

**AIPOL MEMBERS USE ONLY.**  
Please do not hand this out to  
members of the public

# AiPol

Australasian Institute of Policing



Journal of the Australasian Institute of Policing Inc.

Volume 13 Number 1 • 2021



# ENCRYPTION CRIMINALS

**CHALLENGE & OPPORTUNITIES FOR LAW ENFORCEMENT**

# EXCLUSIVE DEALS ON LIGHTFORCE GROUP'S PRECISION PRODUCTS.



Force Ordnance can offer police force personnel special pricing on a range of products from Nightforce, Lightforce, Gunforce and APRS including precision optics, vehicle and handheld lighting, firearms and more.

Visit [forceordnance.com/police-signup](https://forceordnance.com/police-signup) to get offers by email or call (08) 8440 0888 to discuss your needs with one of our team.

## FORCE ORDNANCE

LightFORCE

NIGHTFORCE



GUNFORCE



APRS



Lightforce  
Group



Vol. 13, No. 1  
March 2021

Published by the Australasian Institute of Policing Inc.

A0050444D ABN: 78 937 405 524

ISSN: 1837-7009



Visit [www.aipol.org](http://www.aipol.org) to view previous editions  
and to subscribe to receive future editions.

### Contributions

Articles on issues of professional interest are sought from Australasian police officers and police academics. Articles are to be electronically provided to the Editor, [aipoljournal@aipol.org](mailto:aipoljournal@aipol.org). Articles are to conform to normal academic conventions. Where an article has previously been prepared during the course of employment, whether with a police service or otherwise, the contributor will be responsible for obtaining permission from that employer to submit the article for publication to Australasian Policing.

Contributors are expected to adhere to the Journal's publishing guidelines. These guidelines are available in this Journal. All papers are peer-reviewed.

### Disclaimer

While every effort is made to check for accuracy, the Publishers or Editors cannot be held responsible for the content, errors or omissions inadvertently published in articles and advertisements in Australasian Policing. Views expressed by contributors are not necessarily those of AiPol, the Editors or the Publisher. No responsibility for loss occasioned to any person acting, or refraining from acting, as a result of material in this publication can be accepted.

### Copyright

All rights reserved. No part of this publication may be reproduced or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or be stored in any retrieval system of any nature, without written permission of the copyright holder and the Publisher, application for which in the first instance should be made to the Publisher for AiPol.

# Contents

Editorial	3
Foreword	5
Criminals targeted for encrypted phones	9
Trouble on line for criminals using encrypted phones	10
Decrypted: Phantom Secure takedown a 'significant blow' against Australia's organised crime networks	13
No backdoors: Investigating the Dutch Standpoint on Encryption	14
Cops take out encrypted comms to disrupt organised crime	27
Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe	28
Encryption as a challenge for European law enforcement agencies	30
Assistance and Access Act Overview	35
Debunking the Myths – Australia's Assistance and Access Act	38

# Most recommended super fund<sup>1</sup>

Our members can focus on today,  
knowing their future is safe with us.



Visit [QSuper.com.au](https://www.QSuper.com.au) today

<sup>1</sup> Award is based on information collected from the DBM Atlas research program – feedback from over 80,000 business owners or retail customers January 2019 through December 2019. Award results are based on experiences and perceptions of customers surveyed in this period. For DBM Atlas and DBM Australian Financial Awards information, visit [dmbconsultants.com.au](https://dmbconsultants.com.au).

Product issued by the QSuper Board (ABN 32 125 059 006, AFSL 489650) as trustee for QSuper (ABN 60 905 115 063). Consider the PDS on our website to see whether QSuper is right for you. © QSuper Board



# Editorial

## DR AMANDA DAVIES

Editor, Assistant Professor Policing and Security at the Rabdan Academy, Abu Dhabi



***The technological advances society is experiencing bring both advantages and disadvantages to our daily lives and the pace at which such technology changes is similarly reflected in the manner in which criminal networks adapt these technological developments to support their illegal activities.***

Welcome to the March 2021 edition. Globally, in the world of law enforcement and policing the data indicates the Covid-19 pandemic did not place a brake on criminal activity, it influenced the rate of the types of crimes being committed – including online/cyber crime. Organised crime continued, aided and abetted by the advances in technology, in particular encryption technology to enable undetected communication networks to operate. The successful dismantling of the encrypted network, EncroChat in 2020 as a result of collective efforts of law enforcement across the world highlighted not only the extent to which criminals reach in order to continue 'business as usual' during the upheaval of living with a pandemic it also highlighted the commitment and extensive expertise of our law enforcement agencies. Such dedication and focus on disrupting encryption supported criminal activity requires support from governments and by association legislation to enable effective application of crime fighting strategies.

The Australian law enforcement experience with encrypted phones being a mainstay of criminal activity whilst not new was highlighted in the 2018 joint Canadian/Australian successful shutdown of the Canadian encrypted

communications service Phantom Secure. As was anticipated, a ready alternative, Ciphre was immediately in play as 'crime does not sleep' and law enforcement had a new target.

The use of encryption technology is underpinning a wide range of crime typologies, including cybercrime, serious organized crime and terrorism and as has been witnessed in prosecutions, the rate at which encryption and the intentional hiding of data and communication is involved in criminal activities is on the increase. As reported by David Murray (Criminals Targeted for encrypted phones) it is lucrative business and one of the key challenges for law enforcement is the intrinsic mobile nature of the activity.

Enabling our law enforcement agencies to be equipped with effective and adequate tools including legislative powers is central to strategic and operational plans for counter attacking the extent and influence of encryption supported crime.

In a climate in which criminal activity is dependent on agility and adaptability as evidenced in the rapid transition from one encryption serviced network to a replacement, authority and legislative power needs to be, as a minimum, enabling the efforts of law enforcement.

The technological advances society is experiencing bring both advantages and disadvantages to our daily lives and the pace at which such technology changes is similarly reflected in the manner in which criminal networks adapt these technological developments to support their illegal activities. As discussed by Jon Hunt-Sharman (President's Report), reviewing the application of legislation such as the Australian *Assistance and Access Act* and the influence on investigation and ultimately prosecution of criminal activities demonstrates the relationship between legislation, empowerment of law enforcement, and criminal prosecution.

The body of literature informing on the role of encryption technology and its impact on criminal activity, is slowly emerging, due to the nature of this technology and the parallel increase in law enforcement resourcing dedicated to investigate and expose this area of crime, it is anticipated the monitoring and evaluation of the efforts of law enforcement will continue to develop. This will be an area of continuing interest nationally and internationally, and we look forward to presenting updates in future journal editions.

# PROUDLY SUPPORTING THE NSW POLICE AND AIPOL

The Siding, Petersham



“ Deicorp is a proud sponsor of the AiPol Police Journal and we’re pleased to extend our thanks and appreciation to all serving NSW Police officers for continuing to keep us safe during challenging times. ”

**Fouad Deiri,**  
Managing Director, Deicorp



TNT Residences, Redfern



Downtown, Zetland



Proximity, Rouse Hill

[deicorp.com.au](http://deicorp.com.au)

**02 8665 4100**

Level 3, 161 Redfern Street, Redfern NSW 2016



*Be part of our story!*

# President's Foreword

## JON HUNT-SHARMAN

President, Committee of Management, Australasian Institute of Policing

As a matter of general principle, the Australasian Institute of Policing (Aipol) is of the view that our members within policing and law enforcement are greatly assisted and protected when laws providing law enforcement agencies with intrusive powers are clear, precise and unambiguous in their terms and their interaction with other legislation.

Clarity in decision-making criteria, limitations and grounds where such powers may be exercised, are not just critical for providing public assurance about the use of those powers, but are absolutely critical in protecting police and law enforcement practitioners in the exercise of their duties. The findings of the Royal Commission into the Management of Police Informants demonstrates the pitfalls for policing practitioners of not having unambiguous legislation, policies and procedures to support their actions.

In 2018 Aipol supported the Telecommunications and Other Legislation Amendment Act 2018 (commonly known as the Assistance and Access Act) as we believed that it was important that police and law enforcement officers have the protections of unambiguous legislation in relation to accessing encrypted material during criminal investigations.

The Assistance and Access Act amended a range of Commonwealth legislation to empower law enforcement and national security agencies to request, or compel, assistance from telecommunications providers. It also established powers which enable law enforcement and intelligence agencies to obtain warrants to access data and devices, and amended the search warrant framework under the Crimes Act and the Customs Act to expand the ability of law enforcement agencies to collect evidence from electronic devices.

At the time, the legislation was controversial as Australia was one of the first countries to legislate lawful protections and powers for intelligence and law enforcement agencies within the encrypted space.

This issue again has become topical as a result of a current review of the Assistance and Access Act by

the Parliamentary Joint Committee on Intelligence and Security.

There is a view, particularly from some tech companies and civil libertarian groups, that the legislation should be repealed.

It is the view of Aipol that any weakening of the Assistance and Access Act will have significant negative impact on police and law enforcement agencies combatting organised crime syndicates and investigating serious crime in Australia.

Many overseas governments have avoided any official standpoint on encryption. For example many governments in the European Union (EU) have taken a non-legislative approach to encryption with the EU subsequently focused on enhancing the technical capabilities already available within Europol and revamping Europol as the European Centre of Expertise on Encryption.

Other countries, such as Australia, France, UK, USA, Canada and New Zealand have enacted legislation on law enforcement and national security grounds. This legislative capability has arguably led to the most effective exposure and dismantling of organised crime syndicates globally.

***It is the view of Aipol that any weakening of the Assistance and Access Act will have significant impact on police and law enforcement agencies combatting organised crime syndicates and investigating serious crime in Australia.***

For example, in 2018 the NSW Crime Commission, the AFP the ACIC, the FBI and the RCMP conducted an operation into a Canadian security firm, Phantom Secure, which offered encrypted messaging and chat services as well as encrypted devices. This operation led to the takedown of Phantom Secure globally and the imprisonment of Phantom Secure CEO Victor Ramos. The Court also ordered Ramos to forfeit \$80 million as proceeds of the crime, as well as specifically identified assets, including international bank accounts, real estate, cryptocurrency accounts, and gold coins.

Criminal organisations used Phantom Secure smartphones to facilitate the distribution of wholesale quantities of cocaine, heroin and methamphetamines throughout the world, including the United States, Australia, Mexico, Canada, Thailand and Europe.

Among others, Ramos' clients included the Sinaloa drug cartel of Mexico, a global drug-trafficking and illicit gambling organisation run by Owen Hanson, now serving a 21 years prison sentence. It also included the

*continued on page 6*



Hells Angels in Australia, who used the phones to coordinate several killings.

In 2020, French authorities hacked into encrypted Encrochat phones and shared the data with international counterparts, secretly accessing more than 100 million messages over several months leading to international arrests throughout world of major crime figures, significant disruption of various criminal activities, including pedophile, drug and money laundering syndicates. The operation also resulted in huge seizures of cash, drugs and firearms, identified significant official corruption, prevented kidnapping and executions and stopped international drug shipments to Australia.

Aipol believes that the *Assistance and Access Act* is world leading and proportionate, balancing civil rights and economic imperatives, whilst supporting law enforcement and national security capabilities.

Opponents of the legislation tend to exaggerate the powers under the *Assistance and Access Act*. This is important legislation and it is important that our members and the general public are aware of the facts rather than 'hype' from some media and special interest groups.

### So how successful has the *Assistance and Access Act* been?

In the 12 months prior to the legislation being passed, Cyber Security Minister Angus Taylor advised that 200 cases had arisen where investigations for serious crimes had been impacted by the inability to access that data under the existing legislation.

Minister Angus Taylor stated at the time:

"The risk here is that criminals, terrorists, paedophiles and drug smugglers are getting away with their crimes without us being able to hold them to account."

There have been some significant results under the *Assistance and Access Act*.

During the current Parliamentary review the Department of Home Affairs has advised that:

- in 2018 and early 2019, agencies have used the industry assistance and computer access based powers in the Act to support their lawful investigations and operations into transnational, serious and organised crime, cybercrime and serious crimes against persons;

■ agencies have also been working with providers on national security matters. The Department of Home Affairs also advised that:

- the AFP has used the industry assistance framework in support of their lawful activities. To date all requests for assistance have been provided voluntarily pursuant to technical assistance requests (TAR) TARs;
- the AFP has found its engagement with industry to be positive and cooperative;
- computer access warrants are necessary and the ability to escalate to this level of access is critical to operational effectiveness. The AFP takes the application of such intrusive powers very seriously and with due consideration. These warrants have been used in a very measured and considered way and have provided access to evidence that had not previously been available.

### Statistics on AFP use of *Assistance and Access Act* powers

The AFP's use of the Assistance and Access Act powers, specifically the number of Technical Assistance Requests (TARs), Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs) under the industry assistance framework, is reported annually in line with the Telecommunications (Interception and Access) Act 1979 (TIA Act) and Part 15 of the Telecommunications Act 1997.

Likewise, the AFP's use of Computer Access Warrants (CAWs) is reported annually in line with the Surveillance Devices Act 2004 (SD Act).

### Industry Assistance

Under the *Assistance and Access Act* the AFP issued **eight (8) TARs**. These related to investigations into cybercrime, drug importation and the threat of transnational serious and organised crime.

No TANs or TCNs have been issued by the AFP, and no State or Territory police forces sought the AFP Commissioner's approval to issue TANs under the industry assistance framework.

The AFP experience is that Schedule 1 of the Act has accelerated cooperation from industry, with providers increasingly willing to assist due to the Act providing legal certainties and assurances regarding the commercial scope and impact of requests.

The fact the AFP has not sought any TANs or TCNs to date, does not indicate these provisions are not required. The AFP has advised that it demonstrates the effectiveness of the Act's tiered approach.

### Computer Access Warrants

Under the Assistance and Access Act the AFP has obtained **twenty three (23) CAWs**, two of which were extended. An additional one (1) CAW application was refused by the issuing authority, due to concerns that a physical computer had to be identified.

The AFP obtained 16 computer access warrants under schedule 2, which related to drug trafficking, cybercrime, terrorism and corruption investigations.. Eleven of these computer access warrants related to counter-terrorism investigations.

### AFP operational case examples

The below case examples demonstrate the benefits of the *Assistance and Access Act* powers:

#### Cybercrime – Remote Access Trojan malware (before court)

This matter involved an investigation into the possession and use of "Imminent Monitor – Remote Access Trojan" (IM-RAT) malicious software (malware). The malware allowed remote and secret control over a victim's computer and other devices, to access and view files, record keystrokes and activate the computer's web camera.

A statistically high percentage of Australian-based purchasers of IM-RAT (14.2%) are named as respondents on domestic violence orders, and one of the purchasers is also registered on the Child Sex Offender Register.

Without these powers, the AFP would have been unable to proactively investigate and capture relevant data and evidence stored in Australian and other participating countries, or identify victims and prosecute users of this malware. The powers also enabled the AFP, and it's partners, to identify and stop other serious crimes, including computer misuse, fraud, dealings in the proceeds of crime, narcotics and sexual offences.

An overt search warrant would have alerted the criminals using this malware, precluding further identification, disruption and prosecution on ancillary offending being facilitated by the malware. A traditional search warrant would only yield a limited subset of the customer



***The risk here is that criminals, terrorists, paedophiles and drug smugglers are getting away with their crimes without us being able to hold them to account.***

database (noting the purchase may be made in cryptocurrency and untraceable), and this would not have assisted proactive or the targeting of investigations on the users of the malware.

### Outcomes

As at 30 November 2019 in relation to this investigation:

- 85 warrants had been executed internationally
- 434 devices have been seized (laptops, phones and servers etc.)
- 13 people have been arrested (none yet in Australia)
- The website selling the malware has been taken down.

### Importation of illegal drugs

The AFP used the enhanced search warrant provisions, to execute a section 3E search warrant on a premises, following the suspected importation of illegal drugs which were procured with cryptocurrency via a dark web marketplace.

During execution of the search warrant, the accused was served a notice to assist in accordance with the updated section 3LA provisions. Following consideration of the order and being advised of the new penalties (up to 10 years imprisonment), the accused provided the AFP with passwords to a number of devices, as well as a number of cloud-hosted accounts through which he had facilitated the importation.

This demonstrates the utility of increased section 3LA penalties. Through the provision, the AFP was able to successfully access, identify and collect otherwise secure and encrypted communications and digital records as evidence of the alleged offending.

### Cybercrime DDOS attack on government infrastructure (before court)

The AFP used the Act's powers during an eight-month investigation into the use of a carriage service to

make threats, identify data sets of compromised personal information, inform Australian government and public telecommunications infrastructure of cyber vulnerabilities and compromise and prevent online fraud. This was a parallel investigation to a State police operation investigating dedicated denial of service attacks against their own telephone infrastructure.

The Act's powers were of significant benefit in this investigation, as they enabled the AFP to obtain evidence from multiple electronic systems used by the alleged offender to commit a variety of offences. Information obtained using the Act's powers also identified further avenues of police enquiry, filled significant evidentiary gaps in relation to the alleged offending, and better-directed police resources in relation to this investigation.

A significant proportion of material obtained using these powers is relied on in a brief of evidence in relation to the accused.

### Outcomes

Two men were charged on 14 June 2019 with offences including:

- Unauthorised access to data held on a computer;
- Using a carriage service to make a threat or cause serious harm;
- Dishonestly obtaining or dealing with personal financial information;
- Sabotage; and
- Firearm offences.

### Example of State Police use of the Assistance and Access Act Industry Assistance

Under the *Assistance and Access Act* the NSW Police issued **thirteen (13) TARs** which related to:

- Murder – s.18(1) Crimes Act 1900 (NSW)
- Conspiracy to murder – s.26 Crimes Act 1900 (NSW)

- Discharge firearm with intent – s.33(A)(1) Crimes Act 1900 (NSW)
- Participate in a criminal group – s.93T(1) Crimes Act 1900 (NSW)
- Attempted robbery whilst armed with a dangerous weapon – s.344A/97(2) Crimes Act 1900 (NSW)
- Manufacture prohibited drugs – s.24(1) Drug Misuse and Trafficking Act 1985 (NSW)
- Supply prohibited drugs on an ongoing basis – s.25A(1) Drug Misuse and Trafficking Act 1985 (NSW)
- Supply prohibited drugs – s.25(1) Drug Misuse and Trafficking Act 1985 (NSW)
- Supply prohibited drugs (commercial quantity) – s.25(2) Drug Misuse and Trafficking Act 1985 (NSW)
- Possess unauthorised prohibited firearm – s.7(1) Firearms Act 1996 (NSW)
- Acquisition of firearms – s.50A Firearms Act 1996 (NSW)

### Conclusion

Aipol believes it is important that the *Assistance and Access Act* is put into perspective and that it not be demonised by those who have not educated themselves of the actual, powers, protections and safeguards within the legislation or the positive benefits it's powers provide law enforcement and national security agencies in the fight against those who wish to cause harm to Australia and Australians.

Law enforcement and national security agencies have always possessed lawful access under appropriate legislation to view documents, access premises, utilise listening devices and/or telephone intercepts. Through appropriate legislation, infringement upon privacy is limited, targeted, proportional and reviewable. Criminals are using encrypted communications. Without the additional powers and safeguards provided within the 'Assistance and Access Act' law enforcement and national security are unable to detect, prevent, or solve sophisticated serious and organised crime.

