facilitate the trading of digital currency and digital token) as a recognized market. With that, any person intending to operate cryptocurrencies exchange is required to be registered with the SC as a recognized market operator and comply with certain criterias.
- In addition to the above blockchain law in Malaysia, BNM has also imposes requirement on cryptocurrency exchanges in Malaysia to register itself as a reporting institution pursuant to the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001. BNM has issued the “Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Digital Currencies (Sector 6)” policy document on 27 February 2018 which specifies further detailed requirements imposed on such reporting institutions which includes an obligation to submit a declaration in respect of its business to BNM.

Conclusion – Blockchain Law in Malaysia

- The regulation of the blockchain law in Malaysia and/or cryptocurrencies should be welcomed as it provides much certainty and protection to general investing public.
- However, it remains to be seen whether the existing and future regulatory framework will **spur or stifle the growth of blockchain technology in Malaysia**. As the blockchain technology is still in its pioneering stage and much of its application is still being discovered, **regulating in advance may stifle further innovation**.
- On the hand, regulators must ensure that the legislative process can catch up with the rapid innovation in blockchain technology.

- One of the biggest problem cyber law is encountering is related to development of **jurisprudence relating to social networking**. Increased adoption and usage of social media are likely to bring various legal, policy and regulatory issues. Social media crimes are increasingly gaining attention of relevant stake holders. Misuse of information, other criminal and unwanted activities on social networking platforms and social media are raising significant legal issues and challenges.
- There is a need for the countries across the world **to ensure that rule of law prevails on social media**. Social media legal issues continues to be significant. In order to avoid social media crimes and protect the privacy related to social media, it is **a challenge for cyber law makers across the world to not only provide appropriate legislative and regulatory mechanisms but also provide for effective remedies for redressal to the victims of various unauthorized, unwanted criminal activities done in cyber space and social media**.



Self-governance

- YouTube releases a [transparency report](#), which gives data on its removals of inappropriate content.
- The video-sharing site owned by Google said that 8.8m videos were taken down between July and September 2019, with 93% of them automatically removed by machines, and two thirds of those clips not receiving a single view.
- It also removed 3.3 million channels and 517 million comments.
- Globally, YouTube employs 10,000 people in monitoring and removing content, as well as policy development.
- Facebook, which owns Instagram, told Reality Check it has more than 35,000 people around the world working on safety and security, and it [also releases statistics](#) on its content removals.
- Between July and September 2019 it took action on 30.3 million pieces of content of which it found 98.4% before any users flagged it.
- If illegal content, such as "revenge pornography" or extremist material, is posted on a social media site, it has previously been the person who posted it, rather than the social media companies, who was most at risk of prosecution.
- <https://transparencyreport.google.com/youtube-policy/removals?hl=en> , <https://transparency.facebook.com/community-standards-enforcement>

Germany

- Germany's **NetzDG law** came into effect at the beginning of 2018, applying to companies with more than two million registered users in the country.
- They were **forced to set up procedures to review complaints about content they were hosting, remove anything that was clearly illegal within 24 hours and publish updates every six months about how they were doing.**
- Individuals may be fined up to €5m (\$5.6m; £4.4m) and companies up to €50m for failing to comply with these requirements.
- The government **issued its first fine under the new law to Facebook in July 2019.** The company had to pay €2m (£1.7m) for under-reporting illegal activity on its platforms in Germany, although the company complained that the new law had lacked clarity.

European Union (EU)

- The EU is considering a clampdown, specifically on terror videos.
- Social media platforms face fines if they do not delete extremist content within an hour.
- The EU also introduced the General Data Protection Regulation (GDPR) which **set rules on how companies, including social media platforms, store and use people's data**.
- It has also taken action on copyright. Its copyright directive puts the responsibility on platforms to make sure that **copyright infringing content is not hosted on their sites**.
- **Previous legislation only required the platforms to take down such content if it was pointed out to them.**
- Member states have until 2021 to implement the directive into their domestic law.

