

CompLex



Senter for rettsinformatikk / Avdeling for forvaltningsinformatikk

Brendan John Nixon

The Case for Mandatory Encryption Backdoor Legislation

– Sabotaging the Right to Privacy or a Necessary Measure to Address the ‘Going Dark’ Problem?

2/2021



UiO : Det juridiske fakultet

Henvelselser om denne bok kan g  res til:
Senter for rettsinformatikk
Postboks 6706 St. Olavs plass
0130 Oslo
<http://www.jus.uio.no/ifp/om/organisasjon/seri/>

ISSN 2703-8777 Complex (online)

Grafisk produksjon: 07 Media AS – 07.no

Preface

The majority of the research for this paper was carried out under the aegis of the project ‘Security in Internet Governance and Networks: Analysing the Law’ (SIGNAL), whilst I was employed as a research assistant at the Norwegian Research Center for Computers and Law (NRCCL), University of Oslo. The research assistant position was funded by the Research Council of Norway and UNINETT Norid AS. I would like to thank my colleagues in the SIGNAL project and at the NRCCL for their review and commentary on previous versions of this paper. In particular, special thanks go to Professor Lee A. Bygrave and Ph.D. candidate Peter Davis for their proof-reading assistance and encouragement. The usual author disclaimer otherwise applies. References to legal instruments are to their amended state as of 1 April 2021.

Oslo, 12 April 2021

Brendan Nixon

Brendan John Nixon

BA, LLB (Hons), GDLP, LLM

Former Research Assistant with the Norwegian Research Center for Computers and Law, Department of Private Law, University of Oslo
b.j.nixon@gmail.com

Contents

Preface.....	3
List of terms and abbreviations	6
1 Introduction	8
1.1 Increasing use of encryption.....	8
1.2 Fear of the dark	11
1.3 Aim, scope and methodology.....	12
2 The problem with modern encryption technology from a law enforcement perspective	15
2.1 End-to-end encryption – data in transit	15
2.1.1 What is the problem with end-to-end encryption?.....	18
2.2 Device encryption – data at rest	19
2.2.1 What is the problem with encrypted devices?	20
2.3 What is an encryption backdoor?.....	22
2.4 How often are encrypted data encountered by law enforcement agencies?.....	24
2.5 What methods are available for investigating crimes where encrypted data are encountered?	26
3 Encryption regulation	29
3.1 A brief history of encryption regulation.....	29
3.2 Regulating access to encrypted data	31
3.3 Device backdoors	32
3.3.1 New York State Assembly Bill No. A08093.....	32
3.3.2 California State Assembly Bill No. 1681	33
3.3.3 French proposals	34
3.4 A backdoor for all encryption.....	35
3.5 Investigatory Powers Act 2016 (UK)	37
3.6 Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)	40
3.7 Anti-backdoor pressure from the EU	44

4	Is mandatory encryption backdoor legislation compatible with the right to privacy?	47
4.1	Article 17 of the ICCPR	48
4.1.1	Interference	48
4.1.2	Lawful and non-arbitrary	50
4.1.3	Violation assessment.	53
4.2	Article 8 of the ECHR.	53
4.2.1	Interference	54
4.2.2	In accordance with the law	56
4.2.3	Pursues a legitimate aim	56
4.2.4	Necessary in a democratic society	56
4.2.5	Violation assessment.	58
4.3	Remedies under the ICCPR and ECHR.	58
5	Conclusion.	60

List of terms and abbreviations

A29WP	Article 29 Data Protection Working Party
ACLU	American Civil Liberties Union
AA Act	Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)
AA Bill	Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth)
Android OS	Android mobile operating system
BEREC	Body of European Regulators for Electronic Communications
Charter	Charter of Fundamental Rights of the European Union
CSIS	Center for Strategic and International Studies
EARN IT Act	Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020
E2E	End-to-end
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
FBI	Federal Bureau of Investigation
GC16	General Comment 16
GCHQ	Government Communications Headquarters
ICCPR	International Covenant on Civil and Political Rights
IM	Instant messaging
IMCO	European Parliament Committee on the Internal Market and Consumer Protection
iOS	Apple mobile operating system
IPA	Investigatory Powers Act 2016 (United Kingdom)
LEA	Law enforcement agency

MEBL	Mandatory encryption backdoor legislation
MMS	Multimedia Messaging Service
NSA	National Security Agency
OHCHR	Office of the United Nations High Commissioner for Human Rights
OTT	Over-the-top
PJCIS	Parliamentary Joint Committee on Intelligence and Security
SMS	Short Message Service
SoS	Secretary of State
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNGA	United Nations General Assembly
UNHR Committee	United Nations Human Rights Committee
UK	United Kingdom
UKHO	United Kingdom Home Office
USA	United States of America
USG	United States Government

1 Introduction

The increasing use of end-to-end (E2E) encrypted communications and encryption-enabled devices has prompted legislators in several jurisdictions to propose legislation to ensure law enforcement agencies (LEAs) can access decrypted, intelligible data. The ability to access intelligible data assists LEAs to prevent crime and prosecute criminals. However, pursuing broad legislative measures that target encryption technology raises privacy and security concerns, particularly in the wake of Edward Snowden's revelation of widespread government surveillance practices. To date there has been limited legal analysis of legislative proposals targeting encryption technology to determine if they would be effective in providing LEAs with decrypted data and whether such legislation is compatible with the internationally recognised right to privacy. This paper argues that it is not currently necessary, nor is it proportionate, to pursue legislation mandating the incorporation of so-called encryption 'backdoors' into encryption technology.