The *Assistance and Access Act* should be seen as 'enabling legislation'. It supports traditional law enforcement investigative powers where there is encryption crime and encryption savvy criminals.



# ***STRIPPED DEMOLITION***

**DEMOLITION  
& EXCAVATION**

**Commercial  
& Residential**

**Mob: 0466 997 905**

Find us on  
**Facebook  
and  
Instagram**

Proudly  
Supporting  
Our  
Local  
Police

**[strippeddemo.com.au](http://strippeddemo.com.au)**

**Email: [estimating@strippeddemo.com.au](mailto:estimating@strippeddemo.com.au)**

# Criminals targeted for encrypted phones

9 January 2021

**BY DAVID MURRAY**

National Crime Correspondent The Australian

Law enforcement agencies are examining ways to fight back against specially modified encrypted mobile phones that have become central to organised crime.

The most dominant encrypted phone service in the Australian underworld, Ciphrr, has in recent months alone been connected to massive drug importations, multimillion-dollar cash seizures, kidnappings and torture.

As many as 10,000 encrypted Ciphrr phones are estimated to be in use nationwide, law enforcement sources say.

It's a lucrative business in its own right, with users paying \$2500 every six months to be able to communicate securely with other criminals.

Frustrated investigators say the encrypted phones are needed only for serious and organised crime, and are considering prosecutions of people found in possession of the devices. There are also high-level talks in law enforcement agencies on whether the phones can be explicitly outlawed to shut them down.

NSW Crime Commission executive director for criminal investigations Tim O'Connor said the agency was considering a special project looking at encrypted communications. "We're going to look at the laws seriously. At the end of the day, these are just for criminals," he said.

Australian Federal Police commander for transnational operations Richard Chin said encrypted phones were "not aimed at your average citizen involved in legitimate activity".

"They are used ... across sophisticated money laundering, drug importations and trafficking and the sorts of crimes of violence that surround that industry," Commander Chin said.

A former NSW Comanchero outlaw bikie now living in Dubai, Marco Coffen, is suspected by authorities to have bought the Australasian distribution rights for Ciphrr. Coffen is a person of interest



**BlackBerry phones were the choice of criminals until the Canadian encrypted communications service Phantom Secure was shut down in 2018.**

in the murder of security guard Gary Allibon, shot in the back during a robbery of a cash-in-transit van in Sydney's CBD in 2010.

Australian criminals switched to Ciphrr in droves after Australian authorities helped shut down Canadian encrypted communications service Phantom Secure in 2018. Phantom Secure stripped BlackBerry devices of cameras, microphones, GPS navigation and other features, and equipped them with encrypted messaging software.

Ciphrr's modified Samsung and BlackBerry phones are similarly equipped to avoid prying eyes. The phones can be instantly and remotely wiped if seized.

Phantom Secure founder and chief executive Vincent Ramos was jailed for nine years in 2019 and ordered to forfeit \$80m as proceeds of crime generated by the business in 10 years.

US state attorney Robert Brewer said at the time that Ramos was "going to prison because he provided violent, drug trafficking organisations with a hi-tech tool that enabled them to co-ordinate their crimes while staying in the shadows".

Authorities estimated about half of Phantom Secure's 20,000 devices worldwide were in Australia when it was shut down.

Salvatore Formica and Pierino Forni, accused of being part of a crime syndicate that tried to bring more than half a tonne of cocaine into Australia on a light aircraft via PNG last year, were found with Ciphrr phones.

Separately, Brisbane man Simon Cross had a Ciphrr phone when Queensland police pulled over his car on the Pacific Motorway in July and found \$4.4m stashed inside.

Ciphrr did not respond to a request for comment this week.

In a major blow to organised crime, French authorities last year hacked into encrypted Encrochat phones and shared the data with international counterparts, secretly accessing more than 100 million messages over several months. The operation resulted in huge seizures of cash and firearms, exposed official corruption, prevented kidnappings and executions and stopped international drug shipments to Australia.



# Trouble on line for criminals using encrypted phones

9 January 2021

**BY DAVID MURRAY**

National Crime Correspondent *The Australian*

The title of biggest law enforcement bust in the world last year belongs to the investigators who cracked an encrypted mobile phone network called Encrochat, and took down the organised crime groups that thought their communications impregnable.



In July, it was announced that French authorities had secretly hacked into Encrochat phones and with international counterparts had been monitoring encrypted messages, in real time, for months. More than 100 million messages containing the deepest and darkest secrets of crime gangs had been accessed by law enforcement officers.

There were more than 60,000 Encrochat subscribers worldwide, primarily in Europe but some further afield, and almost all of them were involved in serious criminal activity. They were paying thousands of dollars every six months for the privilege of hatching their plans securely.

Investigators pored over every word as kingpins and their middlemen planned vast drug smuggling operations and arranged kidnappings and executions, their discussions free and open in a manner they would never have contemplated on ordinary phones.

The results were stunning. In Britain, the National Crime Agency launched Operation Venetic to sift through the avalanche of evidence.

The NCA said in July that in Britain alone it had overseen 746

arrests, intercepted more than two tonnes of drugs and “mitigated 200 threats to life”; it had also seized £54m in cash and weapons including submachine guns, grenades and many thousands of rounds of ammunition.

Dutch police swooped on a shipping container converted into a torture chamber, equipped with a dentist’s chair, hedge cutters, pliers, scalpels and handcuffs. Six other containers at the same warehouse in Wouwse Plantage, near the Belgian border, were intended as prisoner holding cells. Photos of the containers were found on Encrochat phones, tipping authorities off.

Law enforcement agencies said organised crime workings had been laid bare in a way never before seen, and announced Encrochat-linked arrests in The Netherlands, Norway, Sweden and France.

“It was as if we were sitting at the table where criminals were chatting,” said Jannine van den Berg, chief constable of Dutch police Central Unit.

Encrochat and other encrypted phone firms like it — in Australia the most popular in the criminal underworld is now Ciphre — take standard phones and modify them so that only those with the device can read the encrypted messages.

Cameras, microphones, GPS navigation and other features are removed, and the phone’s data can be instantly and remotely wiped if it falls into the wrong hands. A set number of incorrect attempts to guess the password also triggers self-destruction of incriminating conversations.

***The NSW Crime Commission warned in its 2020 annual report that encrypted networks were “now regarded as essential tools for organised crime networks”.***



**Almost 450kg of MDMA hidden in an excavator at Brisbane. Picture: Supplied by AFP**

French authorities found a way to install malware on Encrochat's phones that allowed them to read messages before they were encrypted.

By September, Dutch police had set up a team to investigate corruption exposed in the messages, while further information was gleaned about lawyers, real estate brokers and other professional facilitators who grease the wheels of organised crime.

Unsurprisingly, there were ramifications in Australia. The NCA says that by last month a total of two tonnes of cocaine, MDMA and methamphetamine headed to, or in, Australia had been seized in connection to the Encrochat intercepts.

One payload of almost 450kg of MDMA, hidden in the modified boom of an excavator, was shipped into the Port of Brisbane from the UK in March last year.

Intercepted Encrochat messages detailed the shipment's plans and included hand-drawn illustrations of the \$79m concealment, a slam dunk for investigators to seize and arrest. Encrochat, once the device of choice for Europe's gangsters, is no more. In June, its operators realised it was under attack and told users: "Due to the level of sophistication of the attack and the malware code, we can no longer guarantee the security of your device ... Power off and physically dispose of your device immediately."

It was too late.

Australian law enforcement agencies were previously involved in a similar feat when they joined forces with the FBI and Royal Canadian Mounted Police to shut down a pioneer of encrypted phones.

Phantom Secure was founded in 2008 by Canadian Vincent Ramos. Not long after, Australian authorities started seeing Mexican drug runners bringing encrypted Phantom BlackBerry devices to town.

"They caught on quite quickly with the local crew. The Comancheros pushed them big time," a law enforcement source tells Inquirer.

When Australian media reported in 2014 that Phantom devices were hampering murder investigations, Ramos privately wrote that it was "the best verification on what we have been saying all along ... it can't get better than that".

Ramos's mistake was to tell undercover agents in Las Vegas that Phantom Secure was built specifically to facilitate drug trafficking. US authorities charged him with knowingly providing crime syndicates with the encrypted infrastructure to carry out their illicit business.

Unlike the later Encrochat bust, Phantom's encryption was never breached. So while Phantom was shut down and Ramos was jailed for nine years, users switched seamlessly to rival products.

In Australia, almost everyone has swapped to Ciphrr. Up to 10,000 Phantom devices were in Australia, or almost half the worldwide users — the same number of encrypted Ciphrr phones now estimated by law enforcement to be in use across the country.

Ciphrr is based in Canada but was pushed hard by former NSW Comanchero Marco Coffen, based in Dubai, who was believed to have secured the Australasian distribution rights, the law enforcement source says.

If you wanted to do business with a Comanchero you tended to have to have a Ciphrr.

Ciphrr phones have vaults within vaults, helping protect drug ledgers and other sensitive data. USB ports are disabled so they can't do anything except charge the phones.

"We have not struck any legitimate companies or businesses using them, because they're very expensive and there's other forms of communication which can be almost as secure and you don't pay the exorbitant fees," the source said.

"You look at really any high-end organised crime arrest or seizure that's occurred in Australia in the past 12 months and there would be very few that didn't involve Ciphrrs."

In Europe, criminals are believed to have predominantly moved to Sky ECC encrypted phones, big with the Hells Angels. If Australian authorities see Sky ECC phones, they suspect an Angels connection.

Other new players are jostling for a piece of the action in Australia, including Diamond Secure, believed by law enforcement to be linked to a former South Australian Hells Angels bikie now based in Europe.

The NSW Crime Commission warned in its 2020 annual report that encrypted networks were "now regarded as essential tools for organised crime networks".

It said it was essential "that both the commission and other Australian law enforcement agencies develop long-term strategies" in response.

# Living with PTSD? We Can Help

Moving Beyond Trauma is a 5-day residential program at the Quest for Life Centre in Bundanoon, NSW designed to assist people with PTSD reclaim their lives.

The program draws on an understanding of trauma, its effect on the brain and teaches practical skills and tools which bring relief to the troubled body, mind and spirit.

Based on the latest research on health, healing and neuroscience, our nationally acclaimed programs are delivered by a highly qualified professional team in a safe and confidential environment.

## 2021 Programs

15-19 March  
3-7 May

12-16 April  
7-11 June

Call **1300 941 488** or visit  
**[www.questforlife.com.au](http://www.questforlife.com.au)**

NDIS Provider. Fully subsidised places available for people affected by Domestic Violence. Speak to us if you're covered by worker's compensation.



Special Offer for *AiPol*  
*Police Journal* readers

**\$200 off**

the program fee if you mention  
*'AiPol Police Journal'* when booking



**[www.greenzonesolar.com.au](http://www.greenzonesolar.com.au)**

- Mob: 0451 200 046
- Office (03) 8768 9429

Email: [info@greenzonesolar.com.au](mailto:info@greenzonesolar.com.au)

Find us on Facebook & Instagram

Are you looking for an affordable and trustworthy solar panels for home? You don't have to run anywhere in the market, as Green Zone Solar can help you with this!

We are Clean Energy Council Approved Solar Retailers that means you can have confidence when buying solar systems from us!

Servicing Melbourne and surrounds

**Proudly supporting our local Police**





# Decrypted: Phantom Secure takedown a 'significant blow' against Australia's organised crime networks

19 Mar 2018

**SARA BARKER**

---

A collaborative effort by Australian, US and Canada law enforcement agencies has busted a Canadian security firm for allegedly providing secure, encrypted communications to the organised crime market.

Phantom Secure offered encrypted messaging and chat services to customers, according to its website.

However, law enforcement agencies say the company has been providing specially-designed devices for the organised crime market – and may have been the first encrypted communication platform available on a wholesale scale in Australia.

The platform was the single largest supplier to Australia's organised crime market, with approximately 10,000 devices sold in Australia alone.

Criminals were able to use Phantom Secure's services and devices to conduct unrestricted and secure communications 'beyond the capability of law enforcement interception', a press release from the Australian Federal Police says.

"According to court documents, Phantom Secure advertised its products as impervious to decryption, wiretapping or legal third-party records requests. Phantom Secure also guaranteed the destruction of evidence contained within a device if it was compromised, either by an informant or because it fell into the hands of law enforcement," a statement from the US Department of Justice adds.

Phantom Secure has now been dismantled by a number of law enforcement agencies, who worked together to disable the platform and the secure devices used on it.

Five men, including Phantom Secure CEO Vincent Ramos, were indicted in the United States last week. Other men charged include Kim Augustus Rodd, Younes Nasri, Michael Gamboa, and Christopher Poquiz.

According to the Australian Federal Police, the men are charged with "Knowingly participated in a criminal enterprise that facilitated the transnational importation and distribution of narcotics through the sale and service of encrypted communications".

The United States Government was also involved in the takedown through the Federal Bureau of Investigation (FBI). This is the first time the US has targeted a company and its principals for aiding and abetting criminal firms.

"The disruption of the Phantom Secure platform has been one of the most significant blows to organised crime in Australia," comments New South Wales Crime Commission's executive director of Criminal Investigations Division, Timothy O'Connor.

Using this equipment, criminals have been able to confidently communicate securely and control and direct illicit

activity like drug importations, money laundering and associated serious, often violent criminal offending, yet have remained removed from these criminal acts," adds Australian Federal Police Assistant Commissioner of Organised Crime, Neil Gaughan.

The bust was a joint effort between the Australian Federal Police, the US Federal Bureau of Investigation, the Royal Canadian Mounted Police (RCMP), the Australian Criminal Intelligence Commission, New South Wales Crime Commission, New South Wales Police, Queensland Police, Victoria Police, South Australia Police, the Australian Taxation Office and AUSTRAC.

According to RCMP organised crime assistant commissioner Jim Gresham, the investigation is a prime example of law enforcement agencies coming together from around the world and collaborating.

"We remain committed to investigating and disrupting these illegal activities that adversely affect each of our communities."

The Australian Federal Police continues to work with the FBI, RMCP and other partners on the case. Further arrests and charges have not been ruled out.

Authorities are also aware of similar platforms, some of which have direct connections to Phantom Secure, which are also under investigation.

# No Backdoors: Investigating the Dutch Standpoint on Encryption

Policy & Internet, Vol. 10, No. 2, 2018

**JEROEN VEEN AND SERGEI BOEKE**

## Abstract:

The use of end-to-end encryption services by terrorists and criminals has led many of the world's security and law enforcement agencies to emphasize the need for exceptional access: a backdoor in encryption. The debate involves governments and private parties, and can be approached through the different prisms of privacy, national security, and economics. This article provides historical background and context on the issue of government access to encryption, before focusing on the Dutch government's position on encryption. In January 2016 the Netherlands was the first country to adopt an official and unambiguous standpoint that ruled out backdoors in encryption. Building on interviews conducted with policymakers in various ministries, the authors elucidate the decision making process and identify key factors that led to the government's position. The impetus provided by Parliament, the role of the NGO Bits of Freedom, and an approach that transcended sectoral interests all contributed. While the unique political context and culture of the Netherlands complicates the application of lessons identified to other countries, the case study does illustrate how a multistakeholder process can lead to a clear standpoint of ruling out backdoors in encryption.


**Key words:** encryption backdoors, exceptional access, privacy, national security, cybersecurity policy, encryption policy

## Introduction

Following a wave of terrorist attacks in 2015, most notably the Charlie Hebdo shooting in Paris, the issue of encryption again became subject to political debate in various Western countries. The debate, like earlier debates in the 1970s and 1990s, focused on which types of encryption should be available to the general public and whether government agencies should have access to the

public's encrypted data, by means of a special access backdoor. On one side, law enforcement agencies and/or intelligence and security services have argued that encryption has prevented them from accessing terrorists' and criminals' communications. In political discourse this has been described as terrorists having "safe spaces" online, with law enforcement agencies "going dark" (BBC, 2017; Comey &

Yates, 2015). On the other hand, digital rights movements and academics, particularly from the technical community, have pointed out how weakening encryption affects not just the target group of terrorists and criminals, but also negatively impacts everyone using encrypted services (Abelson et al., 2015). This debate is still ongoing, with several governments espousing the contradictory position of emphasizing



the importance of encryption, while at the same time seeking to compel service providers to undermine it by building in special access measures (Abelson et al., 2015; Anderson et al., 1998).

The dilemma surrounding encryption is not new. A similar debate played out in the 1990s when the Clinton administration proposed inserting a chip (the “Clipper Chip”) into mobile phones to allow government agencies to bypass the encryption of mobile voice calls. Government access was to be limited to specific circumstances, and only when permitted by a warrant. In what is referred to as the first “Crypto Wars,” the U.S. debated building backdoors into software, weakening encryption standards, and imposing (further) restrictions on the export of encryption technology. The Clipper Chip was eventually dropped and the U.S. government relaxed export controls on encryption technologies (Blaze, 1994; Kehl, Wilson & Bankston, 2015). After the start of the Snowden leaks in 2013, the demand for end-to-end encryption in communication services increased significantly, with new applications such as WhatsApp and Signal incorporating this by default. At around the same time, the Islamic State/Daesh terrorist group began carrying out attacks in the United States and Europe, and in several cases encrypted communications services were used in preparing these attacks (Sanger & Perlroth, 2015; Sehabat, Mitew, & Alzoubi, 2017). The debate on encryption has pitted law enforcement proponents arguing for exceptional access, against privacy advocates, large companies, and the IT community advocating ubiquitous encryption.

Some governments have been more explicit on the issue of encryption than others. In the United States, the Federal Bureau of Investigation (FBI) took Apple to court to obtain access to an iPhone after the San Bernardino attack in December 2015. The FBI wanted access to the deceased terrorist’s phone; Apple said it did not possess the access code and did not want to compromise security for all its customers (Farivar, 2016). The FBI dropped the case when it managed to break the encryption of the phone in question, allegedly with the assistance of an Israeli company called Cellebrite (Fox-Brewster, 2018). Ultimately, the case was not about unlocking a single phone (which was eventually done by exploiting existing weaknesses), but the FBI’s desire to be able to access any iPhone with a warrant (Zetter, 2016). President Obama proposed a middle way during an interview in 2016, stating “You cannot take an absolutist view on this. If your view is strong encryption no matter what and we can and should create black boxes, that does not strike the balance that we’ve lived with for 200 or 300 years. And it’s fetishizing our phones above every other value. That can’t be the right answer” (Machkovech, 2016). While there is an ongoing debate between tech companies and governments on what the former should do to limit terrorist use of their platforms, many governments seem to avoid official standpoints on encryption. There is one exception: the Netherlands. In 2016 the Dutch government published a statement that supported encryption in principle, and opposed interference with encryption methods. This was a somewhat remarkable departure from Dutch developments in the 1990s, when

a draft law proposed to ban cryptography from those without an official license (Koops & Kosta, 2018).