<https://www.bbc.co.uk/news/technology-45247169> <https://www.bbc.co.uk/news/technology-45495550>

Australia

- Australia passed the Sharing of Abhorrent Violent Material Act in 2019, introducing criminal penalties for social media companies, possible jail sentences for tech executives for up to three years and financial penalties worth up to 10% of a company's global turnover.
- It followed the [live-streaming of the New Zealand shootings](#) on Facebook.
- In 2015, the **Enhancing Online Safety Act** created an eSafety Commissioner with the power to demand that social media companies take down harassing or abusive posts. In 2018, the powers were expanded to include revenge porn.
- The eSafety Commissioner's office can issue companies with 48-hour "takedown notices", and fines of up to 525,000 Australian dollars (£285,000). But it can also fine individuals up to A\$105,000 for posting the content.
- The legislation was introduced after the death of Charlotte Dawson, a TV presenter and a judge on Australia's Next Top Model, who killed herself in 2014 following a campaign of cyber-bullying against her on Twitter. She had a long history of depression.

<https://www.bbc.co.uk/news/business-47620519>

Russia

- [A law came into force in Russia in November](#) giving regulators the power to switch off connections to the worldwide web "in an emergency" although it is not yet clear how effectively they would be able to do this.
- Russia's data laws from 2015 required social media companies to store any data about Russians on servers within the country.
- Its communications watchdog [blocked LinkedIn](#) and fined Facebook and Twitter for not being clear about how they planned to comply with this.
- <https://www.bbc.co.uk/news/world-europe-50259597> <https://www.bbc.co.uk/news/technology-38014501>

China

- Sites such as Twitter, Google and WhatsApp are blocked in China. Their services are provided instead by Chinese providers such as Weibo, Baidu and WeChat.
- Chinese authorities have also had some success in restricting access to the virtual private networks that some users have employed to bypass the blocks on sites.
- [The Cyberspace Administration of China announced at the end of January](#) 2019 that in the previous six months it had closed 733 websites and "cleaned up" 9,382 mobile apps, although those are more likely to be illegal gambling apps or copies of existing apps being used for illegal purposes than social media.
- China has hundreds of thousands of cyber-police, who monitor social media platforms and screen messages that are deemed to be politically sensitive.
- Some keywords are automatically censored outright, such as references to the 1989 Tiananmen Square incident.
- New words that are seen as being sensitive are added to a long list of censored words and are either temporarily banned, or are filtered out from social platforms.

http://www.cac.gov.cn/2019-01/23/c_1124032637.htm

India

- The basis for enforcement and enactment of the Information Technology Act, 2000 was to provide recognition to e-commerce and e-transactions and also to protect the users from digital crimes, piracy etc.
- The Ministry of Electronics and IT has prepared the Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 (hereinafter referred to as "2018 Rules") in order to prevent spreading of fake news, curb obscene information on the internet, prevent misuse of social-media platforms and to provide security to the users.
- The Information Technology (Intermediaries Guidelines) Rules, 2011 (hereinafter referred to as "2011 Rules") created a lot of heat waves in the digital world with regard to the duties and liabilities of the intermediaries even after safe harbor protection provided under Section 79 of the Information Technology Act, 2000 (hereinafter referred to as "the Act").
- Section 79 of the Act provided that the Intermediaries or any person providing services as a network service provider are exempted from the liabilities in certain instances.
- In 2018, the government has come out with certain changes in the 2011 Rules and has elaborately explained the liabilities and functions of the Intermediaries and to oversee that the social media platform is not misused.

- The Rule 2018 categorically specifies that the intermediaries must inform to the users of the computer resource about the Rules and regulations and privacy policy so as to not to host, display, upload, modify, publish, transmit, update or share any information which might affect public health and safety and Critical Information structure. No such provision was present in the Draft Rule 2011 and it is observed that the government is taking necessary and needful steps time and again to aware people about the detrimental effects of consumption of cigarettes and intoxication. It is an important step taken towards public safety as social media platform is one of the most common platform used by every sections of the society as well as by every age group. The government has also taken an initiative to protect critical information structure against cyber terrorism, cyber warfare and other threats.

Spam

Always A Pioneer, Always Ahead

- In the initial years, spam seemed to be targeted at computers but has now also targeted mobile phones. Email spam is the most common form of spamming, Mobile phone spam and instant messaging spam also exist. In **majority of the countries there is no such anti spam law**, which has led to the further growth of spam. There is an increased need for the countries to come up with regulatory and legal framework for spam as many countries have already become **hotspots for generating spam**.

