
LOONG

Agenda

1. Introduction of the Loong Community
2. Community In Singapore
3. Identity Fraud (Deepfake) regulation of different jurisdictions

Who am I?



Captain Kelvin 新增驗證標章

OSCE³, OSEP, OSWE, OSED, OSMR, OSCP, OSDA, OSWA, OSCC, OSWP, KLCP | Black Hat / DEFCON Speaker & Trainer | Penetration Test | Digital Forensics | Incident Response | Hardware and Drone Security Researches & Analysis

Speaker / Trainer

Security Conference:

Black Hat Asia, USA, MEA

DEFCON USA 26, 27, DEFCON China

Hack In The Box, Hack In Taiwan, CodeBlue, AVTokyo, SINCON (InfoSec In the City), hardwear.io, ROOTCON, Off-By-One, OffensiveX

Forensics Conference:

SANS DFIR Summits, HTICA US & Asia Pacific, DFRWS EU, ResponderCON

Research Area:

Forensics Analysis & Investigation, IoT Hacking, Chip-off, Ransom & Crypto Case, RFID, SDR, Drone (UAV)

https://defcon.org/html/defcon-33/dc-33-communities.html

Loong Community



"Loong Community," founded by the creator of DEF CON's iconic **Chipoff Village** and **Variety Exploitation Village**, returns to continue its legacy of blending hardware hacking rigor with cultural storytelling. This year's iteration draws inspiration from the loong (Chinese dragon), symbolizing power, wisdom, and transformation, while honoring a decade of pioneering work in chip forensics, firmware exploitation, and adversarial hardware design.

Loong Community

Founded in 2025

Founding members:

RRG
RFID Research Group

DC852 · DEF CON Group Hong Kong

DNT FPV DRONE ASSOCIATION
HONG KONG , CHINA

[redacted]

OWASP
Hong Kong

BSides
Hong Kong

Previous Activities

Defcon China – Chip Off Village, VX Village

Defcon USA – Chip Off Village, Variety eXploitation Village

Black Hat USA, Asia, MEA – Drone Hacking Training, Chip Off Village, Hardware Hacking Village

Other Conference – Drone Hacking Village, RFID Hacking Village, BadUSB Village, IoT Hacking Village

What’s inside?

Area : 3000 sq feet, next to village area

Activities:

- Supported by Hacker Warehouse, providing products for testing and demonstration
- RFID kits: Proxmark3, FlipperZero, iCopyX, NFC tester & killer
- SDR Devices: SignalSDR Pro, HackRF, KrakenSDR
- BadUSB: USBNInja Pro, O.MG Cable, RubberDucky
- Networking Tools: WiFi Pineapple, Lantap, Packet Squirrel
- Drone Zone: FPV drone, flight simulator, drone components and firmware reverse engineering

LOONG VILLAGE

SDR

SDR STATION: UNLOCK THE INVISIBLE SPECTRUM
HACKRF • SIGLENS PRO • KRAKENSDR —
WEAPONIZING RADIO WAVES

A DEDICATED WAR ROOM AT SECURITY CONS WHERE ATTENDEES DISSECT AMBIENT RF EMISSIONS, INTERCEPT ROGUE TRANSMISSIONS, AND WEAPONIZE SOFTWARE-DEFINED RADIOS AGAINST VULNERABLE WIRELESS SYSTEMS.


SIGNALENS PRO


HACKRF + PORTAPACK


KRAKEN SDR



HACKRF ONE

BROUGHT TO YOU BY

LOONG VILLAGE

RFID

The RFID station is a dedicated space at various security conferences that focuses on Radio Frequency Identification (RFID) technology, its applications, and its associated vulnerabilities.

Demonstration tools such as the Proxmark3, Flipper Zero, and ChameleonUltra are frequently showcased to educate attendees about RFID security, penetration testing, and the risks associated with poorly secured RFID systems.