This article investigates the 2016 Dutch Cabinet position on encryption, focusing on how and why the government reached its official standpoint. We first provide some background on encryption, backdoors and the public debate, and then discuss three different approaches to the dilemma of exceptional access. Recognizing that the broader domains of economics, national security, and privacy are impacted by encryption, the article develops these prisms as reference frameworks for the debate. By formulating the advantages and disadvantages of backdoors when approached through the prisms of economics, national security, and privacy, a comprehensive overview of competing values can be elucidated. We then describe the process leading to the Dutch government’s position on encryption and the actors involved. To do this, we have used official documents and conducted confidential semistructured interviews with civil servants, politicians, and representatives of NGOs that were involved in the formulation of the government standpoint. Following the analysis, we can identify several factors that have contributed to this outcome. While these factors are in some cases tied to the unique political context and culture in the Netherlands and thus cannot be transposed directly onto other countries with different institutional arrangements, they can offer potential lessons for situations where the pendulum has still not swung one way or the other.

---

*continued on page 16*





## The Debate on Encryption

Encryption is, arguably, a fundamental technology that underpins the Internet and (cyber) security as a whole. It helps ensure that the transmitter and designated recipient of personal messages (or the holder of certain data) remain the only parties that have access to the content. In the 1970s, Diffie and Hellman introduced the concept of public and private keys to enable secure communications over a public medium (Diffie & Hellman, 1976), and this was implemented in one of the first public-key cryptosystems, described by Rivest, Shamir and Adleman in 1977 (and subsequently known by the acronym "RSA"). The resulting communication possibilities contributed to the notion that cryptography could pose a problem for national security (Levy, 2001). For a government, gaining access to communications is sometimes necessary to safeguard (national) security or as a part of law enforcement. There are various names for concepts that facilitate

ex ante access, including golden keys, use of key-escrow and backdoors. While these work in different ways, they all result in a third party being able to access the content of two other parties' communications. This option has to be built into the product. Other methods for ex post access include the traditional wiretap and decryption orders. Both, however, can be problematic. Lawful interception of communications that are end-to-end encrypted is impossible; even the telecommunication providers do not possess the cryptographic key to unlock the content. As for decryption orders, these can violate the privilege against self-incrimination, a fundamental right in many jurisdictions (Koops & Kosta, 2018). Moreover, this method is more suited to law enforcement, and is generally predicated on having the suspect (and device) available. This is often not the case in intelligence work, where, for example, a possible terrorist suspect is not yet a suspect as defined by criminal law.

The ensuing debate on encryption did not focus on special access itself but rather on the technical (mostly mathematical) notion that the addition

of special access to encryption protocols weakens these protocols. The Internet's technical community, responsible for the development of standards and protocols, has traditionally been skeptical of government interference in this field. In 1996, the Internet Engineering Task Force (IETF) published a memo on the importance of cryptographic technology as Request For Comment (RFC) 1984; alluding to George Orwell's literary masterpiece on surveillance (IETF, 1996). The first major instance where intelligence agencies feared that they would "go dark" occurred when encryption was built into mobile phones (then delivering just voice services). In part to mitigate this, the U.S. National Security Agency (NSA) developed the Clipper Chip to be added to these phones to allow law enforcement special access (Kehl et al., 2015). In the end, the Clinton administration stopped the Clipper plans, both because they could technically be bypassed and for market reasons (Blaze, 1994). While U.S. companies could legally be obliged to build in the chip, this was not the case for companies based outside the United States. As such, global

***“The question we must ask ourselves is whether, as technology develops, we are content to leave a safe space—a new means of communication—for terrorists to communicate with each other. My answer is no, we should not be”***

Then UK Prime Minister David Cameron

businesses and individuals could just buy a non-U.S. product if they wanted a product without a back door (Kehl, Wilson, & Bankston, 2015).

This first so-called “crypto war” was predominantly a U.S. affair. The recent debate, labeled the “second crypto wars” by some, is more international in scope. Governments in Europe and Australia have called for backdoors while other countries like Russia, China, and India have taken action to limit encrypted services (Australian Government, 2018; Kravets, 2015; Lomas, 2016; Mozur, 2015). This time, the exceptional access requested is not achieved by inserting a chip into a phone, but requires adapting the code of hardware (e.g., phones) as well as software, such as messaging platforms, to allow special access. Nevertheless, in essence the debate revolves around the same principles, as attested by several publications. In the 1990s, a joint paper by a group of technical experts in the field concluded: “The deployment of key-recovery-based encryption infrastructures to meet law enforcement’s stated specifications will result in substantial sacrifices in security and greatly increased costs to the end-user” (Anderson et al., 1998, p. 9). In 2015, a new paper by some of same authors stated: “We have found that the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago” (Abelson et al., 2015, p. 2).

The position toward encryption varies significantly among nation states. Three main categories can be identified.

First, there are countries like Russia and China that force service providers to comply with stringent national laws. Russia banned the messenger application Telegram in 2018, although it remains widely accessible through virtual private networks and the number of users has actually increased since. India has requested that Internet Service Providers explore how Instagram/Facebook/WhatsApp/Telegram and other mobile apps can be blocked on the Internet (Pahwa, 2018). A second category consists of countries that emphasize the dangers of encryption to national security and law enforcement, and propose legislation to prevent their agencies “going dark.” Examples are Australia, France, the United Kingdom, and the United States. The third category involves nations that have clearly stated that strong encryption is a positive development and resist calls to support the incorporation of back doors. The Estonian government agency that coordinates cyber security, for example, has argued that building back doors into e-services would significantly reduce trust in the digital state, and therefore opposes it in principle (Information System Authority, 2017). The Netherlands, however, seems to be the only country that has to date formulated an official government standpoint on the issue.

The spate of terror attacks in France was instrumental in reigniting the debate on encryption in Europe. While not the first attack by Islamic terrorists, the shooting at the office of Charlie Hebdo in January 2015 was followed by multiple terrorist attacks, leading to a firmer

political demand for access to encrypted data. In 2016, the French Interior Minister proposed a global initiative to tackle the problems encountered due to encryption, and planned talks with his German counterpart, stating “Messaging encryption, widely used by Islamist extremists to plan attacks, needs to be fought at international level” (Masnick, 2016). Earlier that year, the French Parliament voted in favor of fines for technology companies that did not cooperate fully in investigations linked to terrorism (France-Presse, 2016). At the time of writing, the debate on encryption is still current in France, though the political climate is more nuanced than at the start of 2016. At that time, the French government was contemplating laws that would outlaw strong encryption altogether (Howell O’Neill, 2016b). Nonetheless, the French Secretary of State said that encryption backdoors were “not the right solution” (Howell O’Neill, 2016c; Thomson, 2016).

The U.K. government, after several terrorist attacks on British soil, also made strong statements on the issue of encryption. In 2015, Prime Minister David Cameron stated: “The question we must ask ourselves is whether, as technology develops, we are content to leave a safe space—a new means of communication—for terrorists to communicate with each other. My answer is no, we should not be” (Bienkov, 2015). Cameron appeared to question whether any form of communication that is not readable by the government should be allowed to exist (Gilbert, 2015). The nation’s signals intelligence service, the Government Communications Headquarters (GCHQ), surprisingly took a more nuanced position, with its director speaking out against weakening end-to-end encryption and adding backdoors (Weitzner, 2016). In a response to a E.U. Council questionnaire, the U.K. noted that their law enforcement authorities “almost always” encounter encryption in the course of criminal procedures. The U.K.’s Investigatory Powers Act, which was made law at the end of 2016, allows the executive to compel communication providers to remove encryption applied to any communications or data. Many analysts, however, recognize that this will face significant practical challenges (Hern, 2017).

---

*continued on page 18*





## Three Prisms on Encryption

There has been no shortage of academic literature on encryption. Much research, however, has been confined to well-defined and narrow conceptual frameworks. Using both qualitative as well as quantitative data, Sivan-Sevilla (2018) illustrates that privacy is often lost to national security in the U.S. policy process. Mueller and Badiei (2019) argue that the popular assertion that human rights can be advanced through the design of the Internet's architecture and standards is not borne out by the evidence. Not only can different rights conflict with each other, it remains difficult to foresee how certain technologies will affect these rights, and designers' intentions are often dictated by economic incentives, laws, and policies. An exploration by Wolff (2016) found clashes between opposing factions in the security debate displaying similar vocabularies but leading to contrasting conclusions, rooted in differing views on the ingredients for a secure Internet. These detailed analyses constitute elements of the broader societal debate on the benefits of encryption, and a holistic approach should integrate values and principles from different domains. From a

conceptual standpoint, three overarching prisms can be distilled through which actors approach encryption technologies. These encompass economics, national security, and privacy. Each of these three core concepts is impacted by encryption. When used as a singular prism for analyzing its effects, they determine to a large extent the position taken in the debate. The arguments transcend national frontiers, although the behavior of states and the role of geopolitics influences practicalities. After all, the technical and business community, as well as the nongovernmental sector that promotes (digital) human rights, are international in their outlook and advocacy. Each community or sector has specific interests to defend in the debate on encryption, and their particular arguments and concerns merit an in-depth analysis.

### The Economic Prism

The economic arguments for strong encryption can revolve around demand, supply, and the ability of states to regulate or influence the behavior of global (technology) companies. From the perspective of demand, encryption technology forms the basis of much of the trust in today's economic contracts. Online banking and shopping depend on it. In a report by Hagemann and Hampson (2015, p. 24) that analyzed growth in economic sectors dependent

on encryption, they concluded that "it is clear that there are immense, semiquantifiable benefits to be attributed to the proliferation of strong and easily accessible cryptographic protocols." Besides business requirements, demand for encrypted personal communication increased significantly after the Snowden revelations starting in 2013. Whether warranted or not, perceptions of mass government surveillance have led to a new market for end-to-end encryption (Howell O'Neill, 2015; Kuchler, 2014). In general, though, the primary goal of strong encryption is to protect users against cybercrime, rather than against government eavesdropping.

On the supply side, the companies that provide encrypted services need to abide by different national laws. A case concerning web services provider Yahoo! in 2000—concerning Nazi paraphernalia offered on its U.S. auction website, which was accessible in France—illustrated how digital corporations are just as bound by the jurisdictions of the countries they operate in as companies dealing in physical goods or services (Goldsmith & Wu, 2006). Any change to a state's laws will alter, either positively or negatively, the ability of a company to continue to operate in a given market. Changes to the terms of use and production of encryption technologies will impact an economy, and in particular large sectors that rely



on this technology, such as telecom, Internet, and hosting services. Changes in encryption legislation will also have an impact on other sectors where privacy and confidentiality are paramount, such as legal services, journalism, and finance. If end-to-end encryption is prohibited or by-passed with a backdoor, then trust in the confidentiality of information will be undermined. This could hinder business confidence and diminish the economic climate. Legislation forcing companies to adapt (ex ante) the design of their soft and hardware is, however, much more far reaching than ex post measures, which can only oblige a provider to do what the given technology permits.

While governments have the formal ability to oblige backdoors in encryption, this faces significant practical hurdles. Economic incentives and market dynamics can be just as effective in influencing behavior as government laws, and sometimes pull in an opposite direction (Lessig, 2006). Technology companies like Facebook, Apple, Google, and Amazon have an influence (and wealth and power) that can surpass those of nation states. In August 2018, for instance, Apple was the world's biggest company by stock value, with its market cap reaching a trillion dollars. This is considerably more than, for instance, the Dutch GDP, and the company's revenues surpass those of most of the world's governments (Galloway, 2017). By implementing end-to-end encryption, Apple can effectively set the world standard for communication security, and the chances are slim that any liberal democracy will deprive its citizens of access to the latest iPhone technology. The U.S. could feasibly force Apple to comply with new U.S. laws on backdoors, but the political will to really do so seems lacking. As of yet, the American executive branch has been extremely reluctant to regulate digital behemoths such as Apple and Google. These market leaders share a strong position on encryption, as formulated by the Information Technology Industry Council that represents them and many others: "[w]eakening security with the aim of advancing security simply does not make sense" (Gibbs, 2015). If the technology sector unambiguously implements end-to-end encryption, there is little that states, especially small ones, can do to prevent this.

From a customer or consumer perspective, a globalized economy

offers a plethora of retailers from which to choose. If a country wants to ensure lawful access to communications, it will need to ban all applications like WhatsApp, Telegram, or Signal, or force them to install backdoors. Either they choose an absolute path whereby every service is brought under the country's control by banning popular Western services and platforms, or they permit them, thereby allowing the customer free reign. China has successfully banned many Western sites and services, including Google, Facebook, and YouTube, replacing them with alternative platforms such as Weibo and WeChat; services that must comply with the government's censorship and surveillance requirements (Chin, 2017). Half-way options, such as the Russian blockade of the Telegram website will probably remain ineffective and leave citizens the option of using other available encrypted services (Marechal, 2018). In the modern era the availability of such products is evident: a 2016 study showed the existence of "865 hardware or software products incorporating encryption from 55 different countries" (Schneier & Seidel, 2016). Encrypted services are proliferating, and according to the economic prism this is both a positive development and one that governments should not hinder.

### **The National Security Prism**

The national security prism produces the most outspoken proponents of curbing encryption technologies. From a principled view, there has never been a space, area or communication platform that has been inaccessible to government when deemed necessary and in accordance with a warrant. Privacy, after all, while a fundamental human right, is not an absolute one, and in some cases must be weighed against other collective values. As the Australian Prime Minister Malcolm Turnbull has argued, "the privacy of a terrorist can never be more important than public safety. Never." (Grant, 2018). Whether opening letters, accessing properties and planting microphones/cameras, or eavesdropping on communications, governments have always possessed lawful access, and have often handled it in legally correct fashion, ensuring that the infringement on privacy was targeted, limited, and proportional. Now, many current crimes are coordinated through online

services—often encrypted—leaving security and law enforcement agencies unable to solve or prevent crimes. In 2017, James Comey, Director of the FBI, described this as an increasing shadow in the room: "First six months of this fiscal year, FBI examiners were presented with over 6,000 devices for which we have a lawful authority search warrant or court order to open and 46 percent of those cases we could not open those devices with any technique. That means half of the devices that we encounter in terrorism cases, in counterintelligence cases, in gang cases, in child pornography cases, cannot be opened with any technique. That is a big problem. And so the shadow continues to fall." (Washington Post, 2017).

Various other governments, including those of the U.K. and the Netherlands, have similarly cited the problem of law enforcement agencies "going dark" (Bienkov, 2015; Pelgrim & Kas, 2015; Vance et al., 2015). This contrasts with the idea that we are currently in a golden age of surveillance (Swire & Ahmad 2012, p. 470), where ubiquitous interconnectivity allows security services access and insights that was previously impossible. Nonetheless, the security sector is not monolithic in its outlook—with national security services generally arguing for backdoors, but foreign intelligence agencies, and specifically signals intelligence services, instead supporting strong encryption. As such, the directors of both the NSA and GCHQ have spoken in favor of end-to-end encryption and against undermining it through the installation of backdoors. These signals intelligence (and cyber) agencies are tasked with keeping national communications secure, while at the same time breaking the encryption of their state and non-state adversaries. Security and intelligence services operate in a different regime/paradigm than law enforcement agencies, with other laws, organizational cultures, and modus operandi (Boeke, 2017a). According to the former director of the NSA and CIA Michael Hayden, "encryption is a law enforcement issue more than an intelligence issue, because, frankly, intelligence gets to break all sorts of rules, to cheat, to use other paths." (Howell O'Neill, 2016a). For Hayden, intelligence agencies can circumvent the

---

*continued on page 20*

problems posed by encryption through bulk data and metadata collection. Since the precise capabilities and limitations of these techniques remain classified, a good open source cost/benefit analysis of limiting encryption versus metadata collection is still lacking.

The argument from the national security prism is therefore a principled one.

Governments have always reserved the right of exceptional access to private communications, in the interest of public safety. Security services and law enforcement agencies infringe, by their very nature, on the privacy of a targeted few, but must do so legally and proportionally. The creation of “safe spaces,” where terrorists, criminals, and pedophiles can “roam unimpeded” is therefore undesirable from this position. Nonetheless, law enforcement agencies (and security and intelligence services) can also use lawful hacking as an access technique. Though governments keep asking for ways into encrypted communication, hacking back has arisen over the recent years as a more acceptable option (Koops & Kosta, 2018), with Bellovin et al. (2014, p. 69) concluding that “The use of vulnerabilities to accomplish legally authorized wiretapping creates uncomfortable issues. Yet we believe the technique is preferable for conducting wiretaps against targets when enabling other methods of wiretapping, such as by deliberately building vulnerabilities into the network or device, would result in less security.” Alongside the exploitation of vulnerabilities, governments can employ companies like Celebrite and Grayshift, which are able to crack encrypted devices. For privacy advocates, it will remain important to distinguish between lawful hacking, collecting metadata, or installing backdoors, as these all have different implications for privacy and national security.

### **The Privacy Prism**

There has been much research on decision making concerning privacy and national security issues, notably in the field of surveillance studies. The privacy prism renders encryption with a backdoor equivalent to no encryption. Privacy advocates advance three main arguments against lawful access; one based on

principle and two on the practical downsides and implications of such a policy. The first focuses on trust: should the government be entrusted with such a capability in the first place, and can it be trusted to use it only in exceptional circumstances and after proper authority? There is a real risk that governments will be unable to resist the temptation of misusing such a powerful capability. The field of Internet censorship provides an example of how many governments across the globe expanded initially limited restrictive policies to more expansive campaigns. Research has shown an increase in the number of governments that conduct Internet censorship. In many cases, censorship expanded from a narrow base, often first starting with pornography but later covering other content categories, such as political opposition sites (Deibert, 2009). This slippery slope of mission creep would potentially also apply to the use of backdoors by states. Why restrict its use to a few counterterrorist cases, when it can also be used to combat fraud?

Second, once a company has installed a backdoor in a communication service or platform for one government, other governments will probably want one. This would oblige the company to devise a cryptographic system with hundreds of additional keys (one for every agency per country that must execute exceptional access warrants) on top of the single pair of private and public keys per user that they would normally design. This would enormously complicate the software, and from a technical perspective, weaken its security. Some governments have already weakened collective security for national security purposes, such as the NSA manipulating the random number generators that form the basis of RSA security protocols, requiring users to switch to different forms of cryptography once this became known (Checkoway et al., 2014; Menn, 2014). For built-in backdoors the design would be inherently problematic to manage. The third argument concerns the security of the decryption keys. By incorporating a backdoor, complexity not only weakens encryption, but new vulnerabilities revolving around key access and storage are created. These cryptographic keys would be a prime target for hackers, whether nation state or criminal. Both the NSA and CIA, arguably amongst the

most technically advanced and secure organizations in the world, have already had their top-secret offensive toolkits leaked or stolen through the Shadow Brokers (for Eternal Blue and other exploits) and Vault 7 (for other access vectors) (Weaver, 2016). The leaked NSA exploits were later used in the WannaCry Malware that struck a multitude of victims in 2017 and caused billions of dollars of damage across the world. A compromise of decryption keys would have an even greater destructive effect: it would render the whole encryption system useless. From a practical perspective, therefore, it is inconceivable that the world's nation states—competing on many levels—will be able to keep a backdoor key secret. It would also quickly become of use to the world's foreign intelligence agencies conducting espionage operations in each other's countries.