8	United Kingdom	Number of Current Live Spam Issues: 498
9	Turkey	Number of Current Live Spam Issues: 413
10	Brazil	Number of Current Live Spam Issues: 402

The 10 Worst Spam Countries		
As of 22 March 2020 the world's worst Spam Haven countries for enabling spamming are:		
1	China	Number of Current Live Spam Issues: 3735
2	United States of America	Number of Current Live Spam Issues: 3083
3	Russian Federation	Number of Current Live Spam Issues: 1141
4	Ukraine	Number of Current Live Spam Issues: 712
5	India	Number of Current Live Spam Issues: 627
6	Japan	Number of Current Live Spam Issues: 551
7	Hong Kong	Number of Current Live Spam Issues: 503

- An Overview of Section 233 of the CMA 1998 ... "A person who initiates a 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."
- The intent underlying Section 233(1)(b) may be utilised to deal with unsolicited communications. It may be an appropriate section to deal with the problems faced by spamming activities.
- Notwithstanding, to fall within the scope of the section however the communication must have been initiated with the intention of annoying, abusing, threatening or harassing a person. In cases of spamming, the consequences or effect of such communication may be that the recipients are annoyed, harassed or abused.

- However, it may be difficult to argue that this was the **intention of the sender**. The requirement or kind of "intent" the section requires may not always exist or be difficult to determine.
- This may give rise to enforcement problems, bearing in mind that the onus of proof is on the prosecution. Further, such intention may not exist given that people who initiate such communication for marketing and advertising purposes are unlikely to initiate such communication with the intent to annoy abuse, threaten or harass potential clients.
- **Section 233**, however, may be seen as being **inadequate in some aspects**, for instance:
 - There are NO provisions in this section that allow a person to opt in or opt out to receive unsolicited Internet e-mail or short messages;
 - There is NO requirement that all electronic messaging contains accurate details of the sender's name and address;
 - There are NO civil sanctions for unlawful conduct including financial penalties and ability to seek enforceable undertakings and injunctions to minimize the proliferation of spamming.

Cybersecurity and related issues

Always A Pioneer, Always Ahead

- It is impossible to argue the importance of Cybersecurity Law at this time and age. There was a [survey](#) which found that on average, Malaysians spend **around 8 hours and 5 minutes** using the internet via any device.
- We rely heavily on the internet and various other online applications day in and out, to deal with our finances, shopping, corresponding, news-reading and many other activities, it is no wonder that criminals or misusers would be tempted to seek for their target in the cyber world, and such misdemeanors are often motivated by financial gains, revenge, or even curiosity or apathy.
- While Malaysia does have a number of sporadic laws in some areas of cybercrime, more specific laws that deals with issues like **phishing**, and **spamming** as well as specific laws dealing with other new technologies like **AI, IoT, cloud computing, blockchain** are still lacking.
- Furthermore, more effort must be taken to ensure that Malaysia's Critical National Infrastructure (CNI) and Critical National Information Infrastructure (CNII) are secure from any types of cyberattacks.
- It is hoped that the new proposed Cybersecurity Law for Malaysia will be introduced soon. Many countries around the world have enacted their own Cybersecurity Laws like Germany, China and the Czech Republic.

Case Study: [Singapore Cybersecurity Act](#)

- The Cybersecurity Bill was passed on 5 Feb 2018 and received the President's assent on 2 Mar 2018 to become the Cybersecurity Act. The Act establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore. Its four key objectives are to:
 - Strengthen the protection of Critical Information Infrastructure (CII) against cyber-attacks.
 - Authorise Singapore Cybersecurity Agency (CSA) to prevent and respond to cybersecurity threats and incidents.
 - Establish a framework for sharing cybersecurity information.
 - Establish a light-touch licensing framework for cybersecurity service providers

Case Study: [Germany IT Security Law 2.0](#)

- **Main intention:** Further development of cybersecurity for the society as a whole.
- Not only protection of Critical Infrastructures, but for all relevant companies and the state, as well as for consumers, including IoT products.
- **Co-regulation** of EU Cybersecurity Act and German IT Security Law 2.0 in certain fields of interest (it can be assumed that the German regulator influenced the European cyber legislation).