PROXMARK3

SWISS ARMY KNIFE FOR RFID RESEARCH


FLIPPERZERO

POCKET TOOL OF HARDWARE HACKING


CHAMELEONULTRA

RFID EMULATION POWERHOUSE


RFID DETECTORS

RFID SIGNAL SNIFFER

BROUGHT TO YOU BY

LOONG VILLAGE

NETWORKING

NETWORK ESPIONAGE STATION: SILENT INFILTRATION

LAN TAP PRO • PACKET SQUIRREL • SHARK JACK • PLUNDER BUG – WEAPONIZING PHYSICAL ACCESS

A DEDICATED DEMO ZONE EXPOSING HARDWARE-BASED NETWORK INTRUSION TECHNIQUES, WHERE ATTENDEES WITNESS LIVE NETWORK COMPROMISES THROUGH SEEMINGLY INNOCUOUS DEVICES.


LAN TAP PRO


SHARK JACK


PLUNDER BUG


PACKET SQUIRREL

BROUGHT TO YOU BY

LOONG VILLAGE

BADUSB

WITNESS LIVE HACKS | TEST DEVICES
BUILD YOUR OWN | BADUSB STATION

THE BADUSB DEMONSTRATION STATION
A DEDICATED SPACE AT SECURITY CONFERENCES FOCUSING ON USB HUMAN INTERFACE DEVICE (HID) EXPLOITATION, PHYSICAL ACCESS THREATS, AND MALICIOUS PERIPHERAL RISKS. THIS INTERACTIVE AREA SHOWCASES HOW INNOCUOUS-LOOKING USB DEVICES BYPASS SECURITY CONTROLS TO COMPROMISE SYSTEMS WITHIN SECONDS.


USBNINJA

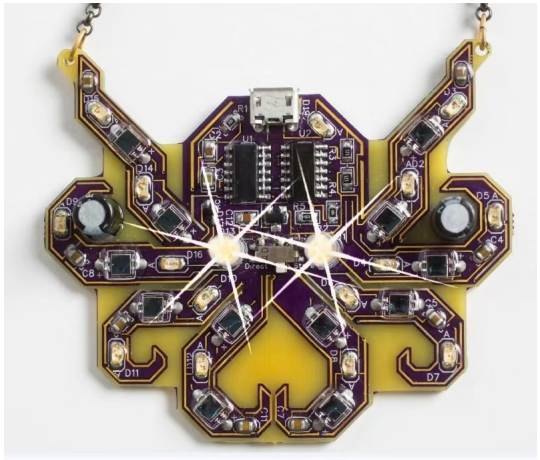


O.MG CABLE


RUBBER DUCKY


BADMOUSE BY USBNINJA

BROUGHT TO YOU BY




Badge Faces


#BadgeLife
X
STAR Labs SG
Main Menu:
4. BLE Spam
A: Enter
B: Back
A
B

DIVISION ZERO (div0

SINGAPORE CYBERSECURITY COMMUNITY GROUP

est. 2011

MISSION

To promote a vibrant cybersecurity community, and a safer cyberspace

ABOUT US

Div0 is an open, inclusive, and volunteer-driven cybersecurity community group.

We provide a platform where cybersecurity professionals, practitioners, and enthusiasts can **meet like-minded people**, **explore and learn with peers**, and **contribute to the community**.

We do so by organizing events, driving programs and initiatives, encouraging collaboration and contributions, and reaching out to the public.

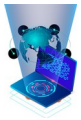
FOLLOW US: https://linktr.ee/div0linktree