Mandates to put backdoors in encryption have also been viewed as damaging for human rights beyond the right to privacy. It is commonplace in certain regimes for governments to exploit intelligence collection to enhance their political stranglehold of a country, using data to seek out and clamp down on dissenters (Human Rights Watch, 2017; Kaye, 2015). Thus, preventing the installment of backdoors not only preserves privacy, but enhances freedom of speech and provides security for the individual. The debate between the prisms of national security and privacy can henceforth be seen as a debate between collective security and personal security. But these concepts overlap to an extent: privacy advocates have correctly identified the risks of abuse by states and argue that such a breach of personal security will eventually also negatively impact collective security. A statement by ENISA and the European Union Agency for Law Enforcement Cooperation (Europol) has phrased similar sentiments: “While this would give investigators lawful access in the event of serious crimes or terrorist threats, it would also increase the attack surface for malicious abuse, which, consequently, would have much wider implications for society” (Europol and ENISA, 2016). Interestingly, privacy and economic prisms seem to come to more or less the same conclusion for this particular debate, with protected privacy and security—without backdoors—seen as an enabler for a growing digital economy.



## The Official Dutch Standpoint on Encryption

On the 4th of January 2016, the Dutch Minister of Security and Justice sent a letter to Parliament outlining the Cabinet's position on encryption. The five-page paper described the different dilemmas involved, the importance of the topic and the potential impact of certain choices on Dutch society. It concluded with the official position that the government promised to extol internationally. The letter was signed by two ministers—the Minister of Security and Justice, and the Minister of Economic Affairs. The difficulty of striking a balance between the different issues at stake was described in detail: “There are currently no options in a general sense, for example, via standards, to weaken encryption products without compromising the security of digital systems that use encryption. For

instance, introducing technical access into an encryption product would make it possible for investigation services to inspect encrypted files, digital systems can become vulnerable to, for instance, criminals, terrorists and foreign intelligence services. This would have undesirable consequences for the security of communicated and stored information and the integrity of IT systems, which are increasingly important for the functioning of society” (van der Steur and Kamp, 2016, p. 4).

The final paragraph stated the official position: “The cabinet endorses the importance of strong encryption for Internet security to support the protection of personal privacy of citizens, for confidential communication of the government and companies and for the Dutch economy. The cabinet is therefore of the opinion that at this point in time it is not desirable to take restrictive legal measures as regards the development, availability and use of encryption in the Netherlands.” (van der Steur and Kamp, 2016, p. 4). This official statement on

encryption, which seemed to appear out of the blue, was covered by various international news sites (BBC, 2016; Hackett, 2016; Moody, no date; Schneier, 2016). The hedge in the last sentence—“at this point in time”—is superfluous from a legal perspective as governments can always change policy. After the Parliamentary elections in 2017 and the formation of a new government, the position on encryption was maintained. From an international perspective, the Dutch Cabinet position remains unique. In other countries, there has been no shortage of government departments, Cabinet ministers, and Parliamentary representatives giving statements on the merits or risks of encryption. The policy process in the Hague weighed all the different governmental and societal interests to come up with an integrated and comprehensive standpoint, which was then communicated to Parliament (and abroad) as the official Dutch position.

---

*continued on page 22*



To investigate how this official standpoint came into being, one of the authors interviewed several policymakers directly involved in the interministerial process on the issue. The civil servants worked for the ministries of Defence, Economic Affairs, and Justice and Security. Another interviewee was an aide to a member of Parliament. In addition, a representative of the Dutch NGO *Bits of Freedom* (BoF) was consulted. The interviews were conducted in a semistructured fashion, but all participants working for the government requested that their names not be published. In addition, the minutes of Parliamentary debates were consulted. While this approach has provided valuable insights into the closed process of government decision making, there are limitations to this methodology. Points raised by individual interviewees were often corroborated by the others, but it cannot be excluded that certain developments and negotiation dynamics were missed or not well represented in the interviews. The first section below describes our findings relating to the overall process, the second section places the interviewees' considerations in our framework of prisms.

### Parliamentary Process

Parliament played an important role as a catalyst for the government position. In its introduction, the government letter stated that the official standpoint was a follow-up to a pledge made during two Parliamentary debates. In the debate on June 10, 2015, Kees Verhoeven, a member of Parliament for the D66 party, asked for the Dutch Cabinet's reaction to the French and U.K. governments' proposition that encryption should have a backdoor. This was but one of many issues discussed during the debate; most time was spent on the topics of net neutrality and roaming. Henk Kamp, the Minister of Economic Affairs, initially replied to Verhoeven's question that the topic of backdoors was a rather complicated issue requiring a balanced approach, and that he himself had not taken a position either way. When Verhoeven returned to the subject of encryption at the end of the debate, Minister Kamp replied that he would deliberate whether to address this together with the Minister of Security and

Justice, and that he would come back to the issue in due course (Tweede Kamer Der Staten-generaal, 2015b). As the Dutch Second Chamber (lower House of Parliament) monitors (and influences) government policy through written questions and Parliamentary debates, questions in debates can require a subsequent written response from the government. In this case, the minutes of the debate indicate that the pledge to work out a Cabinet position was soft (and without a deadline), implying a strong role for Minister Kamp in starting the government process. In the second parliamentary debate noted in the standpoint, encryption and backdoors are mentioned in relation to capabilities for law enforcement. The then Minister of Justice & Security (van der Steur) mentioned that there was no national position on encryption yet but the minutes finished with a summary of commitments, in which a cabinet standpoint on encrypted communication is recorded, to be communicated to Parliament within a month (the session was on October 7, 2015) (Tweede Kamer Der Staten-generaal, 2015a).

As a result of the question by Kees Verhoeven, the government initiated the process to formulate a position on encryption. In principle, the ministry/minister responsible for the topic takes the lead in formulating a policy response, aligning with other government departments where necessary. Unique here is that the Minister of Economic Affairs initiated the policy process, but that the lead/coordinating authority was fulfilled by the Ministry of Justice and Security, in close cooperation with several other ministries. In the Netherlands, the lead ministry for coordinating cybersecurity was the Ministry of Security and Justice, also responsible for the National Cyber Security Centre (NCSC) (Boeke, 2017b). As the issue of encryption also concerned the intelligence and security services, the two ministries responsible for these agencies were involved in consultations; the Ministry of the Interior for the General Intelligence and Security Service (AIVD) and the Ministry of Defence for the Military Intelligence and Security Service (MIVD). A civil servant from the ministry of Foreign Affairs also joined the interdepartmental deliberations. A cryptographer was also involved in all the discussions, and according to the

interviewee from the Ministry of Economic Affairs, played an important role in the process. As encryption is built on mathematical concepts, which neither the average citizen nor the average politician is familiar with, policy options that seem like a good idea can prove to be impossible when studied in detail, such as the golden key. By involving technical expertise, the process did not lead to unrealistic policy propositions. The civil servants interviewed indicated that the process of reaching a common position was not an easy one. The plan was to have the letter ready before the Christmas recess; in the end it appeared in early January 2016. The interdepartmental process did not vary much from regular procedures, and the output here was focused on formulating a policy position rather than legislating new law. Several interviewees mentioned that the discussions started out from different "entrenched positions" and that these only softened as the negotiations advanced. They emphasized how mutual respect and an understanding of the different interests—by first allowing for clarification of interests before exploring whether these could be catered to concurrently—contributed to the final government position. While the end result transcended the initial partisan approach of the different government representatives, the interviews corroborate how initial reasoning followed the three prisms.

### Transposing the Three Prisms

The Ministry of Economic Affairs was concerned about the market's free access to encryption technologies, and the reputation of the Netherlands in safeguarding Internet freedom. Dutch economic growth is greatly dependent on ICT; national and international companies doing business in the Netherlands need to be able to trust governmental policy and the integrity of encryption. Were backdoors to be made compulsory, the Ministry feared this would damage the Netherlands' international reputation and reduce its attractiveness to international IT companies. Contrasting with the debate on exceptional access, the Ministry of Economic Affairs renewed funding for the further development of open (i.e., freely adoptable, implementable, and extendable) encryption standards (Miltenburg, 2015). But the Ministry

***The availability and use of high-grade encryption is essential for the protection of our digital infrastructure and communications. It is not only important for our democratic freedoms, but also vital for innovation and economic growth.***

did not limit itself to the economic prism—the policymaker interviewed specifically mentioned that the NGO *Bits of Freedom* (which itself operates mostly from a privacy prism) was consulted—perhaps a demonstration of the common ground between privacy and economic prisms on the topic of backdoors. *BoF* subsequently delivered objective sources that helped answer questions raised during the process. In turn, *BoF* claimed it represented a wide consensus against backdoors from different areas of the market, including hardware providers, service providers, and notably, the provider of cybersecurity solutions to the Dutch government; Fox-IT. Dutch civil servants also made some use of other governments' deliberations on the issue of encryption.

Interviews with officials from the Ministry of Defence and the Ministry of Justice and Security accentuated how policy reasoning transcended departmental boundaries. While driven by the interests of national security, officials described a balanced approach in the interviews, sketching how the policy process incorporated broader dilemmas. For Defence this initially meant a narrow position that would both support the encryption of its own systems and communications, and allow the MIVD to execute lawful interception of communications (predominantly abroad). As the MIVD worked within the framework of the Law on Intelligence and Security Services, the Ministry of Defence judged that this framework provided a sufficient mandate. Perhaps as with the U.S. and U.K. signals intelligence services, encryption was seen as more of a national security

issue than a foreign intelligence one. As such, balancing security and privacy was seen as a task for government and not the ministry, and according to the interviewee, Defence in no way pushed for backdoors in encryption. At that time, the new law for intelligence services was under consultation in Parliament, which offered the services new possibilities for bulk interception and use of metadata in targeted collection (Eijkman, van Eijk and van Schaik, 2018). This law has since been passed.

Furthermore, the Ministry of Defence also showed signs of reasoning through the economic prism. As many private sector companies supply the ministry with services (notably the Dutch telecommunication provider KPN), the Defence sector was concerned that backdoors in encryption would complicate their relationship with this sector. Many departments within the Ministry of Defence were dependent on private sector parties, and unable to fulfill important national security missions without their support and service. The official in the coordinating Ministry of Security and Justice equally emphasized balancing the needs of specific government agencies with security for society as a whole. The ministry of Economic Affairs, and in particular the Ministry of Foreign Affairs, promoted the importance of human rights and privacy during the process. According to one interviewee, the mentioning of “fundamental rights and liberties” in the official statement primarily came from the Ministry of Foreign Affairs. This ministry actively supported fundamental rights and freedoms abroad (in a variety of settings

and topics), and later mentioned the encryption standpoint in its international cyber strategy (called “Building Bridges”). It was referenced under the header “the right to personal data protection and the right to privacy” (Ministerie van Buitenlandse Zaken, 2017).

Much of the pressure from Parliament on the issue of backdoors focused on the issue of privacy. Two members of Parliament stand out in their advocacy for encryption: Kees Verhoeven (D66) and Astrid Oosenbrug (PvdA). The first was most active, and as a member of a relatively small opposition party at the time, Verhoeven was able to put several items concerning technological developments and human rights on the political agenda. His party was one of the few to present a technological vision, in which encryption was described as a fundamental right, emphasizing its importance for both economic development and democratic freedom (Verhoeven et al., 2016). The Dutch electoral system of proportional representation results in many parties, allowing each to cater for different niches in the political landscape. Oosenbrug, whose party was a member of the governing coalition, was less prominent on the issue, but did submit Parliamentary questions on encryption focusing on privacy on a number of occasions, sometimes together with Verhoeven (Tweede Kamer Der Staten-generaal, 2017b, 2017a), keeping the pressure on the government to both formulate a standpoint and then extol and support it. According to the interviewee at the Ministry of Security and Justice, the questions and remarks of these well-informed Parliamentarians also helped the civil servants in their conviction to reach a common position on encryption.

As an NGO, *Bits of Freedom* was successful in conveying its position on encryption to the general public, politicians, and civil servants alike. After the Cabinet position was released, *BoF* expressed satisfaction (except concerning the “for now” statement) but stressed that more support and structural investment in digital security was needed. The NGO subsequently published a position paper that stated the following: “The availability and use of high-grade encryption is essential for the protection of our digital infrastructure and communications. It is not only important for our democratic freedoms, but also

vital for innovation and economic growth" (BoF, 2016, p. 2). On the later concept of "hacking-back" by government agencies, BoF commented that this seemed to be more in line with regular work of intelligence agencies but wondered what would be done with generic vulnerabilities in software and hardware found during the process (Zenger, 2016). This seems to express a position that ex-post usage of weaknesses that stem from the normal design and implementation of technology are less of a problem than ex-ante predefined weaknesses that must be taken along in development.

There were few other external influences on the internal policy process. The questions in Parliament constituted the catalyst for the objective of formulating a common position, but this was not followed by additional direction or time pressure from MPs. Some of the Parliamentarians considered the whole decision making process a black box, and they had little indication of which position would emerge or when. The timing and broader context of the process did, however, favor strong encryption. One of the civil servants had informally brainstormed on the topic with Jaya Baloo, the chief information security officer of KPN, who had a very public profile. With the Snowden revelations still resonating in the media, Baloo had presented a keynote speech during the ONE conference in April 2015 (organized by the Dutch NCSC), wishing that everyone would "live long, laugh a lot and encrypt everything" (Zaske, 2015). According to the interviewee at the Ministry of Economic affairs, a document from the Obama administration was used in the interministerial policymaking process. This report concluded that all options for backdoors had significant drawbacks (Anonymous, 2015). There was little contact with policymakers from other countries regarding the deliberations on encryption. For the Ministry of Justice and Security, differences in how other countries had organized their departments were considered a complicating factor.

### Aftermath

Some months after the publication of the Cabinet's standpoint, the government prosecutor for cybercrime and the director general of the AIVD commented

in the media on how encryption posed problems for their fields of work. In August 2016, prosecutor Martijn Egberts stated that he wanted the ability to access—with a warrant—WhatsApp and other encrypted communications (Schellevis, 2016). This led to Parliamentary questions from Oosenbrug and Recourt (both members of the PvdA party, then part of the governing coalition). In its response, the government referred to its official standpoint on encryption (Tweede Kamer Der Statengeneraal, 2017a). In September 2016, Rob Bertholee, then director general of the AIVD, made the case for backdoors in encryption during an extensive interview with the *Volkskrant*, a major Dutch newspaper. Noting the unprecedented threat of terrorism and terrorists' use of end-to-end encryption, he openly questioned the official position and argued the case for exceptional access (Modderkolk, 2016). In October 2016 MP Kees Verhoeven again submitted written questions on the government's position vis-à-vis the new French/German initiative regarding an international approach on access to encrypted communications. Here too the government reiterated its official standpoint, indicated that it had been translated into English and that it would be promoted abroad (van der Steur, 2016).

Despite expressions of frustration by senior Dutch civil servants on the policy of no backdoors, the government did pass legislation that provided law enforcement agencies and the intelligence and security services with far-reaching mandates to hack and conduct surveillance of targets. A new controversial law, *Computercriminaliteit III* (cybercrime III), allows the police to hack back and install spyware, and destroy or disable access to files with the notice and take down order (Pool and Custers, 2017). A renewal of the 2002 legal framework mandating the work of the two intelligence and security agencies was also required, and the law (*Wet op de Inlichtingen en Veiligheidsdiensten*/WIV 2017) was passed by Parliament after an extensive consultation process. It became subject to an advisory referendum after four university students managed to collect the required 300,000 signatures, and in March 2018 the referendum was held alongside the municipal elections. With a turnout of

51.5 percent, 49.5 percent voted against the new law, and 46.5 percent for (the remainder being blank votes) (Kiesraad, 2018). After some small adjustments, the government implemented the new law. Nonetheless, calls for backdoors in encryption have continued. In November 2019 the new Minister of Justice and Security (Ferdinand Grapperhaus of the CDA party) called for access to encrypted communications for the justice department in cases where there is proof of suspect behavior (Bouma, 2019). The official standpoint, however, remained intact.

## Conclusion

As surprising as its announcement was in January 2016, the Dutch Cabinet position on encryption was the result of a long process of interdepartmental alignment and coordination. The catalyst for an official standpoint appears to lie in a question asked by a Member of Parliament, Kees Verhoeven, one of the few MPs to focus on topics of information technology and its implications for security and privacy. His party saw the issue not only as an item of importance but also as an opportunity to politically exploit a niche in the fragmented multiparty system of the Dutch political landscape. The government set to work on establishing a formal Cabinet position, with the Ministry of Security and Justice taking the lead and coordinating the interdepartmental process. Various stakeholders inside and outside the public sector were included in the consultations, including the NGO *Bits of Freedom* and technical experts from the intelligence and security services. Once established, the standpoint of ruling out backdoors in encryption was signed by the Minister of Security and Justice and the Minister of Economic Affairs. Later in 2016, as terrorist attacks in France and Germany prompted further announcements from these governments on the need for exceptional access, Dutch MPs requested the government's opinion on these statements. In its replies, the Dutch government referred to its official standpoint on encryption, and that it would promote this position internationally.

Viewing the debate through the three different prisms—privacy, national security, and economics—helps to understand the different positions in the backdoor debate, and illustrates the wide-ranging implications of a binary



decision on the issue. Surprisingly, interviews with the civil servants in different ministries did not reveal a dogmatic reliance on the positions inherent in three prisms. Perhaps the Dutch culture of political consensus—the so-called polder model—contributed. This can be compared with a multistakeholder model where different stakeholders are involved in the decision making process. Considering the unique context of political systems and cultures, it is therefore difficult to extrapolate conclusions from the Dutch case to other countries. Differences in exposure to terrorism may also have allowed for a less heated debate in the Netherlands. While the country did suffer terrorist acts, the frequency and scope of these were more limited

than in countries like the United States, France, and the United Kingdom. This could have contributed to a more balanced political dialogue (with less emphasis on the national security prism), although this was not expressed by any of our interviewees. The Dutch situation highlights that a policy process is possible where NGOs and technical experts are included, and that broader, national interests can prevail over parochial ones. Nonetheless, a multistakeholder approach frequently implies a slow and difficult process, culminating in a trade-off or compromise between different parties. It is therefore remarkable that the Dutch government decision was in no way a compromise, and clearly ruled out backdoors in encryption.

## Note

The authors would like to thank the anonymous reviewers for their valuable comments on earlier versions of the article.

1. These interviews were not recorded but notes were kept. Most of the interviews were conducted on government premises where recording equipment was not permitted. In addition, recording equipment would have influenced the openness of the interviews. Several interviewees requested not to be quoted directly, which is why this article uses paraphrased information.