<https://www.csa.gov.sg/legislation/cybersecurity-act> <https://cert.vde.com/de-de/news/presentation-it-sig-2-0-eng.pdf>

Cybersecurity and related issues (cont...)

Always A Pioneer, Always Ahead

- Core elements of the new regulatory approach include:
 - **Protection of citizens: Unified IT security mark, so that a higher visibility for IT security can be reached especially for consumer products/applications**
 - **Extensions of the legal power of the German BSI, as well as for criminal prosecution authorities to fight against cybercrime**
 - **Extensions in the German Criminal Code and the German Criminal Prosecution Code**
 - **New cybersecurity duties especially for providers, e.g. concerning the deletion, reporting, and the provision of information regarding cybercrime issues**
 - **More and effective cooperation among authorities to deal with cybercrime**
 - **Amended regulations for operators of Critical Infrastructures**

Cybersecurity and related issues (cont...)

Always A Pioneer, Always Ahead

Elephant in the Room

On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack. We have since determined that this incident involves ransomware. In response, we **proactively took certain systems offline** to contain the threat, which has temporarily **halted all pipeline operations**, and **affected some of our IT systems**.



Tim Conway

SANS

SANS ICS | sans.org/ics


10

20

Cybersecurity and related issues (cont...)


Always A Pioneer, Always Ahead

Colonial Pipeline Details



- Largest refined products pipeline in the US
- Moves 100 million gallons of fuel daily across 5,500 miles of pipeline
- Over 280 facilities and field terminals, transporting 45% of the fuel to the East Coast
- On Friday May 7th Colonial temporarily shut down all pipeline operations due to a ransomware attack on its IT business systems

Tim Conway



SANS

SANS ICS | sans.org/ics

2021-05-13 11:08:50

Cybersecurity and related issues (cont...)

Always A Pioneer, Always Ahead

```
sophos_READ [REDACTED].TXT - Notepad
File Edit Format View Help
----- [ Welcome to DarkSide ] ----->

What happend?
-----
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.

Data leak
-----
First of all we have uploaded more then 140GB data.

These files include:
- Accounting
- Research & Development

Your personal leak page: http://darksid[REDACTED]
On the page you will find examples of files that have been stolen.
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.

We are ready:
- To provide you the evidence of stolen data
- To delete all the stolen data.

What guarantees?
-----
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.

How to get access on website?
-----
Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://darksid[REDACTED]

When you open our website, put the following data in the input form:
Key:
```



Cybersecurity and related issues (cont...)

Always A Pioneer, Always Ahead

DarkSide Ransomware

Let's start

10.03.2020

We are a new product on the market, but that does not mean that we have no experience and we came from nowhere. We received millions of dollars profit by partnering with other well known cryptolockers. We created DarkSide because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that develop and participate (to a large extent) in the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business. Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income. You can ask all your questions in the chat before paying and our support will answer them.

We provide the following guarantees for our targets:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

If you refuse to pay:

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will NEVER provide you decryptors.