OUR AFFILIATES: SHERPASEC | b10s

OUR KEY INITIATIVES



COMMUNITY BUILDING
Meetups & Workshops



INTERNATIONAL EXCHANGES
INFOSEC IN THE CITY PRESENTS SINCON



YOUTH DEVELOPMENT
Conference, Competitions, International Exchanges



CAPx DEVELOPMENT
Cybersecurity Community OJT and Tools Development



MICRO-COMMUNITIES
Special Interest Groups



PUBLIC OUTREACH
Cybersecurity Awareness



#BornToHack | Our Ethos, Our Manifesto

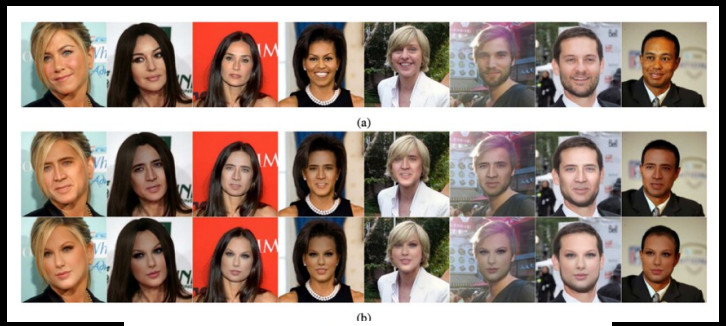
- We Explore to Discover
- We Innovate to Advance
- We Collaborate to Elevate

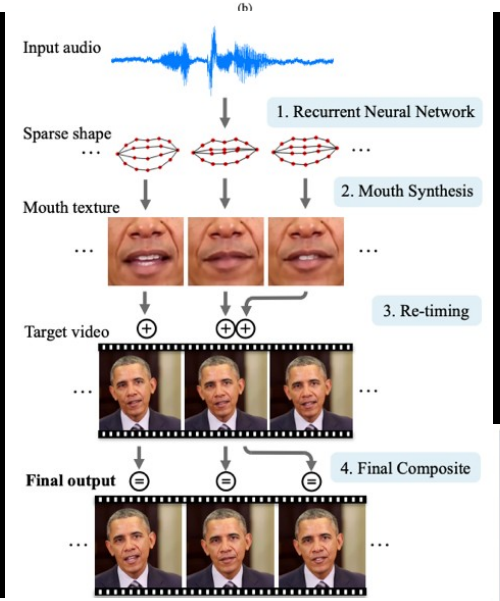
OUR SPONSORS / PARTNER: CyberSG TIC COLLABORATION CENTRE | RED ALPHA

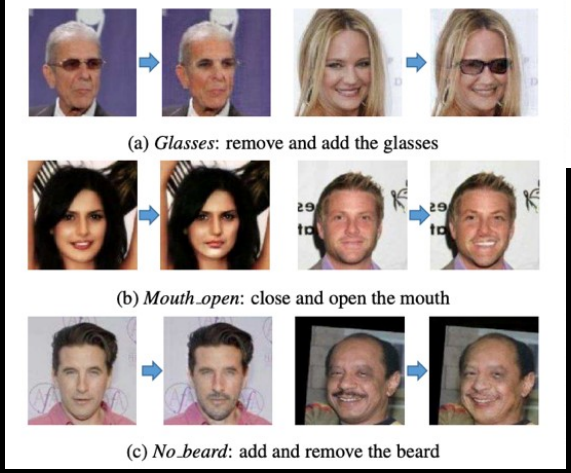
Synthetic Shadows? The Deepfake Identity Fraud Legal and Regulatory Across UK, EU, China & Hong Kong