## References

- Abelson, H., R. Anderson, S.M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, and J. Gilmore, et al. 2015. "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications." *Journal of Cyber Security* 1 (1): 69–79. <https://doi.org/10.1093/cybssec/tyv009>
- Anderson, R., S.M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, and P.G. Neumann, et al. 1998. "The Risks of Key Recovery, Key Escrow & Trusted Third Party Encryption." *Digital Issues*, (3).
- Anonymous. 2015. *read-the-obama-administrations-draft-paper-on.pdf*. <https://assets.documentcloud.org/documents/2430092/read-the-obama-administrations-draft-paper-on.pdf>
- Australian Government. 2018. "Statement of Principles on Access to Evidence and Encryption." *homeaffairs.gov.au*. <https://archive.homeaffairs.gov.au/about/national-security/live-country-ministerial/2018/access-evidence-encryption>
- BBC. 2016. "Dutch Government Says no to 'Encryption Backdoors.'" *BBC.com*. <http://www.bbc.com/news/technology-35251429>
- BBC. 2017. "Theresa May Warns Tech Firms Over Terror Content." *BBC.com*. <https://www.bbc.com/news/uk-politics-41327816>
- Bellovin, S., M. Blaze, S. Clark, and S. Landau. 2014. "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet." *Northwestern Journal of Technology and Intellectual Property* 12 (1): 1–66. <http://goodtimesweb.org/surveillance/2013/lawful-hacking.pdf>
- Bienkov, A. 2015. "David Cameron: Twitter and Facebook Privacy is Unsustainable—Home Affairs." *politics.co.uk*. <http://www.politics.co.uk/news/2015/06/30/david-cameron-twitter-and-facebookprivacy-is-unsustainable>
- Blaze, M. 1994. "Protocol Failure in the Escrowed Encryption Standard." In *Proceedings of Second ACM Conference on Computer and Communications Security*, (April 1993), 59–67.
- Boeke, S. 2017a. "Reframing 'Mass Surveillance'." In *Terrorists' Use of the Internet: Assessment and Response*, ed. M. Conway. Amsterdam: OS Press. <http://ebooks.iospress.com/volume/terroristsuse-of-the-internet-assessment-and-response>
- Boeke, S. 2017b. "Sergei Boeke, 'National Cyber Crisis Management: Different European Approaches'." *Governance* 31 (3): 449–64. <https://doi.org/10.1111/gove.12309>
- BoF. 2016. *Position Paper on Encryption*. <https://www.edri.org/files/20160125-edri-crypto-positionpaper.pdf>
- Bouma, R. 2019. "Minister Grapperhaus wil toegang tot chaten berichtendiensten." *nos.nl*. <https://nos.nl/nieuwsuur/artikel/2308847-minister-grapperhaus-wil-toegang-tot-chat-en-berichtendiensten.html>
- Checkoway, S., R. Niederhagen, A. Everspaugh, M. Green, T. Lange, T. Ristenpart, and D.J. Bernstein, et al. 2014. "On the Practical Exploitability of Dual EC in TLS Implementations." *USENIX Security* 2014: 319–35.
- Chin, J. 2017. "China Targets Social-Media Giants WeChat, Weibo in Cybersecurity Probe." *wsj.com*. <https://www.wsj.com/articles/wechat-weibo-among-targets-in-china-cybersecurity-probe-1502432081>
- Comey, J.B., and S.Q. Yates. 2015. "Statement of Deputy Attorney General Department of Justice and Federal Bureau of Investigation Before the Committee on the Judiciary United States Senate 'Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy' Presente'.
- Deibert, R.J. 2009. "The Geopolitics of Internet Control." In *Routledge Handbook of Internet Politics*, eds. A. Chadwick, and P.N. Howard. London: Routledge, 323–36.
- Diffie, W., and M.E. Hellman. 1976. "Multiuser Cryptographic Techniques." In *Proceedings of the June 710, 1976, National Computer Conference and Exposition on—AFIPS '76*, p. 109. <https://doi.org/10.1145/1499799.1499815>
- Eijkman, Q., N. van Eijk, and R. van Schaik. 2018. *Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence*. Utrecht/Amsterdam. [https://www.ivir.nl/publicaties/download/Wiv\\_2017.pdf](https://www.ivir.nl/publicaties/download/Wiv_2017.pdf)
- Europol and ENISA. 2016. *On Lawful Criminal Investigation That Respects 21st Century Data Protection*. <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawfulcriminal-investigation-that-respects-21st-century-data-protection>
- Farivar, C. 2016. "Feds to Court: Apple Must be Forced to Help Us Unlock Seized iPhone I Ars Technica." *arstechnica.com*. <http://arstechnica.com/tech-policy/2016/02/feds-to-court-apple-must-be-forced-tohelp-us-unlock-seized-iphone/>
- Fox-Brewster, T. 2018. "The Feds Can Now (Probably) Unlock Every iPhone Model In Existence—UPDATED." *Forbes.com*. <https://www.forbes.com/sites/thomasbrewster/2018/02/26/governmentcan-access-any-apple-iphone-cellebrite>
- France-Presse. 2016. "French Parliament Votes to Penalise Smartphone Makers Over Encryption." *theguardian.com*. <https://www.theguardian.com/technology/2016/mar/03/french-parliamentpenalise-smartphone-makers-over-encryption>
- Galloway, S. 2017. "The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google." 1st ed., Portfolio.
- Gibbs, S. 2015. "Apple, Google and Microsoft: Weakening Encryption Lets the Bad Guys in." *The Guardian*, November.
- Gilbert, D. 2015. "David Cameron Preying on Our Fears After Charlie Hebdo Massacre With Encryption Ban Calls." *ibtimes.co.uk*. <http://www.ibtimes.co.uk/charlie-hebdo-massacre-calls-encryption-ban-1483201>
- Goldsmith, J., and T. Wu. 2006. *Who Controls the Internet? Illusions of a Borderless World*. New York: Oxford University Press.
- Grant, M. 2018. "Navigating the Balance Between Privacy and Security." *aspistrategist.org.au*. <https://www.aspistrategist.org.au/navigating-the-balance-between-privacy-and-security/>
- Hackett, R. 2016. "Dutch Government Backs Uncrackable Encryption." *fortune.com*. <http://fortune.com/2016/01/05/dutch-government-encryption-no-backdoors/>
- Hagemann, B.Y.R., and J. Hampson. 2015. *Encryption, Trust, and the Online Economy*. [https://niskanencenter.org/wp-content/uploads/2015/11/RESEARCH-PAPER\\_EncryptionEconomicBenefits.pdf](https://niskanencenter.org/wp-content/uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf)
- Hern, A. 2017. "UK Government Can Force Encryption Removal, But Fears Losing, Experts Say." *theguardian.com*. <https://www.theguardian.com/technology/2017/mar/29/uk-government-encryptionwhatsapp-investigatory-powers-act>
- Howell O'Neill, P. 2015. "The State of Encryption Tools, 2 Years After Snowden Leaks." *dailydot.com*. <https://www.dailydot.com/layer8/encryption-since-snowden-trending-up/>

- Howell O'Neill, P. 2016a. "Former NSA Chief Says U.S. Can Get Around Encryption With Metadata, Argues Against Backdoors." *dailydot.com*. <http://www.dailydot.com/politics/michael-haydenencryption-debate-clinton-bush/?tw=pl>
- Howell O'Neill, P. 2016b. "French Government Considers Law That Would Outlaw Strong Encryption." *dailydot.com*. <http://www.dailydot.com/layer8/encryption-backdoors-french-parliament-legislationparis-attacks-crypto-wars/>
- Howell O'Neill, P. 2016c. "French Secretary of State Says Encryption Backdoors Are 'Not the Right Solution'." *dailydot.com*. <http://www.dailydot.com/politics/france-encryption-backdoors-secretaryof-state-rejection-crypto-wars/>
- Human Rights Watch. 2017. "Perils of Back Door Encryption Mandates: 'Five Eyes' Nations Should Support, Not Threaten, Digital Security." *Human Rights Watch*, June.
- IETF. 1996. "IAB and IESG Statement on Cryptographic Technology and the Internet." *ietf.org*. <https://tools.ietf.org/html/rfc1984>
- Information System Authority, R. of E. 2017. *Annual Cyber Security Assessment 2017 Estonian Information System Authority*. [https://www.ria.ee/public/Kuberturvalisus/RIA\\_CSA\\_2017.PDF](https://www.ria.ee/public/Kuberturvalisus/RIA_CSA_2017.PDF)
- Kaye, D. 2015. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>
- Kehl, D., A. Wilson, and K. Bankston. 2015. "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s." *New America*. <https://static.newamerica.org/attachments/3407-125/Lessons-from-the-crypto-wars-of-the-1990s>
- Kiesraad. 2018. "Uitslag referendum over Wiv: meerderheid tegen." *kiesraad.nl*. <https://www.kiesraad.nl/actueel/nieuws/2018/03/29/uitslag-referendum-over-wiv-meerderheid-tegen>
- Koops, B.J., and E. Kosta. 2018. "Looking for Some Light Through the Lens of 'Cryptowar' History: Policy Options for Law Enforcement Authorities Against 'Going Dark'." *Computer Law and Security Review* 34 (4): 890–900. <https://doi.org/10.1016/j.clsr.2018.06.003>
- Kravets, D. 2015. "UK Prime Minister Wants Backdoors Into Messaging Apps or He'll Ban Them I Ars Technica." *arstechnica.com*. <http://arstechnica.com/tech-policy/2015/01/uk-prime-minister-wantsbackdoors-into-messaging-apps-or-hell-ban-them/>
- Kuchler, H. 2014. "Tech Companies Step up Encryption in Wake of Snowden." *ft.com*. The state of encryption tools, 2 years after Snowden leaks.
- Lessig, L. 2006. *Code version 2.0*. New York: Basic Books, Perseus Books Group.
- Levy, S. 2001. "Crypto." *Newsweek* 137 (3): 42–53.
- Lomas, N. 2016. "Encryption Under Fire in Europe as France and Germany Call for Decrypt Law." *techcrunch.com*. <https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-franceand-germany-call-for-decrypt-law/>
- Machkovech, S. 2016. "Obama Weighs in on Apple v. FBI: 'You Can't Take an Absolutist View'." *arstechnica.com*. <http://arstechnica.com/tech-policy/2016/03/obama-weighs-in-on-apple-v-fbi-youcant-take-an-absolutist-view/>
- Marechal, N. 2018. "From Russia With Crypto: A Political History of Telegram." In *8th \$! (\$USENIX\$!\$ Workshop on Free and Open Communications on the Internet*, 1–20.
- Masnick, M. 2016. "French Government Wants a 'Global Initiative' to Undermine Encryption and Put Everyone at Risk." *techdirt.com*. <https://www.techdirt.com/articles/20160811/17370035220/french-government-wants-global-initiative-to-undermine-encryption-put-everyone-risk.shtml>
- Menn, J. 2014. "Exclusive: NSA Infiltrated RSA Security More Deeply Than Thought—Study." *reuters.com*. <http://www.reuters.com/article/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331>
- Ministerie van Buitenlandse Zaken. 2017. "International Cyber Strategy." *government.nl*. <https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy>
- Modderkolk, H. 2016. "Dreiging is in jaren nog niet zo groot geweest." *de Volkskrant*, 17 September. <http://www.volkskrant.nl/4378383>
- Moody, G. no date. "Dutch Government: Encryption Good, Backdoors Bad." *arstechnica.com*. <http://arstechnica.com/tech-policy/2016/01/dutch-government-encryption-good-backdoors-bad/>
- Mozur, P. 2015. "New Rules in China Upset Western Tech Companies—NYTimes.com." *nytimes.com*. <http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturbwestern-tech-companies.html>
- Mueller, M.L., and F. Badieli. 2019. "Requiem for a Dream: On Advancing Human Rights via Internet Architecture." *Policy and Internet* 11 (1): 61–83. <https://doi.org/10.1002/poi3.190>
- Pahwa, N. 2018. "Indian Govt Seeks Inputs from ISPs for Blocking Instagram, Facebook, Whatsapp, Telegram." *Medianama.com*. <https://www.medianama.com/2018/08/223-indian-govt-seeksinputs-from-isps-for-blocking-instagram-facebook-whatsapp-telegram/>
- Pelgrim, C., and A. Kas. 2015. "Nieuwe wet geeft inlichtendiensten meer bevoegdheden." *nrc.nl*. <https://www.nrc.nl/nieuws/2015/07/02/nieuwe-wet-geeft-inlichtendiensten-meer-bevoegdheden-a1415042>
- Pool, R.L.D., and B.H.M. Custers. 2017. "The Police Hack Back: Legitimacy, Necessity & Privacy Implications of the Next Step in Fighting Cybercrime." *European Journal of Crime, Criminal Law and Criminal Justice* 25 (2): 123–44. <https://doi.org/10.1163/15718174-25022109>
- Sanger, D.E., and N. Perlroth. 2015. "Encrypted Messaging Apps Face New Scrutiny Over Possible Role in Paris Attacks." *nytimes.com*.
- Schellevis, J. 2016. "OM: versleutelde diensten als WhatsApp steeds groter probleem." *nos.nl*. <http://nos.nl/artikel/2127446-om-versleutelde-diensten-als-whatsapp-steeds-groter-probleem.html>
- Schneier, B. 2016. "Michael Hayden and the Dutch Government are Against Crypto Backdoors." *schneier.com*. [https://www.schneier.com/blog/archives/2016/01/michael\\_hayden\\_.html](https://www.schneier.com/blog/archives/2016/01/michael_hayden_.html)
- Schneier, B., and K. Seidel. 2016. A Worldwide Survey of Encryption Products. 7641, pp. 1–23.
- Sehabat, A., T. Mitew, and Y. Alzoubi. 2017. "Encrypted Jihad: Investigating the Role of Telegram App in Lone Wolf Attacks in the West." *Journal of Strategic Security* 10 (3): 27–53. <https://doi.org/10.5038/1944-0472.10.3.1604>
- Sivan-Sevilla, I. 2018. "Complementaries and Contradictions: National Security and Privacy Risks in U.S. Federal Policy, 1968–2018." *Policy and Internet* 9999 (9999): 1–43. <https://doi.org/10.1002/poi3.189>
- Swire, P., and K. Ahmad. 2012. "Encryption & Globalization." *The Columbia Science & Technology Law Review* 23: 416–81.
- Thomson, I. 2016. "French Say 'Non, merci' to Encryption Backdoors • The Register." *theregister.co.uk*. [http://www.theregister.co.uk/2016/01/15/france\\_backdoor\\_law/](http://www.theregister.co.uk/2016/01/15/france_backdoor_law/)
- Tweede Kamer Der Staten-generaal. 2015a. JBZ-Raad; Verslag van een algemeen overleg; Verslag van een algemeen overleg, gehouden op 7 oktober 2015, over de JBZ-Raad van 8 en 9 oktober 2015 (JBZonderwerpen op het terrein van asielen vreemdelingenbeleid) en behandelvoorbehoud EU-migratiepakket, 356, 1–26.
- Tweede Kamer Der Staten-generaal. 2015b. Raad voor Vervoer, Telecommunicatie en Energie; Verslag van een algemeen overleg.
- Tweede Kamer Der Staten-generaal. 2017a. *Antwoord op vragen van de leden Oosenbrug en Recourt over het bericht dat het openbaar ministerie toegang tot versleutelde informatie wil*. <https://zoek.officielebekendmakingen.nl/ah-786406.pdf>
- Tweede Kamer Der Staten-generaal. 2017b. *Verwerking en bescherming persoonsgegevens; Motie; Motie van de leden Verhoeven en Oosenbrug over het niet verzwakken van encryptiesoftware*.
- Vance, C, Leppard, A, and Zaragoza, J. 2015. "When Phone Encryption Blocks Justice—The New York Times." *The New York Times Online*. [http://www.nytimes.com/2015/08/12/opinion/applegoogle-when-phone-encryption-blocks-justice.html?\\_r=0](http://www.nytimes.com/2015/08/12/opinion/applegoogle-when-phone-encryption-blocks-justice.html?_r=0)
- van Miltenburg, O. 2015. "Open encryptieprojecten krijgen half miljoen euro van Nederlandse overheid." *tweakers.net*. <https://tweakers.net/nieuws/106723/open-encryptieprojecten-krijgenhalf-miljoen-euro-van-nederlandse-overheid.html>
- van der Steur, G.A. 2016. *Antwoorden Kamervragen over het bericht dat Frankrijk een internationale aanpak wil op het gebied van encryptie*. <https://www.rijksoverheid.nl/documenten/kamerstukken/2016/10/17/antwoorden-kamervragen-over-het-bericht-dat-frankrijk-een-internationale-aanpak-wil-op-het-gebied-van-encryptie>
- van der Steur, G.A., and H.G.J. Kamp. 2016. *Cabinet's View on Encryption*. <https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/nl-cabinetposition-on-encryption>
- Verhoeven, K., van Vliet, M., Mastenbroek, N., van Dieijen, M., van Egmond, D., and Arts, O. 2016. Techvisie D66.
- Washington Post. 2017. "Read the full testimony of FBI Director James Comey in which he discusses Clinton email investigation." *washingtonpost.com*. <https://www.washingtonpost.com/news/postpolitics/wp/2017/05/03/read-the-full-testimony-of-fbi-director-james-comey-in-which-he-discusses-clinton-email-investigation/>
- Weaver, N. 2016. "NSA and the No Good, Very Bad Monday." *lawfareblog.com*. <https://www.lawfareblog.com/very-bad-monday-nsa-0>
- Weitzner, D.J. 2016. "The Encryption Debate Enters Phase Two." *lawfareblog.com*. <https://www.lawfareblog.com/encryption-debate-enters-phase-two>
- Wolff, J. 2016. "What We Talk About When We Talk About Cybersecurity: Security in Internet Governance Debates." *Internet Policy Review* 5 (3): 1–13. <https://doi.org/10.14763/2016.3.430>
- Zaske, S. 2015. "EMEA: KPN Pushes Blackphones for Security, Encryption." *rcwireless.com*. <https://www.rcwireless.com/20150415/carriers/emea-kpn-cio-pushes-encryption-and-ultra-secure-blackphones-tag7>
- Zenger, R. 2016. "Stel de AIVD doorbreekt versleuteling. Wat dan?" *bof.nl*. <https://www.bof.nl/2016/12/18/stel-de-aivd-doorbreekt-versleuteling-wat-dan/>
- Zetter, K. 2016. "Apple's FBI Battle is Complicated. Here's What's Really Going On." *Wired.com*. <https://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/>

# Cops take out encrypted comms to disrupt organised crime

2 July 2020

**BY ALEX SCROXTON**

The EncroChat encrypted communications platform has been infiltrated and taken out by the collaborative efforts of law enforcement agencies from across Europe, including the UK's National Crime Agency (NCA), resulting in massive disruption to organised criminal activity.

A major provider of encrypted communications and supplier of a secure mobile phone instant messaging service, EncroChat's encryption was cracked by Dutch and French law enforcement agencies some time ago.

The bespoke platform was found to have 60,000 users worldwide and about 10,000 in the UK. The NCA said its sole use was for coordinating and planning the distribution of illicit commodities, money laundering, and even plotting to murder rivals.

The resulting effort in the UK, dubbed Operation Venetic, has so far resulted in 746 arrests and the seizure of £54m in cash, 77 illegal firearms including AK47 assault rifles, submachine guns and grenades, and two tonnes of class A and B drugs and illicit Valium, 55 luxury cars and 73 luxury watches.