1.1 Increasing use of encryption

The widespread government surveillance of electronic communications revealed by Edward Snowden in June 2013 was a global catalyst for increased privacy concerns. Classified documents released by Snowden revealed extensive warrantless surveillance of electronic communications was being conducted by government agencies, including the National Security Agency (NSA) in the United States of America (USA) and the Government Communications Headquarters (GCHQ) in the United Kingdom (UK).¹ The surveillance was possible in part because the data sent between the internal company data centres and service providers of major technology companies, such as Apple, Google, Microsoft and Yahoo, were not encrypted.² In the fallout from the revelations, technology companies scrambled to announce new encryption policies and sought to incorporate encryption into their products and services to protect both internal data and customer data from unauthorised access.³ In September 2014, Apple

1 David O'Brien, 'Half Measures on Encryption Since Snowden' (*MIT Technology Review*, 25 January 2016) <www.technologyreview.com/s/545636/half-measures-on-encryption-since-snowden/>. All hyperlinks cited within this paper were active as at 1 April 2021 unless stated otherwise. Accordingly, access dates for each hyperlink have not been provided.

2 *ibid.*

3 *ibid.*

announced plans to incorporate encryption of all passcode protected content on Apple devices by default in the next version of Apple's mobile operating system, iOS.⁴ In November 2014, the Financial Times reported that companies including Facebook, Google and Yahoo had tried to improve their respective approaches to encryption dramatically in response to the Snowden revelations.⁵ Within the next few months, Google announced the upcoming version of its mobile operating system, Android OS, would enable devices to be encrypted by default, WhatsApp announced it would support E2E encryption of messages and Yahoo introduced source code for an Internet browser extension that would encrypt communications sent via Yahoo Mail.⁶ By 2019, encryption-by-default was a central part of the products provided by major technology companies.⁷

E2E encryption provides a cheap and effective way to ensure electronic communications are restricted to the intended audience and inaccessible in an intelligible format to third parties, including LEAs. E2E encryption is currently widely available via free to use instant messaging (IM) applications such as Apple's iMessage, Facebook Messenger, Signal, Telegram and WhatsApp.⁸ Several IM applications, including WhatsApp and iMessage, have enabled E2E encryption by default, removing any conscious choice by users of these applications to utilise E2E encryption.⁹ According to estimates in a report published by the Center for Strategic and International Studies (CSIS) in February 2017, approximately 18% of global communications traffic, which includes messages sent via Short Message Service (SMS), multimedia message service (MMS), email and IM

4 Johnathan L Zittrain and others, 'Don't Panic: Making Progress on the "Going Dark" Debate' (The Berkman Center for Internet and Security of Harvard University, 1 February 2016) <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf>, 3.

5 Hannah Kuchler, 'Tech Companies Step Up Encryption in Wake of Snowden' (*Financial Times*, 5 November 2014) <www.ft.com/content/3c1553a6-6429-11e4-bac8-00144feabdc0>.

6 Zittrain and others (n 4) 3-4.

7 Edward Snowden, 'Without Encryption, We Will Lose All Privacy. This is Our New Battleground' (*The Guardian*, 15 October 2019) <www.theguardian.com/commentisfree/2019/oct/15/encryption-lose-privacy-us-uk-australia-facebook>.

8 IM applications allow real-time, two-way communication over the Internet. See 'instant messaging' entry in Charles Doyle (ed), *A Dictionary of Marketing* (Oxford University Press 2016).

9 WhatsApp, 'End-to-End Encryption' <<https://faq.whatsapp.com/en/general/28030015/?category=5245250>> and Apple, 'Privacy' (see section under 'iMessage and Facetime') <www.apple.com/privacy/approach-to-privacy/>.

applications, utilised E2E encryption.¹⁰ The share of E2E encrypted traffic is predicted to grow as IM applications continue to usurp traditional electronic communication methods, such as SMS, MMS and email.¹¹

In addition to the widespread availability of E2E encrypted IM applications, encryption-enabled devices are becoming more common. The operating systems running on many current generation personal computers, tablets and smartphones allow users to restrict access to the data stored on the device through a process known as full disk encryption.¹² When a device is encryption-enabled, the content of the device, or more specifically, the data stored on the hard disk(s) of the device, can be encrypted manually by the user or automatically when the device is locked or turned off. The subsequent decryption of the data is commonly linked with accessing the device, so when the device is unlocked, be it by way of a passcode, a pattern or through a biometric scanner, the data are decrypted for the user to view and edit.¹³ According to the previously cited 2017 report from CSIS, an average of 21% of mobile devices in the world have full disk encryption and 47% of all mobile devices in the USA have full disk encryption.¹⁴ These figures should be treated with some caution, however, as the CSIS report does not provide a definition of mobile device and does not make a clear distinction between devices that are *encryption-enabled* and devices that have full disk encryption *enabled by default*. It does not automatically follow that data stored on an encryption-enabled device are encrypted.