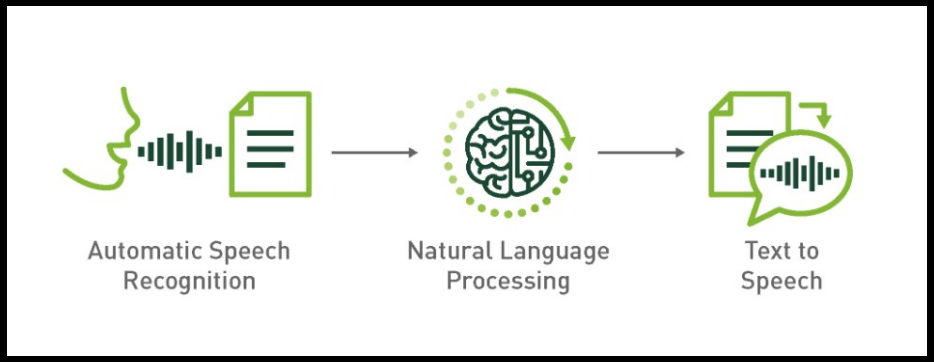


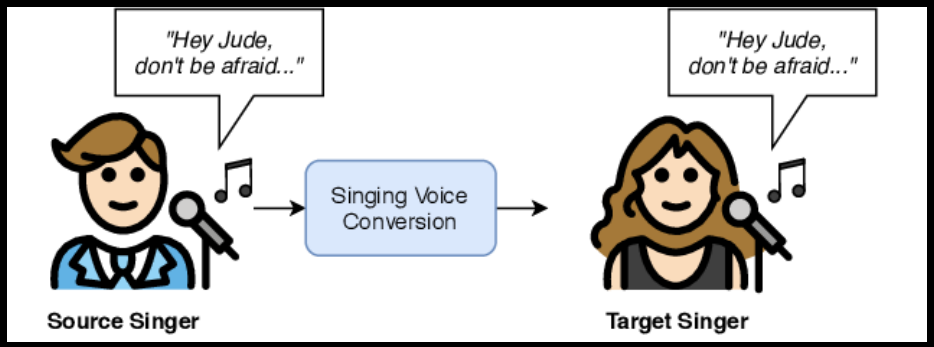
Wong Noel
MSc Crime Science with Cyber Crime - University College London (2024-2025)
BA Criminology - Durham University (2021-2024)













Deepfake
Visual & Audio

Reuters

World Business Markets Sustainability Legal Commentary Technology Investigations

BEIJING, May 22 (Reuters) - A fraud in northern China that used sophisticated "deepfake" technology to convince a man to transfer money to a supposed friend has sparked concern about the potential of artificial intelligence (AI) techniques to aid financial crimes.

This article is mor

UK engineering firm Arup falls victim to £20m deepfake scam

Hong Kong employee was duped into sending cash to criminals by AI-generated video call

Business live – latest updates

ase Exampl

Yahoo! Autos

Ferrari CEO Impersonated by AI in Deepfake Scam Attempt – Report

In a recent attempt to defraud Ferrari, scammers impersonating CEO Benedetto Vigna were thwarted by a vigilant executive.

CNN World Africa Americas Asia

World / Asia

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

Forbes

A Voice Deepfake Was Used To Scam A CEO Out Of $243,000

The CEO of an unnamed UK-based energy firm believed he was on the phone with his boss, the chief executive of firm's the German parent company.

Craiyon

AI Art Generator

DEEP FAKE



reface

The best face swap app

4.8

455.2K ratings

Download on the App Store

Terms Of Use Privacy Policy

DEEPFAKES WEB

Sukumaran (2023)



THE BROADER DEMOCRATISATION OF AI TOOLS

(WESTERLUND, 2019)


IS THERE A NEED FOR
NEW LEGISLATION
AND REGULATORY MEASURES
TO ADDRESS POTENTIAL GAPS?


NO SPECIFIC CRIMINAL LAW
TARGETING DEEPFAKES
EXISTING STATUTES MAY
APPLY

Punitive Legislative

Fraud Act 2006

Section 2 – Fraud by false representation

Section 7 – Making or supplying articles for use in frauds

Section 9 – Participating in a fraudulent business by sole trader

Computer Misuse Act 1990

Section 1 – Unauthorised access to computer material

Section 3 – Unauthorised acts with intent to impair

Section 3A – Making, supplying or obtaining articles for use in offences under section 1, 3 or 3ZA

Sensitive area of national sovereignty

= EU does not have its own criminal code

Directive - Sets binding goals for EU countries but leaves them free to choose how to achieve these objectives.

Decision - Fully binding, but only for those it is addressed to.

Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA

Chapter IV Article 253-1 [Crime of infringing citizens' personal information] Whoever sells or provides

Chapter V Article 266 [Fraud] Whoever swindles public or private money or property.

Chapter VI Article 287-1 [Crime of Illegal Use of Information Networks] Whoever commits any of the following conduct by using the information network:

(1) Creating or managing online platforms to facilitate fraud, teach criminal methods, or trade illegal content.
(2) Publishing information about the production or sales of illegal goods or activities.
(3) Sharing content to commit fraud or other crimes.