NCA director of investigations Nikki Holland described Venetic as the broadest and deepest ever UK operation to disrupt serious and organised crime.

"The infiltration of this command and control communication platform for the UK's criminal marketplace is like having an inside person in every top organised crime group in the country. The NCA is proud to have led the UK part of this operation, working in partnership with policing and other agencies. The results have been outstanding, but this is just the start," she said.

"A dedicated team of over 500 NCA officers has been working on Operation Venetic night and day, and thousands

***Organised crime groups have used encrypted communications to enable their offending. They have openly discussed plots to murder, launder money, deal drugs and sell firearms capable of causing atrocious scenes in our communities.***

more across policing. And it's all been made possible because of superb work with our international partners" she said.

Ms Holland said: "Together we've protected the public by arresting middle-tier criminals and the kingpins, the so-called iconic untouchables who have evaded law enforcement for years, and now we have the evidence to prosecute them. The NCA plays a key role in international efforts to combat encrypted comms. I'd say to any criminal who uses an encrypted phone, you should be very, very worried."

The operators of EncroChat, who charged up to £1,500 for a six-month contract on one of their £3,500 encrypted handsets – which came complete with pre-loaded instant messaging apps, encrypted VoIP and a remote kill code

to wipe them – warned users of a data breach on 13 June 2020.

Home secretary Priti Patel said: "This operation demonstrates that criminals will not get away with using encrypted devices to plot vile crimes under the radar. The NCA's relentless targeting of these gangs has helped to keep us all safe. I congratulate them and law enforcement partners on this significant achievement.

"I will continue working closely with the NCA and others to tackle the use of such devices – giving them the resources, powers and tools they need to keep our country safe."

In London, the Metropolitan Police said Operation Venetic had delivered results in 34 ongoing investigations, and enabled 171 arrests in the city. So far, the Met has charged 99 people and seized £13.4m in cash, the largest single cash seizure in its history.

The force described one investigation into one of London's most dangerous organised crime groups with long-standing links to violent crime, members of which lead lavish lifestyles and lived in multi-million pound properties.

"Organised crime groups have used encrypted communications to enable their offending. They have openly discussed plots to murder, launder money, deal drugs and sell firearms capable of causing atrocious scenes in our communities. They were brazen and thought they were beyond the reach of the law," said Met commissioner Cressida Dick.

"This offending has a direct impact on our communities – those involved appear to have an air of respectability, but their actions leave a trail of misery and are inextricably linked to the violent scenes we see play out on our streets."



# Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe

2 July 2020

## EUROPOL/EUROJUST JOINT PRESS RELEASE

At a joint press conference today, French and Dutch law enforcement and judicial authorities, Europol and Eurojust have presented the impressive results of a joint investigation team to dismantle EncroChat, an encrypted phone network widely used by criminal networks.

Over the last months, the joint investigation made it possible to intercept, share and analyse millions of messages that were exchanged between criminals to plan serious crimes. For an important part, these messages were read by law enforcement in real time, over the shoulder of the unsuspecting senders.

The information has already been relevant in a large number of ongoing criminal investigations, resulting in the disruption of criminal activities including violent attacks, corruption, attempted murders and large-scale drug transports. Certain messages indicated plans to commit imminent violent crimes and triggered immediate action.

The information will be further analysed as a source of unique insight, giving access to unprecedented volumes of new evidence to profoundly tackle organised criminal networks.

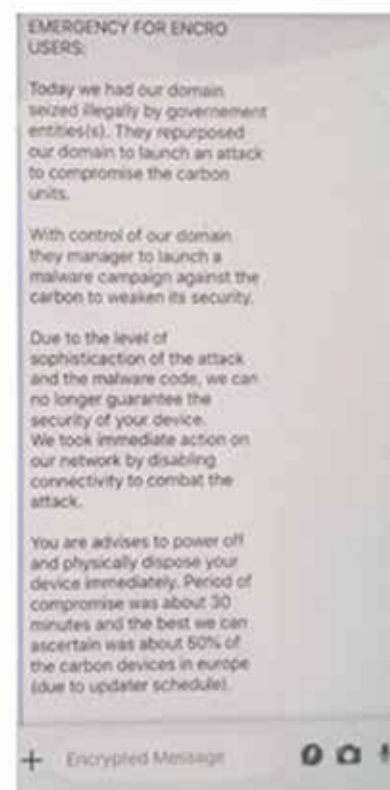
In recent years, European countries have been increasingly affected by organised crime groups who are pervasive and highly adaptive, posing one of the most pressing security challenges faced by law enforcement and judicial authorities. In this regard, the abuse of the encrypted communication technologies is a key facilitator of their criminal activities.

Since 2017, the French Gendarmerie and judicial authorities have been investigating phones that used the



secured communication tool EncroChat, after discovering that the phones were regularly found in operations against organised crime groups and that the company was operating from servers in France. Eventually, it was possible to put a technical device in place to go beyond the encryption technique and have access to the users' correspondence.

In early 2020, EncroChat was one of the largest providers of encrypted



digital communication with a very high share of users presumably engaged in criminal activity. User hotspots were particularly present in source and destination countries for cocaine and cannabis trade, as well as in money laundering centres.

Given the widespread use of the encrypted telephone solution by EncroChat among international criminal networks around the world,

French authorities decided to open a case at Eurojust, the EU Agency for Criminal Justice Cooperation, towards the Netherlands in 2019. Further developments in the investigations led to organising the processing of the data, which was captured on the basis of the provisions of French law and with judicial authorisation, through the frameworks for international judicial and law enforcement cooperation.

The data was in first instance shared with the Netherlands. Eurojust facilitated the creation of a Joint Investigation Team (JIT) between the two countries and with the participation of Europol, the European Union Agency for Law Enforcement Cooperation, in April 2020.

Europol has been actively involved in the investigations led by France and the Netherlands since 2018, relating to the provision and use of encrypted communication services by organised crime groups. Through its role as an information hub and its extensive analytical and technical support system, Europol was able to create and provide a unique and global insight on the scale and functioning of organised crime, as a result of this investigation. This will help law enforcement to combat organised crime in the future more successfully.

Europol's support from the early stages of this JIT included: promoting and arranging international cooperation, providing extensive analytical and financial support, technical expertise and a secured platform for the exchange of information between the countries involved. A large dedicated team at Europol investigated in real time millions of messages and data that it received from the JIT partners during the investigation, cross-checked and analysed the data, and provided and coordinated with the JIT partners the information exchange to concerned countries.

A large number of suspects have also been arrested in several countries which were not participating in the JIT but particularly affected by the illegal use of these phones by individuals active in organised crime, including in the UK, Sweden and Norway. Many of these investigations were connected with international drug trafficking and violent criminal activities.

At the same time, numerous operational meetings for the daily coordination between the law enforcement entities of the JIT partners

and other countries took place at Europol, partly during COVID-19.

Eurojust intensively facilitated the judicial cooperation, during the extensive use of European judicial cooperation instruments such as European Investigation Orders. Throughout the investigation, the JIT members organised five coordination meetings at Eurojust to bring all involved parties together in a secure environment, identify parallel or linked investigations, decide on the most suitable framework for cooperation and solve potential conflicts of jurisdiction.

In France, where the operation takes place under the code name "Emma 95", the Gendarmerie has set-up a Taskforce since March 2020. With more than 60 officers, the Gendarmerie leads the investigations targeting the EncroChat encrypted telephone solution under the supervision of the magistrates of the JIRS of Lille. The Taskforce has been monitoring the communications of thousands of criminals, leading to the opening of a wide range of incidental proceedings. France does not wish to communicate further on these on-going investigations nor on the results obtained. The considerable resources deployed demonstrate the importance of these investigations and the importance attached to their success in France.

In the Netherlands, where the operation went under the code name "Lemont", hundreds of investigators have, with authorisation of the examining magistrate, followed the communications of thousands of criminals day and night since the operation began to unravel and act on the intercepted data stream.

The criminal investigation has been led by prosecutors from the Dutch National Public Prosecution Service and the information has been made available to about a hundred ongoing criminal investigations. The investigation has so far led to the arrest of more than 100 suspects, the seizure of drugs (more than 8 000 kilo cocaine and 1 200 kilo crystal meth), the dismantling of 19 synthetic drugs labs, the seizure of dozens of (automatic) fire weapons, expensive watches and 25 cars, including vehicles with hidden compartments, and almost EUR 20 million in cash. The expectation is that information will be made available in more than 300 investigations. In a number of cases, more arrests are very likely to follow in the coming period.

The interception of EncroChat messages came to an end on 13 June 2020, when the company realised that a public authority had penetrated the platform. EncroChat then sent a warning to all its users with the advice to immediately throw away the phones.

While the activities on EncroChat have been stopped, this complex operation shows the global scope of serious and organised crime and the connectivity of criminal networks who use advanced technologies to cooperate on a national and international level.

The effects of the operation will continue to echo in criminal circles for many years to come, as the information has been provided to hundreds of ongoing investigations and, at the same time, is triggering a very large number of new criminal investigations of organised crime across the European continent and beyond.

## WHAT IS ENCROCHAT?

EncroChat phones were presented to customers as guaranteeing perfect anonymity (no device or SIM card association on the customer's account, acquisition under conditions guaranteeing the absence of traceability) and perfect discretion both of the encrypted interface (dual operating system, the encrypted interface being hidden so as not to be detectable) and the terminal itself (removal of the camera, microphone, GPS and USB port). It also had functions intended to ensure the 'impunity' of users (automatic deletion of messages on the terminals of their recipients, specific PIN code intended for the immediate deletion of all data on the device, deletion of all data in the event of consecutive entries of a wrong password), functions that apparently were specially developed to make it possible to quickly erase compromising messages, for example at the time of arrest by the police. In addition, the device could be erased from a distance by the reseller/helpdesk.

EncroChat sold the cryptotelephones (at a cost of around EUR 1 000 each) at international scale and offered subscriptions with a worldwide coverage, at a cost of 1 500 EUR for a six-month period, with 24/7 support.

# Encryption as a challenge for European law enforcement agencies

**MILANA PISARI , PHD<sup>1</sup>**

Faculty of Law, University of Novi Sad, Serbia

## **Abstract:**

Strong encryption is of great importance to digital economy and digital privacy. At the same time the use of encryption by criminals was recognized by *Europol and national law enforcement authorities* as a significant challenge for *detection and investigation* of cybercrime and cyber-facilitated crime, rendering traditional investigative techniques ineffective. Since encryption is continuously depriving law enforcement of evidential opportunities, EU member states started to demand a European solution to questions around encryption as a threat to security in Europe. However, there are many political inconsistencies among EU institutions and member states on encryption. The aim of this paperwork is to present and analyze the current state of legal and practical implications of criminal use of encryption and to consider alternative approaches, mainly those aimed to enhance the law enforcement agencies' decryption capabilities of lawfully obtained encrypted data in criminal investigations.

**Keywords:** encryption, cybercrime, law enforcement, European Union.

## **Introduction**

Although no one can deny the importance of strong encryption for digital economy and digital privacy, it is a fact that legitimate anonymity and encryption services and tools are being misused for criminal activity. The more and more common use of encryption by offenders to protect their communications or stored data poses a serious challenge for detection and investigation of crime, denying law enforcement the access to electronic evidence. This challenge is not present only in cybercrime investigation, but in investigation of all criminal offences which are enabled by information technologies whose traces may be found in digital devices or whose offenders use these technologies to communicate and conceal their identity and/or location. Because of that many traditional investigative techniques and digital forensic analysis are used not in their full potential or even ineffectively. These issues are recognized as a major problem by national law enforcement agencies (LEA) of Member States

(MS) and by key stakeholders in fight against cybercrime, organized crime and terrorism in European Union (EU). As the commercial use of strong encryption technology has been on the increase since 2014 and the use of encryption by criminals was recognized by Europol and national LEA as a significant challenge for detection, investigation, and prosecution of all areas of cyber-facilitated crime with cross-border dimension, depriving law enforcement of evidential opportunities, EU has debated how to regulate encryption in order to tackle this "Going dark" problem. The fundamental policy question involving encryption is how to balance competing values: how to promote privacy and spur economic growth and at the same time find proper tools for crime prevention and investigation which are tackled by destructive consequences of encryption misuse. The aim of this paper is to present and analyze the current state of encryption debate and possible legal and technical solutions for it at the EU level.

## **Encryption as an obstacle in criminal investigation**

Since 2016 the ability of LEA to access the data needed to conduct criminal investigations has been recognized as an increasing challenge, as a result of the enhanced use of encryption.

In September 2016, the Council asked MS to provide answers in a questionnaire in order to map the situation and identify the obstacles faced by LEA when gathering or securing encrypted evidence for the purposes of criminal proceedings (Council of the European Union (2016a)). Replies revealed that in the majority of MS encryption is encountered often or almost always in the context of criminal investigations, and this experience is present both with regard to online (in the form of encrypted emails or other forms of e-communication and/or commercial applications such as Facebook, Skype, WhatsApp or Telegram) and offline encryption (most often criminal investigation involving encrypted digital devices and encrypting applications). While national legal framework aimed at

1. mpisari@pf.uns.ac.rs





securing e-evidence when encrypted is considered sufficiently effective, the main problem is of technical nature: the lack of sufficient technical capacity, in terms of efficient technical solutions to decrypt and respective equipment, is among the top three challenges followed by the lack of sufficient financial resources and personal capacity, in terms of numbers and training of staff.

In 2016 Europol in its Internet Organized Crime Threat Assessment (IOCTA) pointed to encryption as a key threat and serious impediment to the detection, investigation, and prosecution of criminal activity (Europol, 2016a: 50). Twenty European countries reported the use of encrypting software by cybercriminals to protect their stored data, while eight MS specifically stated that dealing with encryption is a major challenge to investigating cybercrime. It was noticed that encryption is no longer restricted to desktop computers, but it is being used on mobile devices. Furthermore, almost half of MS indicated that their investigations involved the use of some form of encrypted communications, such as WhatsApp and Viber, which introduced encryption by default, by way of end-to-end encryption, making communication hard to intercept.

A combination of legislative and technical factors, which deny LEA access to timely and accurate electronic communications data and digital forensic opportunities, such as lack of data retention and encryption, were recognized in IOCTA 2017 as leading to a loss of both investigative leads and the ability to effectively attribute and prosecute online criminal activity (Europol, 2017a: 13). While the implementation of the European Investigation Order was expected to

simplify cooperation between judicial authorities and expediting investigations, existing legal frameworks and operational processes need to be further harmonized and streamlined for dealing with cross-border e-evidence. Such measures, as well as the parallel EU policy processes on encryption, data retention and internet governance challenges, should thoroughly consider the specific law enforcement needs and strive for practical and proportionate solutions to empower innovative, efficient and effective approaches to conducting lawful cybercrime investigations. The growing prevalence and sophistication of cybercrime requires dedicated legislation that more specifically enables law enforcement presence and action in an online environment (Europol, 2017a: 17).

Communication and storage applications and devices increasingly come with encryption by default, which along with data protection and privacy issues, means that law enforcement can increasingly be denied access to the relevant data it needs to locate and identify offenders and to secure evidence (Europol, 2017a: 41). LEA highlighted the difficulties posed by encrypted communication apps and software, and the use of encryption to effectively and indefinitely hide critical evidence, applicable across all aspects of cybercrime (Europol, 2017a: 63).

Owing to the expansion of Internet enabled mobile devices, the wide diversity of platforms and services used, the easy availability of online anonymity and encryption tools and the growing use of the Darknet, it became easier for offenders to store and share material with lower risks of detection, especially in connection with online Child Sexual Exploitation

Material (CSEM) (Europol, 2018a: 9) and ransomware (Europol, 2018a: 26).

In June 2019, Europol and Eurojust issued assessment on the common challenges in combatting cybercrime. It is noted that encryption is more and more a cross-cutting challenge that affects all crime areas, including cybercrime, serious organized crime and terrorism. EU LEA indicate that a significant and increasing percentage of cybercrime investigations involve the use of some form of encryption to hide relevant data and communications evidence. Since growing number of electronic service providers implement encryption by default in their services, law enforcement has also observed the increasing misuse of and reliance by cybercriminals upon secure communication apps and channels providing end-to-end encryption, leading to that *investigative techniques*, such as lawful interception, *are becoming increasingly* less effective or even technically impossible (Europol, Eurojust 2019a:10). The increased implementation of encryption also negatively affects digital forensic analysis. Apart from the legal challenges, disclosing the data or circumventing the encryption is not always technically possible. This assessment however concludes with that although a number of the legislative and practical measures addressing the identified challenges are making progress on both national and international levels, the need for a comprehensive international legal and practical framework to address fundamental problems, such as access to cloud data and encryption, is more pressing than ever (Europol, Eurojust 2019a: 20).

---

*continued on page 32*

The criminal abuse of encryption technologies, whether it be anonymization via VPNs or Tor, encrypted communications or the obfuscation of digital evidence (especially in cases of CSEM) is represented as a significant threat highlighted by respondents to 2019 survey (Europol, 2019a: 56-57). However, inaccessibility of relevant data also comes due to legislative barriers or shortcomings, which we must overcome to enhance cross-border access to electronic evidence and the effectiveness of public-private cooperation through facilitated information exchange (Europol, 2019a: 7). As criminals adapt, law enforcement and legislators must also innovate in order to stay ahead, and seek to capitalize on new and developing technologies. To do so, however, law enforcement needs the knowledge, tools and legislation required to do so quickly and effectively. This is also recognized as the main direction of EU policy on encryption.

### **EU position on encryption**

Although since 2016 the encryption has globally been considered as a major obstacle for criminal investigation, opposite to Five eyes countries commitment to legislating backdoors (Five Country Ministerial 2018), there is a clear opposition to this approach in the EU.

Europol and ENISA agreed that built-in backdoors to encryption do not provide a secure fix to police frustrations. The directors of the two agencies said that while [backdoors] would give investigators lawful access in the event of serious crimes or terrorist threats, it would also increase the attack surface for malicious abuse, which consequently would have much wider implications for society (Europol, ENISA 2016). As both France and Germany suffered terrorist attacks throughout 2015/2016, including attack in Paris in November 2015 and in Nice in July 2016, at the meeting of French and German interior ministers on August 23rd 2016, they called for feasible solutions to decryption, but without weakening the protective mechanisms, both in legislation and through continuous technical evolution that would afford security agencies the ability to access encrypted data and enable courts to demand that Internet companies decrypt data to help further criminal investigations (Tech Crunch (2016, August 24). In December 2016, ENISA issued

opinion in which it recognized requests of law enforcement for creating means to circumvent encryption as protection measures as legitimate, but also stressed out that limiting the use of cryptographic tools would create vulnerabilities that can in turn be used by terrorists and criminals, and lower trust in electronic services, which would eventually damage industry and civil society in the EU (ENISA 2016, 16).