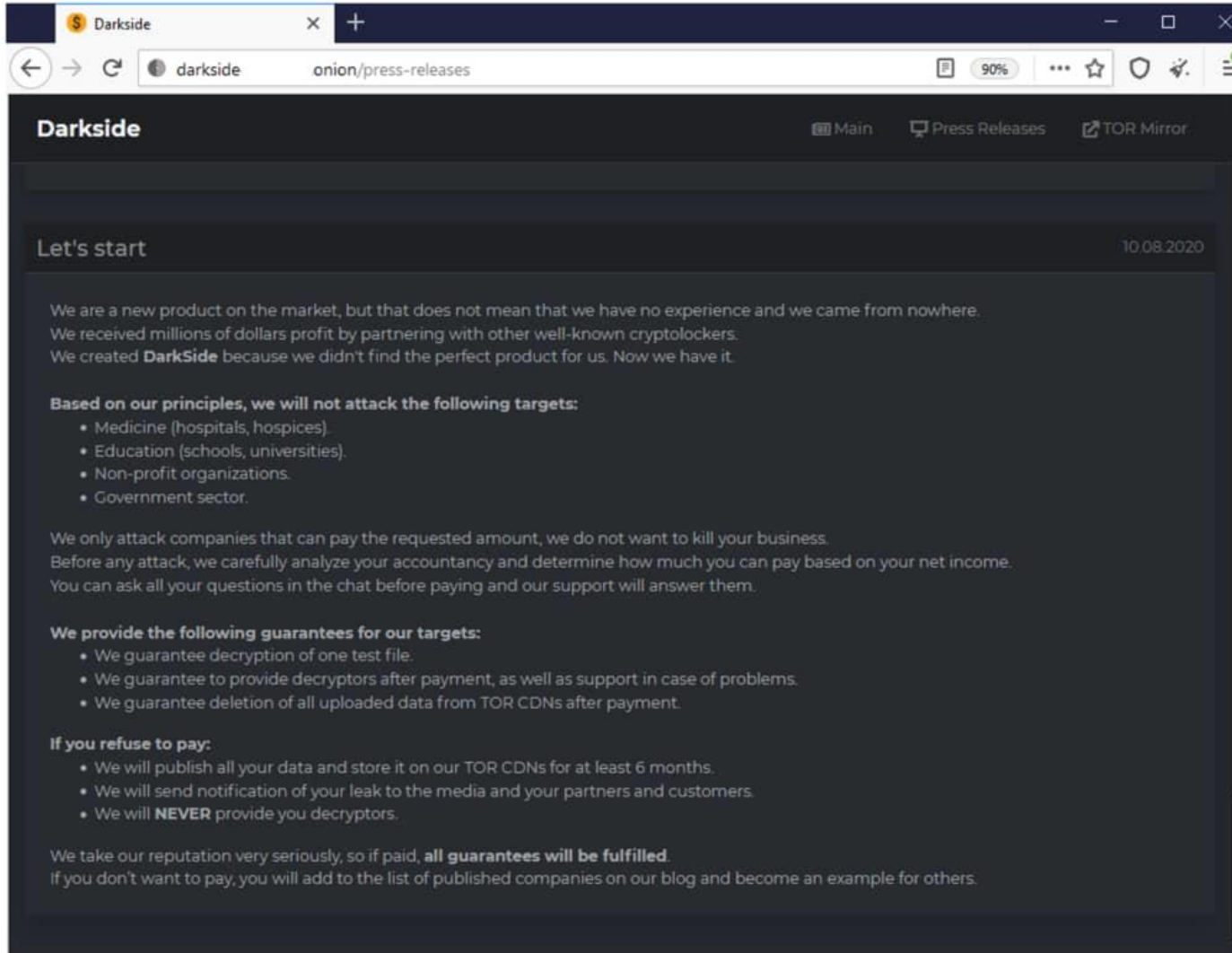
We take our reputation very seriously, so if paid, all guarantees will be fulfilled.

If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.

- Ransomware-as-a-service
- Double extortion – payment for decryption and payment to delete stolen data
- Operates with affiliates
- Claims no geopolitical affiliation and claims only driver is financial
- Intends to provide moderation and review future targets

Cybersecurity and related issues (cont...)

Always A Pioneer, Always Ahead



Cybersecurity and related issues (cont...)

Always A Pioneer, Always Ahead

Your network has been locked!

You need pay **\$ 2,000,000**
190.363 BTC (+10%) - 22537.751 XMR

After payment we will provide you universal decryptor for all network.

Don't worry, we are good decryption specialists.

How to decrypt files ?

1. Buy the required amount of XMR (Monero) or BTC (Bitcoin).
2. Send required amount to wallets in payments section.
3. Wait for 10 confirmations for XMR or 3 confirmations of BTC.
4. Reload current page after, and get a link download Decryptor.

Time is over
Price increased

Data leak
Your data stolen. Read our blog.

Chat support

30 days ago

Are you there ??? please reply man we are waiting for you.. still we are getting the error

30 days ago

Sir - this is the representative you spoke to earlier this week. This chat is compromised. Please do not respond further. Contact me here, and provide secure URL to continue: tgpx339@protonmail.com

30 days ago

For the safety of your data during verification, write to us at 2dsfr.minotpi@protonmail.com After we make sure that it is you, you will be given a new chat link. All next messages in this chat will be ignored.

30 days ago

i need my files

14 days ago

Type your question here

Thank You



www.utem.edu.my