Cap. 200 Crimes Ordinance Section 161. Access to computer with criminal or dishonest intent

Cap. 210 Theft Ordinance Section 16A Fraud and Blackmail - Fraud

Jurisdiction	Case Criminal Convictions?	Legal Development
UK	Cases still under investigation	/
EU		/
China	Nanjing 2024	Applied Criminal Law Art. 253-1, 266 • 4 years and 6 months in prison • RMB¥40,000 fine • Public apology in national media
Hong Kong	Cases still under investigation (e.g. Arup case)	/

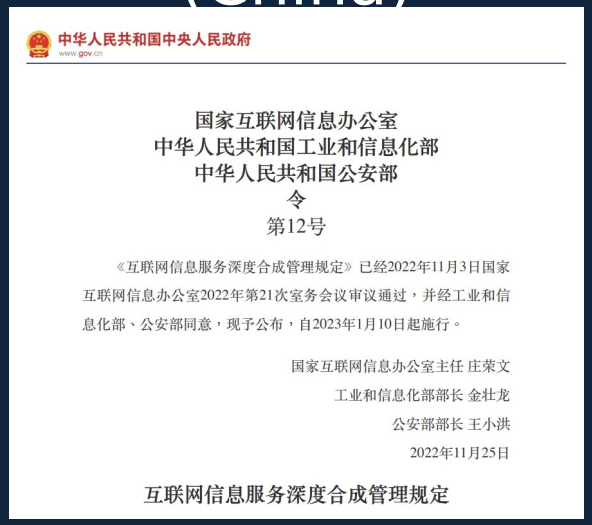


IS THERE A NEED FOR NEW LEGISLATION AND REGULATORY MEASURES TO ADDRESS POTENTIAL GAPS?

Common Law

Civil Law

Provisions on the Administration of Deep Synthesis Internet Information Services (China)



中华人民共和国中央人民政府
www.gov.cn

国家互联网信息办公室
中华人民共和国工业和信息化部
中华人民共和国公安部
令
第12号

《互联网信息服务深度合成管理规定》已经2022年11月3日国家互联网信息办公室2022年第21次室务会议审议通过，并经工业和信息化部、公安部同意，现予公布，自2023年1月10日起施行。

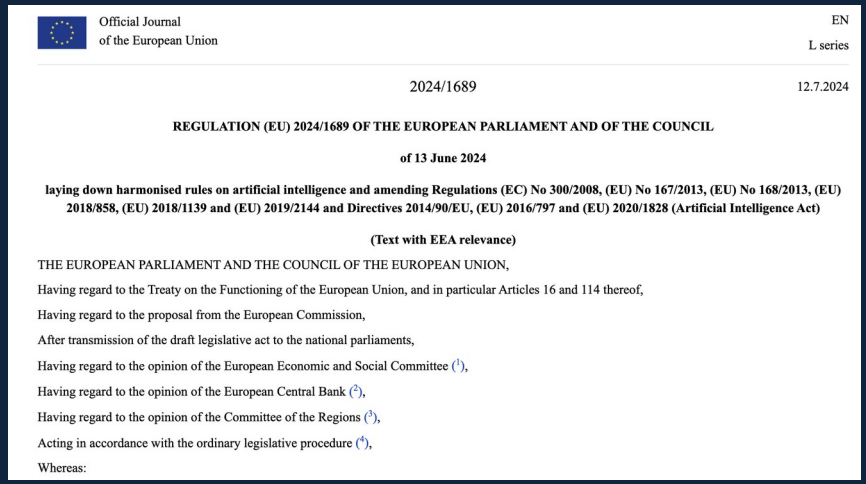
国家互联网信息办公室主任 庄荣文
工业和信息化部部长 金壮龙
公安部部长 王小洪
2022年11月25日

互联网信息服务深度合成管理规定

Regulate synthetic content to maintain social order and national security

One of the most comprehensive and enforceable deepfake laws globally, reflecting China's top-down and security-focused

AI Act (EU)