Because all MS, except five of them, favored the need for practically orientated measures (more resources and tools) prevailed over the need for adoption of new anti-crypto legislation at the EU level, the Council endorsed the four-steps approach as basis for the future work in this regard: A. Launch of a reflection process on the challenges faced by criminal justice in relation to the use of encryption with the purpose to define practical solutions that would allow the possible disclosure of encrypted data/ devices through an integrated EU approach and framework; B. Explore possibilities for improving the technical expertise both at the national and EU level to face current and future challenges stemming from encryption; C. Encourage the members of the European Judicial Cybercrime Network to bring to its forum for discussion, exchange of information, good practices and expertise also the practical/operational aspects related to encryption; D. Deepen the practical/operational aspects of the encryption-related trainings for LEA provided by EU entities and increase the capacity building efforts (Council of the European Union, 2016b).

In the Resolution passed in early October 2017, the European Parliament explicitly asked MS to refrain from enforcing measures that may weaken the networks or services that encryption providers offer. The Resolution stressed that feasible solutions must be offered, via both legislation and continuous technological evolution, in aligning the conditions for the lawful use of investigative tools online (European Parliament 2017).

Besides, the Cybersecurity strategy (European Commission 2017a) recognized encryption as a vital tool for the protection of personal data and fundamental rights, the Commission adopted on 18 October 2017 its position on encryption used by criminals, embedding it in its anti-terrorism package in the Eleventh progress report towards an effective and genuine Security Union (European Commission 2017b). The Commission set out a package of anti-terrorism

measures including measures to support law enforcement and judicial authorities when they encounter the use of encryption by criminals in criminal investigations. These includes (a) legal measures to facilitate access to encrypted evidence, and (b) technical measures to enhance decryption capabilities. As for the legal measure, creation of appropriate legal framework for cross-border access to electronic evidence that would overcome challenge of cross-border access to electronic evidence located in another country was announced. Technical measures do not mean prohibiting, limiting or weakening encryption. Instead of that 1) the Commission will support Europol to further develop its decryption capability; 2) a network of points of expertise should be established, with Europol as a network hub to facilitate collaboration among them; 3) MS authorities should have a toolbox of alternative investigation techniques at their disposal to facilitate the development and use of measures to obtain needed information encrypted by criminals, and the European Cybercrime Centre (EC3) at Europol should be the best-placed to set up and keep a repository of those techniques and tools; 4) the attention should be paid to the important role of service providers and other industry partners in providing solutions with strong encryption; 5) training programs for law enforcement and judicial authorities should ensure that responsible officers are better prepared to obtain necessary information encrypted by criminals; 6) the Commission will support the development of an observatory function in collaboration with the EC3 at Europol, the European Judicial Cybercrime Centre (EJCN) and Eurojust. So, instead of legislating backdoors, the Commission appears to be exploring alternative approaches, including investing in decryption. Although the Commission opted for non-legislative approach by building on Europol's existing toolbox of decryption capabilities, because these technical measures could mean anything, they could highlight the shortcomings of current laws and policies and thus fail to safeguard encryption in the longer term, leaving the door open to future legislation toward the so-called backdoors for LEA to access private data.

The Commission proposed to fund and develop means to break encryption without prohibiting, limiting or weakening encryption, but workarounds applied in achieving this goal could pose a legal

challenge, especially if it is in a form of government hacking developed and used without an adequate legal framework and often without respect for national or international human rights safeguards. Since the current debate about encryption has become too polarized, with tech companies unnecessarily framing the issue as a zero-sum game, in which any tool that provides lawful access to law enforcement will necessarily compromise user privacy, the EU advocates targeted approaches to the development of new investigative tools that are proportionate to the crime that was committed. This approach is consistent with the Commission's prior commitment to research functional encryption: technologies that would change the way data is encrypted in the first place to allow law enforcement to gain selective access to data in certain circumstances, instead of granting all or nothing law enforcement access to a device (European Commission 2019). In other words, the aim is to come up with a solution that could be later implemented by service providers and device manufacturers so that all three sides of the "Going dark" debate (the user, the provider and the government) are satisfied.<sup>2</sup>

## Role of Europol

The current non-legislative approach to encryption in EU is focused on enhancing the technical capabilities already available within Europol and encouraging their use by MS in the respective limits of its mandate, as well as the further developing of Europol as European Centre of expertise on encryption.

As concluded in Report in 2017 that most MS do not have access to the right level of expertise and technical

resources, which seriously challenges law enforcement and judicial authorities' ability to access encrypted information in criminal investigations, the Commission has supported Europol ever since to further develop its decryption capability.

Since 2014, Europol has been offering Member States support in decrypting data carriers or mobile phones. The unit is based at the EC3. EC3 provides operational capabilities, such as advanced digital forensic, technology tools and platforms. According to Consolidated Annual Activity Reports (CAAR), this decryption platform was so far used on 35 occasions during 2014 with no indication of successful results (CAAR 2014, 15),<sup>3</sup> on 26 occasions during 2016 with no indication of successful results (Europol 2016b: 30), during 2017 it was used on 28 occasions achieving successful results 9 times (Europol, 2017b: 30), during 2018 on 32 occasions achieving successful results 12 times (Europol, 2018 b: 38), and on 59 occasions during 2019 with a 39% successful decryption rate (Europol, 2019b: 28).

Additional resources were provided for Europol to enable its EC3 support to MS to address challenges related to encryption in criminal investigations.<sup>4</sup> While in the Report from December 2017 (European Commission (2017c), the Commission stressed that the assessment of the specific needs for additional resources was ongoing, in January 2018 the Commission declared it would amend the 2018 Europol budget with an additional EUR 5 million to reinforce Europol's capabilities to decrypt information lawfully obtained in criminal investigations (European Commission, 2018).<sup>5</sup> This amount was aimed to set up a new dedicated Decryption Platform in cooperation with the

EU Joint Research Centre (JRC), which was finally created in early 2020.<sup>6</sup>

IOCTA 2019 declared that EUROPOL is at the forefront of law enforcement innovation and acts as a knowledge platform for the provision of EU policing solutions in relation to encryption and other issues. In order to play an active role in the efforts of law enforcement against the use of encryption for criminal purposes, EC3 focuses on digital forensics and cross-departmental encryption support for recovering encrypted criminal data and will be further developing and utilizing its potential to perform as a European center of expertise on decryption (Europol 2018 b:15, 24). Europol has the function of a network hub to facilitate collaboration among national expertise points<sup>7</sup> and Europol's EC3 was elected as the best-placed to set up and keep a repository toolbox of alternative investigation techniques and tools at disposal to MS to facilitate the development and use of measures to obtain needed information encrypted by criminals. EC3 will expand the toolbox available to law enforcement officers across Europe and beyond, increasing their technical and forensic capabilities (Europol, 2019a: 4). Such a toolbox has not been developed yet, and one may doubt that national LEAs might be willing to share sensitive encryption-cracking forensic tools and expertise across borders without the impetus of legislation. Europol's EC3 has observatory function in collaboration with the European Judicial Cybercrime Centre (EJCN) and Eurojust. Europol and Eurojust released joint "First

*continued on page 34*

2. For instance, EU will contribute over EUR 4.2 million to FENTEC project developing "functional encryption" ("FE") technology. FE has recently been introduced as a new paradigm of encryption systems with the aim to overcome all-or-nothing limitations of classical encryption. In an FE system the decryptor deciphers a function over the message plaintext: such functional decryptability makes it feasible to process encrypted data (e.g. on the Internet) and obtain a partial view of the message plaintext. These systems would effectively encrypt private messages and data and at the same time they would allow law enforcement to obtain a partial view of the message plaintext.

3. There are no available data on the use of decryption platform in 2015 in CAAR 2015.

4. The Commission proposed a total of 86 additional security-related posts for Europol (19 more than in the 2017 budget), in particular to reinforce Europol's EC3. Future technological developments should be taken into account on the basis of research and development under the Horizon 2020 program and other EU-funded programs.

5. After that, encryption has not been mentioned in the reports, concluding the 20th Report from 30th October 2019.

6. These funds were received in May 2018 (CAAR 2018, 9). Meetings with the different stakeholders to capture the requirements were held and different cooling technologies and equipment contracting options were considered. Service Level Agreement (SLA), facility and security requirements and budget planning with regards to the offsite platform located within one of the premises of the JRC were finalized in 2018. One decryption expert was recruited and worked on the development of a decryption manual that would serve as valuable input for the project. In May 2019, Europol addressed a note to the European Parliament and the Council with information regarding decryption platform at Europol, in which they explained that the JRC computing room and involved services were used by Europol to support the decryption activities to be conducted by Europol. The support would consist of the setup and maintenance of high-performance computing platform for decryption located in one of the JRC's premises. The realization was planned for 2019 – 2020 (operational use in 2020), while afterwards an addendum would be attached and signed for the maintenance period. Europol and the JRC finalized a service level agreement (SLA) which covered the design, procurement, installation, configuration, maintenance and administration of a High Performance Computing decryption platform at Ispra (Italy). The first meeting of the Steering Committee took place in June and the first equipment and tests were scheduled for Q4, with the go-live planned for Q1 2020. However, due to some challenges the JRC was facing with the contractor working on the building integration the go-live of the project was delayed to Q2 (Europol, 2019b: 27).

7. For example, capacity building for LEA community continued and three training courses on Hashcat were organized and delivered by the Forensic team to (24) MS representatives. Additionally, an internal course on applied Python programming was delivered to Europol staff by members of the Forensic team. Two decryption expert groups were created in 2019. The first one for practitioners who attended the Hashcat training course delivered by Europol and the second one (End-to-End Encryption E2EE) for those experts who attended the Encryption Network meetings organized by the Forensic team. Europol acquired new tools to enable the extraction of data from password protected mobile devices (Europol (2019b: 28).



Report of the observatory function on encryption” in January 2019 (Europol, Eurojust (2019b) and “Second Report of the observatory function on encryption” in February 2020 (Europol, Eurojust (2020) containing relevant statements or propositions made with respect to how law enforcement can potentially cope with encryption and its related challenges.

## Conclusion

Encryption is more and more a cross-cutting challenge that affects all crime areas, including cybercrime, serious organized crime and terrorism, and significant and increasing percentage of investigations involve the use of some form of encryption to hide relevant data and communications evidence. Because growing number of electronic service providers implement encryption by default in their services, law enforcement

has also observed the increasing misuse of and reliance by cybercriminals upon secure communication apps and channels providing end-to-end encryption, leading to that *investigative techniques*, such as lawful interception, *are becoming increasingly* less effective or even technically impossible. Apart from the legal challenges, disclosing the data or circumventing the encryption is not always technically possible. This assessment however concludes with that although a number of the legislative and practical measures addressing the identified challenges are making progress on both national and international levels, the need for a comprehensive international legal and practical framework to address fundamental problems, such as access to cloud data and encryption, is more pressing than ever.

Since 2016 encryption has been recognized as an obstacle to criminal investigation and therefore a threat to security in Europe. As data access policies and capabilities differ among MS, problems

with encryption in criminal investigations vary from one MS to another. There is also the problem with legal frameworks for cooperation between MS and states outside the EU, while they are considered as slow and inadequate for addressing forms of cross-border criminal cases involving encrypted information. In order to counter the criminal abuse of encryption, LEA need proper tools, techniques and expertise in digital forensics. They must be equipped with adequate training and resources to obtain and handle electronic evidence in situ using techniques, such as live data forensics. LEA should continue to monitor trends in the use of applications and software by cybercriminals and maintain awareness of the different investigative opportunities and challenges that each provides. It is essential for LAE to build and maintain relationships with academia and private industry as they may be able to assist or advise law enforcement where it lacks the technical capability.

## References

1. Council of the European Union (2016a). *Encryption of data – Questionnaire*. Accessed on July 15, 2020. <http://data.consilium.europa.eu/doc/document/ST-12368-2016-INIT/en/pdf>.
2. Council of the European Union (2016b). *Encryption: Challenges for criminal justice in relation to the use of encryption - future steps - progress report*. Accessed on July 15, 2020. <https://data.consilium.europa.eu/doc/document/ST-14711-2016-INIT/en/pdf>.
3. ENISA (2016). *Opinion Paper on Encryption Strong Encryption Safeguards our Digital Identity*. Accessed on July 15, 2020. <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption>.
4. European Commission (2017a). Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 13.9.2017. Accessed on July 15, 2020. <https://ec.europa.eu/transparency/regdoc/rep/10101/2017/EN/JOIN-2017-450-F1-EN-MAIN-PART-1.PDF>.
5. European Commission (2017b). Communication from the Commission to the European Parliament, the European Council and the Council, *Eleventh progress report towards an effective and genuine Security Union* COM(2017)0608 final. Accessed on July 15, 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0608&from=EN>.
6. European Commission (2017c). Communication from the Commission to the European Parliament, the European Council and the Council, *Twelfth progress report towards an effective and genuine Security Union*, 12.12.2017. Accessed on July 15, 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0779&from=EN>.
7. European Commission (2018). Communication from the Commission to the European Parliament, the European Council and the Council, *Thirteenth progress report towards an effective and genuine Security Union*, COM(2018)046 final, 24.1.2018. Accessed on July 15, 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0046&from=EN>.
8. European Commission (2019). *Functional Encryption Technologies*, 6.9.2019. Accessed on July 15, 2020. <https://cordis.europa.eu/project/rcn/213111/factsheet/en>.
9. European Parliament (2017). *Resolution of 3 October 2017 on the fight against cybercrime* (2017/2068(INI)). Accessed on July 15, 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017IP0366&from=EN>.
10. Europol (2014). *Consolidated Annual Activity Report (CAAR)*. Accessed on July 15, 2020. [https://www.europol.europa.eu/sites/default/files/documents/consolidated\\_annual\\_activity\\_report\\_caar\\_2014\\_0.pdf](https://www.europol.europa.eu/sites/default/files/documents/consolidated_annual_activity_report_caar_2014_0.pdf).
11. Europol (2016a). *The Internet Organised Crime Threat Assessment (IOCTA) 2016*. Accessed on July 15, 2020. <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016>.
12. Europol (2016b). *Consolidated Annual Activity Report (CAAR)*. Accessed on July 15, 2020. [https://www.europol.europa.eu/sites/default/files/documents/europol\\_annual\\_activity\\_report\\_2016.pdf](https://www.europol.europa.eu/sites/default/files/documents/europol_annual_activity_report_2016.pdf).
13. Europol (2017a). *Internet Organised Crime Threat Assessment (IOCTA) 2017*. Accessed on July 15, 2020. <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>.
14. Europol (2017b). *Consolidated Annual Activity Report (CAAR)*. Accessed on July 15, 2020. <https://www.europol.europa.eu/publications-documents/consolidated-annual-activity-report-caar-2017>.
15. Europol (2018 b). *Consolidated Annual Activity Report (CAAR)*. Accessed on July 15, 2020. <https://www.europol.europa.eu/publications-documents/consolidated-annual-activity-report-caar-2018>.
16. Europol (2018a). *Internet Organised Crime Threat Assessment (IOCTA) 2018*. Accessed on July 15, 2020. <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018>.
17. Europol (2019a). *Internet Organised Crime Threat Assessment (IOCTA) 2019*. Accessed on July 15, 2020. <https://www.europol.europa.eu/publications-documents/consolidated-annual-activity-report-caar-2019>.
18. Europol (2019b). *Consolidated Annual Activity Report (CAAR)*. Accessed on July 15, 2020. [https://www.europol.europa.eu/publications-documents/consolidated\\_annual\\_activity\\_report\\_2019.pdf](https://www.europol.europa.eu/publications-documents/consolidated_annual_activity_report_2019.pdf).
19. Europol, ENISA (2016). *Joint Statement: On lawful criminal investigation that respects 21st Century data protection*. Accessed on July 15, 2020. <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection>.
20. Europol, Eurojust (2019a). *Common challenges in combating cybercrime*. Accessed on July 15, 2020. <https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cyber-crime>.
21. Europol, Eurojust (2019b). *Joint Report First Report of the observatory function on encryption*. Accessed on July 15, 2020. <https://www.europol.europa.eu/publications-documents/first-report-of-observatory-function-encryption>.
22. Europol, Eurojust (2020). *Joint Report Second Report of the observatory function on encryption*. Accessed on July 15, 2020. <https://www.europol.europa.eu/publications-documents/second-report-of-observatory-function-encryption>.
23. Five Country Ministerial (2018). *Statement of Principles on Access to Evidence and Encryption*. Accessed on July 15, 2020. <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018>.
24. Lomas, N. (2016, August 24). Encryption under fire in Europe as France and Germany call for decrypt law. *Tech Crunch*. Accessed on July 5, 2020. [https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-france-and-germany-call-for-decrypt-law/?guccounter=1&guce\\_referrer\\_us=aHR0cHM-6Ly93d3cu29vZ2xlMmNvbS8&guce\\_referrer\\_cs=sMnhNkTpqBEB3VgCB0PgRA](https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-france-and-germany-call-for-decrypt-law/?guccounter=1&guce_referrer_us=aHR0cHM-6Ly93d3cu29vZ2xlMmNvbS8&guce_referrer_cs=sMnhNkTpqBEB3VgCB0PgRA).

# Assistance and Access Act Overview

Source: Information provided by the Department of Home Affairs

The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (the Assistance and Access Act) addresses law enforcement and intelligence agencies' challenges with the evolution of the communications environment, including the growth of encrypted communication.

The Act:

- enhances the obligations of businesses that provide communications services to assist agencies
- establishes new 'computer access warrants' for law enforcement
- strengthens agencies' existing search and seizure powers for computers (including mobile devices) to access unencrypted data

## Schedule 1 – Industry Assistance

In the modern era, criminal activity is frequently conducted online and through communications systems. Australian agencies need the help of the communications industry to detect and disrupt this activity.

Schedule 1 of the Act establishes a framework for government and the communications industry to work together on law enforcement and national security investigations, allowing:

- agencies to request voluntary assistance from providers with a technical assistance request
- agencies to require assistance from providers with a technical assistance notice where the provider is already capable of giving the required assistance

- the Attorney-General and Minister for Communications to jointly require a provider develop a new capability with a technical capability notice where the provider is not already capable of offering that type of assistance

Schedule 1 of the Act provides that:

- any assistance or capability requested must be reasonable, proportionate, practicable and technically feasible
- assistance to law enforcement must be related to investigating offences with a maximum penalty of at least three years imprisonment or more
- providers may be asked to build or use capabilities that can provide targeted access to data where this does not remove electronic protection or jeopardise the information security of general users

Schedule 1 of the Act **does not**:

- allow for assistance that creates 'systemic weaknesses' or backdoors into encrypted devices and communication systems. This includes requesting or requiring providers:
  - refrain from fixing vulnerabilities or making their services more secure
  - build a decryption capability, or
  - reduce the broader security of their systems
- allow agencies to see the content of personal communications, or intercept communications – these things continue to be governed by existing legislation and warrant regimes

- compel providers to build a capability to remove electronic protection
- extend existing data retention or interception obligations to new providers

Other safeguards to Schedule 1 of the Act include:

- review of technical capability notices upon referral by providers to determine if they abridge any of the Act's limitations, such as the backdoors prohibition
- a whole-Act review by the Independent National Security Legislation Monitor
- decisions by agencies and the Attorney-General are subject to judicial review
- any requests by State and Territories police must be approved by the Australian Federal Police which will coordinate compulsory requests across Australia
- extensive oversight from dedicated bodies including the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security

## Schedule 2 – Computer Access Warrants

Schedule 2 of the Act creates computer access warrants, which allows law enforcement:

- to covertly access devices to investigate serious crimes

*continued on page 36*

- to search devices such as laptops, mobile phones and USBs, and collect information
- to conceal the fact that a device has been accessed

Schedule 2 of the Act also amends ASIO's existing warrant regime with the power to conceal the fact that a device has been accessed.

Law enforcement computer access warrants must be issued by an independent authority (a judge or AAT member) and cannot authorise interference with, or material loss or damage to, a computer.

Computer access warrants can be sought only for serious offences (offences that attract a penalty of three years or more).

### Schedule 3 and 4 – Strengthening search and seize powers

Schedules 3 and 4 of the Act extend the maximum penalties associated with the power of a Magistrate to require an individual unlock a device where they know the password:

- In the Crimes Act, from two years to five years imprisonment – ten years for serious offences
- In the Customs Act, from six months to five years imprisonment – ten years for serious offences

Schedules 3 and 4 of the Act also extend the time available for examining electronic devices seized under warrant:

- In the Crimes Act, from 14 to 30 days
- In the Customs Act, from 72 hours to 30 days

Schedule 3 also allows police to access account-based data (i.e. social media accounts) via a search warrant.

### Limitations & Safeguards

There are a number of key limitations located throughout Part 15 of the Telecommunications Act. Some key safeguards are contained within Division 7 of the Part. These include:

- Requirements and requests must not contravene the prohibition against building or implementing systemic weaknesses or vulnerabilities – 317ZG
- A TAR, TAN or TCN must not be used to do things for which the requesting agency would otherwise require a warrant or authorisation – 317ZH
- New capabilities must not require the construction of interception capabilities or data retention capabilities (for a TCN) – 317ZGA

### No systemic weaknesses

Systemic weakness, so-called 'backdoors', weaken the digital security of Australians and others.

This is why notices under the Act cannot require a provider to implement or build systemic weaknesses into electronic protection. The Australian Government has no interest in undermining systems that protect the fundamental security of communications. This includes an explicit prohibition on building a decryption capability or requiring that providers make their encrypted systems less effective.

Notices cannot prevent a provider from fixing a security flaw in their products. Providers can, and should, continue to update their products to ensure customers enjoy the most secure services available.

The prohibition against systemic weakness ('backdoors') was clarified and strengthened following a review by the Parliamentary Joint Committee on Intelligence and Security.

### What is a systemic weakness

Section 317B defines a systemic weakness/vulnerability as 'a weakness/vulnerability' that affects a whole class of technology...'. The term 'class of technology' is deliberately broad and captures general items of technology across and within a category of product. It encompasses, for example, mobile phone technology, a particular model of mobile phone, a particular type of operating system within that phone model or a particular type of software installed on an operating system. The wide scope is intended to protect the services and devices used by the whole, or legitimate segments of, the general public and business community.

Further elements of the definition clarify that the inherently targeted surveillance activities of agencies are not captured by this definition. However, new subsections 317ZG(4A), (4B) and (4C) make clear that even requirements to assist in these legitimate and authorised agency activities must not have the inadvertent effect of weakening information security. That is, industry cannot be asked to do things that would be likely to create a material risk of unauthorised access to the information of a person not connected to an investigation.

The intent and application of the protection is to provide for targeted, proportionate access and prevent weakening cybersecurity.

### What is 'electronic protection'

Electronic protection includes encryption. However, the Act's prohibition against systemic weaknesses also extends to other forms of electronic protection, including authentication systems like passwords.

### Warrant to undertake surveillance

The framework does not serve as an independent channel to obtain private communications, metadata or undertake surveillance. Section 317ZH of the Act states that if a warrant or authorisation was required before, it is still required. Interception of communications, access to metadata or search powers still require existing thresholds to be met. Further, providers can't be asked to build an interception, data retention or decryption capability (or build anything that removes a form of electronic protection, like encryption).

In order to undertake these privacy-intrusive activities, agencies must seek a warrant or authorisation under the Telecommunications (Interception and Access) Act 1979 (TIA Act) or Surveillance Devices Act 2004. Agencies must meet the applicable thresholds and receive independent approval.

### Additional safeguards for TCNs Independent assessments of any new capability

To attain third-party verification that the Act's legal protections are not being circumvented (and that requirements are otherwise reasonable, proportionate, practical and technically feasible) industry may refer any requirements to build a new capability for review by a technical expert and a retired senior judge. The findings on this assessment panel are extremely influential on the decision to issue a notice by the Attorney-General. Industry may also apply for judicial review of executive decisions as an inherent part of the Australian legal system.

### Added safeguards against data retention, interception and others

None of the powers can be used to require the construction of a data



retention, interception or decryption capability. Additional safeguards exist to prevent new capabilities built under a TCN from extending telecommunications interception, data retention or users' browsing history. These are set out at 317ZGA.

### **Reasonable, proportionate, practicable and technically feasible**

Decision-makers must be satisfied that a TAR, TAN or TCN is reasonable, proportionate, practical and technically feasible. These decisions, by law, include consideration of industry interests, necessity, privacy, cyber security and intrusiveness. In addition to mandatory consultation, this ensures any representations of industry are taken into account and decision-makers turn their mind to the impact on the Australian public.

Decision-makers must revoke a technical assistance notice or technical capability notice if satisfied that any ongoing requirements are no longer reasonable, proportionate, practical or technically feasible. This ensures that any requirements on industry are under constant assessment and continue to meet the necessary thresholds, even as circumstances change.

### **Review by the courts, experts and arbitration**

Affected people and companies have an avenue to challenge a decision to issue a notice. Judicial review by the courts is available under the Judiciary Act 1903.

Independent technical experts may be appointed to report on any potential security weaknesses associated with requirements of TCNs.

### **Arbitration for disputes on terms and conditions**

In the exceptional cases where providers and Government disagree on the terms and conditions for compliance with a notice, an arbitrator will determine terms and conditions.

### **Oversight mechanisms**

#### **The scope of notices is limited to core agency functions and a serious offence threshold**

Things specified in notices must be for the purpose of helping an agency perform its core functions conferred under law, as they specifically relate to:

- enforcing the criminal law for serious Australian offences, or
- assisting the enforcement of the criminal laws in force in a foreign country for serious foreign offences, or
- safeguarding national security.

As a result of these requirements, law enforcement agencies are only permitted to use these powers in the course of enforcing a criminal offence with a penalty of three years or more imprisonment, domestically or overseas.

### **Providers must be informed of their obligations and their right of complaint**

If a notice or request is given under the Act, the issuer must give advice relating to the provider's obligations.

This ensures that smaller providers will clearly understand their requirements. When issued with a TAN or TCN, providers must also be informed of their right to lodge a complaint with the Commonwealth Ombudsman or IGIS, depending on the issuing agency.

### **Information is protected**

Unauthorised disclosure of information about, or obtained under, a notice is an offence. This ensures that any assistance is provided on a confidential basis and the sharing of information, including commercially sensitive information is restricted.

### **Additional reporting requirements add to transparency**

The public has visibility of the use of the powers through annual reporting requirements. The Minister is required to publish a written report every financial year that sets out the number of technical assistance notices and technical capability notices. Providers may produce transparency reports disclosing the number of notices received in a six month period. Providers may also apply for conditional disclosure exemptions to reveal the nature of assistance they have provided.

### **Powers reserved to senior decision-makers**

The power to issue TCNs is reserved for the joint authorisation of the Attorney-General and Minister for Communications. Requirements under TANs can only be set by the head of ASIO or an interception agency or a senior official in their organisation delegated by them.

### **Approval of State and Territory notices by AFP**

Before a TAN can be issued by a police force of a State and Territory it must be approved by the AFP Commissioner. The Commissioner will act as centralised coordinator and is intended to reduce duplicate requests, enable the exchange of relevant information across jurisdictions and advise on the types and forms of assistance commonly requested.

### **Joint ministerial approval of TCNs**

Before a TCN can be issued, it must be approved by the Minister for Communications in consideration of the notice's objectives, the legitimate interests of the provider, the notice's impact on the international competitiveness of the Australian communications industry and any representations made by the Attorney-General. This joint approval mechanism is an additional avenue for industry to feed directly into the decision-making process.

### **Extensive oversight by the Inspector-General of Intelligence and Security (IGIS) and the Commonwealth Ombudsman**

The powers are oversighted by the IGIS (for ASIO, ASD & ASIS) and the Commonwealth Ombudsman (AFP, ACIC and State & Territory Police). This oversight includes:

- Notification to these bodies when the powers are issued, variations, extension, revocation.
- Clear inspection and reporting authority, including explicit discretion for the Commonwealth Ombudsman to conduct an inspection, report on that inspection and have that report tabled in Parliament.
- Information sharing provisions which allow exchange of information under the regime between Commonwealth, State and Territory oversight bodies.

### **Review by the Independent National Security Legislation Monitor (INSLM) and Parliamentary Joint Committee on Intelligence and Security (PJCIS)**

The operation of the Assistance and Access Act and each of its 5 schedules has recently been reviewed by the INSLM and the PJCIS is currently conducting a review into the legislation.

# Debunking the Myths – Australia's Assistance and Access Act

## Common myths and misconceptions

Source: Information provide by the Department of Home Affairs

The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (the Assistance and Access Act) creates a pathway for industry to deliver assistance to law enforcement and intelligence agencies where necessary. It does not allow for mass surveillance, the creation of decryption capabilities, the implementation of so-called 'backdoors' or the issuing of 'secret notices' on employees of communications providers.

The Assistance and Access Act is focused on seeking help from corporate entities that are critical to the supply of communications services and devices in Australia. It does not discriminate between foreign and Australian companies conducting business offshore or place obligations on persons by virtue of their Australian citizenship.

Some common myths about the Assistance and Access Act are identified and corrected below.

### **This law has created backdoors and undermines information security**

The Assistance and Access Act contains an express prohibition against building or implementing any weakness or vulnerability in software or physical devices that would jeopardise the security of innocent users. This is found

in **section 317ZG** of the Act which also makes clear that any assistance that makes a system's encryption or authentication less effective for general users is strictly prohibited. This same section prohibits the construction of new decryption capabilities and rules out any requirements that would prevent a company from patching existing security flaws in their systems.

All proposed requirements to build a new capability can be referred to an independent assessment panel consisting of a technical expert and a retired judge. This panel must consider whether the proposed requirements contravene the explicit prohibition against 'backdoors'.

In fact, the Act has no ability to compel a company to build any type of capability that removes a form of electronic protection, like encryption. That is, if the company is not already capable of decrypting something, nothing in the Act can require them to build a capability to do it.

### **This law does not have adequate oversight**


All requests and requirements on industry are subject to extensive independent oversight by either the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman or State and Territory oversight bodies.

The relevant Commonwealth body is notified whenever a notice for assistance is issued, varied, extended or revoked. When an agency issues a notice, they must notify the company of their right to complain to the relevant body. Both the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security have the authority to inspect agency use of these powers by relevant agencies at any time. These bodies may make reports to Parliament on the outcome of their inspections.

Compulsory powers carry additional oversight measures to ensure they are used appropriately. For example, where a State or Territory law enforcement agency issues a notice to compel technical assistance, it must first be reviewed by the Australian Federal Police Commissioner.

Strict oversight also applies before a company can be compelled to build a new capability. Technical capability notices may only be issued by the Attorney-General. The Attorney-General's decision must also be reviewed and approved by the Minister for Communications. This creates a double-lock approval process to ensure the assistance sought has been thoroughly scrutinised and is reasonable, proportionate, practicable and technically feasible.





A company may also refer any requirement to build a capability to an independent assessment panel consisting of a retired senior judge and a technical expert. This panel must consider whether proposed requirements will inadvertently create a backdoor. Further, any decision to compel assistance may be challenged through judicial review proceedings.

### Public transparency is insufficient

Given the sensitive work done by law enforcement, security and intelligence agencies and the need to protect commercially sensitive information, it will not always be possible to disclose sensitive details of how assistance has been provided. This principle is consistent with the current protections given to operational intelligence held by Australia's law enforcement and intelligence community.

Visibility over the use of the industry assistance powers is possible through mandated annual reporting requirements which require law enforcement agencies to record the number of times each power is used within a 12-month period and also disclose the type of offences the powers were used to investigate. This data will be included in the annual report required to be prepared under **subsection 186(2)**

of the Telecommunications (Interception and Access) Act 1979 alongside data concerning the use of related warrants and authorisations.

Companies and their specified personnel are also authorised to make statistical disclosures to reveal the number of requests and notices received over the course of a six-month period and reveal whether that assistance was voluntary or compulsory. Additionally, where a company provides assistance they may seek authorisation from the issuing agency to disclose information about this assistance. This process will ensure operational details are protected, while giving companies the possibility to inform interested parties about the help they are giving to authorities. Provision for these disclosures appears in **subsections 317ZF(13) and 317ZF(14) – (17)**.

### Police use this law to prosecute minor offences

The industry assistance powers are only available to agencies in limited circumstances. There is an express requirement that the industry assistance powers can only be used by police to enforce the criminal law for serious offences, being offences that involve a penalty of at least three years imprisonment.

To access communications content and data an underlying warrant or authorisation is still required. For example, the legislation does not replace the need for police to seek a warrant from an independent authority to intercept communications. Generally these warrants are available for offences punishable by a maximum of seven years imprisonment or more.

### The availability of these powers may expand due to scope creep

The list of agencies with access to industry assistance powers can only be expanded through legislative amendment, which would include further parliamentary scrutiny. Only Australia's core law enforcement, security and intelligence agencies are able to utilise the industry assistance powers.

### The Five Eyes alliance may take advantage of this law

The Assistance and Access Act is an Australian solution to an Australian problem – it was not requested by, or designed for, Australia's Five Eyes partner countries. While the Five Eyes share intelligence for security purposes, foreign assistance in connection with information obtained under this legislation

---

*continued on page 40*



will be undertaken consistent within the established mutual legal assistance process or through existing, and bounded, channels of cooperation.

Foreign partnerships are critical to the detection and disruption of transnational crime and attacks that are coordinated through several countries.

The industry assistance powers for intelligence gathering are limited to collecting intelligence connected with Australia. This is because the Act requires a geographical nexus between the activities of a company and Australia. Further, access to content or non-content data through industry assistance powers requires a valid warrant or authorisation.

### Capabilities built by the Government will leak

Both industry and law enforcement and security agencies have robust procedures in place to protect sensitive information and have made significant investments in the development of strong cyber security protocols that will be used to secure information relating to any form of assistance. Additionally, Australia's law enforcement and security agencies are experienced in managing operational sensitivities and will take steps to minimise risks or exposure of information.

### This law has lead to mass surveillance

The Assistance and Access Act does not authorise mass surveillance. The Act expressly prohibits the Government from requiring a company to build an interception capability or a data retention capability. Any requirements must be reasonable, proportionate, practicable and technically feasible and are subject to independent oversight and judicial review.

If conducted, digital surveillance must be consistent with existing legal regimes, like the warrant process for intercepting telecommunications in the Telecommunications (Interception and Access) Act 1979.

The powers available under these laws are inherently targeted.

### This law can compel employees to work in secret without the knowledge of their organisation

Media reporting that has proposed this scenario is incorrect and misleading. The industry assistance framework

is concerned with getting help from companies not people acting in their capacity as an employee of a company.

Requests for assistance are served on the corporate entity itself in line with the deeming service provisions in **section 317ZL**. A notice may be served on an individual if that individual is a sole-trader and their own corporate entity.

A company issued with a notice can disclose information about it under **paragraph 317ZF(3)(a)** in connection with the administration or execution of that notice. This allows an employer to disclose information to their employee and vice versa in the normal course of their duty.

Additionally, a company may disclose statistical information about the fact that they have received a notice consistent with **subsection 317ZF(13)**. Further, companies and their specified personnel may disclose notice information for the purposes of legal proceedings, in accordance with any requirements of law or for the purpose of obtaining legal advice. The notices themselves are therefore not 'secret' but information about their substance is controlled to protect sensitive operational and commercial information.

### This law harms Australia's tech sector

The Assistance and Access Act and, specifically, the industry assistance powers are not unique to Australia.

This legislation came after the passage of the UK's Investigatory Powers Act 2016 and New Zealand's Telecommunications (Interception Capability and Security) Act 2013, both of which deal with similar subject matter and provide powers to compel assistance from private companies.

During the development of the Australian legislation, the Government recognised concerns that the possibility of undisclosed changes to a company's services could harm products' competitiveness at market. To answer these concerns, the legislation includes provisions for companies to publish statistics regarding the number of requests or notices they have received in a six month period under **subsection 317ZF(13)** – including where this number is zero – and make conditional disclosures to interested parties about assistance given under **subsections 317ZF(14)-(17)**. In practice, this leaves

most companies unaffected, as they will be able to disclose that they have not been asked to provide assistance, while companies who do assist can demonstrate that their systems are not compromised by the assistance they have provided, consistent with the law's explicit protections against the creation of backdoors or the degradation of security features.

### Australian companies and their employees are hardest hit by this law

Companies that supply communications services and devices in Australia, regardless of whether they are incorporated in Australia or not, may be the subject of technical assistance obligations under the Assistance and Access Act. The measures do not place a greater burden on Australian companies nor do they allow authorities to compel Australian citizens working for communications companies offshore. Additionally, if issued a notice, Australian companies who primarily conduct business overseas are only obliged to assist Australian authorities to the extent that their activities relate to products and services being used within Australia. Services provided by Australian companies to persons offshore that relate to activities offshore are not classified as 'eligible activities' for the purposes of the legislation and are thus not captured by these laws.

The Act's provision for penalties against individuals is not intended to apply to employees of a non-compliant company. If a company does not comply with their assistance obligations, any enforcement action that may be undertaken will apply to the enterprise. Penalties for individuals in the legislation are for the purpose of potential enforcement proceedings against sole-traders and individuals acting as businesses.

Criminal offences for the disclosure of sensitive and protected information (including sensitive commercial information) apply equally to Government officials and agency personnel and are consistent with secrecy provisions in other Commonwealth laws. Importantly, a suite of exceptions to the offence of unauthorised disclosure applicable to providers and specified personnel are listed in **subsections 317ZF(3), (12B), (13), (15) and (16)**.



**THE INCOME TAX  
PROFESSIONALS**

**[www.itp.com.au](http://www.itp.com.au)**

**Proudly Supporting  
the AiPol Magazine.**





Lunar New Year is a festival celebrated in many places around the world. For those who celebrate, this time of the year when we usher in the Year of the Ox is a significant one.

For Buddhists, Lunar New Year and Maitreya Buddha's Holy Birthday are celebrated on the same day.

In folk culture, Maitreya Buddha is often known as the Laughing Buddha. Many people have a small statue of His joyful form in their hallways for good luck.

However, what many might not be aware of is that Maitreya Buddha is also known as the Compassion Clan Bodhisattva. His big belly can contain all the unfairness and suffering under the sun. His laugh welcomes all those looking for refuge in his compassion, and reminds us to be positive and forgiving.

Wishing everyone a happy and auspicious Lunar New Year!