Official Journal
of the European Union

EN
L series

2024/1689

12.7.2024

REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 13 June 2024

laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee [1],

Having regard to the opinion of the European Central Bank [2],

Having regard to the opinion of the Committee of the Regions [3],

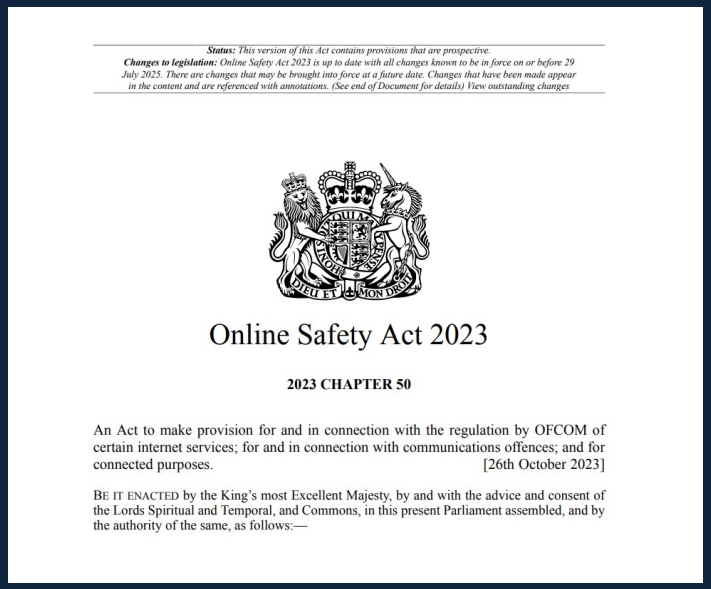
Acting in accordance with the ordinary legislative procedure [4],

Whereas:

A risk-based regulatory framework focusing on human rights and innovation

More flexible, focusing on accountability and transparency rather than strict prohibition.

Online Safety Act & AI White Paper (UK)



Status: This version of this Act contains provisions that are prospective.
Changes to legislation: Online Safety Act 2023 is up to date with all changes known to be in force on or before 29 July 2025. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes

Online Safety Act 2023

2023 CHAPTER 50

An Act to make provision for and in connection with the regulation by OFCOM of certain internet services; for and in connection with communications offences; and for connected purposes. [26th October 2023]

BE IT ENACTED by the King's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—



Department for Science, Innovation & Technology

A pro-innovation approach to AI regulation

Government response to consultation

February 2024

Non-consensual deepfake pornography
Accountability and user protection
Protect children online (harmful content)

Pro-innovation

Hong Kong

Cybercrime Policing Advisory Panel (CPAP)

- To enhance public awareness on the potential risks of AI.

Through its Facebook page and the Cyber Defender website

- Disseminating information about the latest crime situation and anti-deception advice related to deepfake technology



The Government of the Hong Kong Special Administrative Region

Press Releases

GovHK 香港政府一站通 繁體版 简体版

LCQ9: Combating frauds involving deepfake GO

LCQ9: Combating frauds involving deepfake

****

Following is a question by Dr the Hon Tan Yueheng and a written reply by the Secretary for Security, Mr Tang Ping-keung, in the Legislative Council today (June 26):

Question:

A study has reportedly found that the number of scams involving deepfake in Hong Kong in the first quarter of this year has scored a 10-fold increase year-on-year, which is among the highest in the Asia-Pacific region, and the rate of deepfake identity fraud involving the fintech industry in Hong Kong is the highest in the Asia-Pacific region. On the other hand, some members of the public are worried that there is no way to guard against law-breakers who have in recent years successfully committed frauds by making use of deepfake technology to create highly realistic faces and voices. In this connection, will the Government inform this Council:

(1) of the respective numbers of proactive investigations conducted and reports received by the Government in each of the past three years in respect of fraudulent activities using deepfake technology, and set out for each case the type of fraud and amount of money involved; the detection rate of such cases;


IS THERE A NEED FOR
NEW LEGISLATION
AND REGULATORY MEASURES
TO ADDRESS POTENTIAL GAPS?

]

Thank You!



Synthetic Shadows? The Deepfake Identity Fraud Legal and Regulatory Across UK, EU, China & Hong Kong

Wong Noel (University College London – United Kingdom)

https://www.linkedin.com/in/wong-noel-911b03261/