10 William A Carter, James A Lewis and Denise E Zhang, *The Effect of Encryption on Lawful Access to Communications and Data* (A Report of the CSIS Technology Policy Program, Rowman & Littlefield 2017) iv and 7. The Center for Strategic & International Studies (CSIS) has been criticised for its reliance on funding from foreign governments and potential bias associated with its sources of funding, see Eric Lipton, Brooke Williams and Nicholas Confessore, 'Foreign Powers Buy Influence at Think Tanks' (*The New York Times*, 6 September 2014) <www.nytimes.com/2014/09/07/us/politics/foreign-powers-buy-influence-at-think-tanks.html>. However, the estimates in the cited CSIS report regarding encryption use in global communications traffic are based on publicly available statistics and have been cited by the European Commission (see European Commission, 'Encryption' <https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/encryption_en>).

11 Carter, Lewis and Zhang (n 10) 7-8.

12 Information Commissioner's Office, 'Encryption and Data Storage' <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/encryption-and-data-storage>>.

13 For an example of the decryption process on Apple devices running iOS, see Apple, 'Apple Platform Strategy' <<https://support.apple.com/en-au/guide/security/welcome/web>>, particularly the content regarding encryption and data protection.

14 Carter, Lewis and Zhang (n 10) 9.

1.2 Fear of the dark

E2E encrypted communications and encryption-enabled devices help to protect against interference with privacy in an increasingly online society where privacy can be elusive. However, the increasing use of encryption has implications for the ability of LEAs to gather evidence for the prevention and prosecution of crime. For example, E2E encrypted communications inhibit the efforts of LEAs to actively monitor, intercept and access the content of communications sent or received by identified or potential suspects, even in circumstances where LEAs have legal authority to conduct such activities. Similarly, a lawfully seized electronic device is of limited evidentiary value to a LEA, beyond being a potential source of fingerprints or DNA, if the data stored on the device are encrypted and the LEA is unable to access the data in an intelligible format.

The difficulties experienced by LEAs in attempting to legally intercept and access intelligible data as a result of the use of encryption has been described as the ‘going dark’ problem.¹⁵ The challenges posed by the so-called going dark problem have prompted statements from government representatives and law enforcement officials in several countries, including Australia, France, Germany, the UK and the USA, indicating an intent to enact legislation to ensure LEAs can lawfully access intelligible data.¹⁶ Government representatives from Australia, the UK and the USA have attempted to pressure Facebook not to proceed with plans to implement E2E encryption across various Facebook owned messaging services without including an ability to lawfully access the content of the communications in an intelligible format.¹⁷ A recurring theme in these

15 Federal Bureau of Investigation (FBI), ‘Going Dark’ <www.fbi.gov/services/operational-technology/going-dark>.

16 For example, see statements from the former Director of the FBI, James Comey, in October 2014 (James B Comey, ‘Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?’ (FBI, 16 October 2014) <www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>; the French and German interior ministers in August 2016 (Natasha Lomas, ‘Encryption Under Fire in Europe as France and Germany Call For Decrypt Law’ (TechCrunch, 24 August 2016) <<https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-france-and-germany-call-for-decrypt-law/?guccounter=1>>; former Australian Prime Minister, Malcolm Turnbull, in July 2017 (Alexandra Beech, ‘Facebook, Google Obligated to Decrypt Online Messages to Help Government Fight Terrorism’ (Australian Broadcasting Corporation, 14 July 2017) <www.abc.net.au/news/2017-07-14/facebook-google-to-be-forced-to-decrypt-messages-fight-terrorism/8707748>; former Home Secretary of the UK, Amber Rudd, in August 2017 (Mark Bridge, ‘Amber Rudd Demands ‘Back Door’ Access to Encrypted Messaging Apps’ (The Times, 2 August 2017) <www.thetimes.co.uk/article/amber-rudd-demands-back-door-access-to-encrypted-messaging-apps-0st27hzc>).

17 Julia Carrie Wong, ‘US, UK and Australia Urge Facebook to Create Backdoor Access to Encrypted Messages’ (The Guardian, 4 October 2019) <www.theguardian.com/technology/2019/oct/03/facebook-surveillance-us-uk-australia-backdoor-encryption>.

efforts is the idea that encrypted communications should not be above the law and providers of encryption technology must be able to provide data in an intelligible format when requested to do so by an LEA. Incorporating such an ability into encryption technology is sometimes referred to as providing an encryption backdoor or providing exceptional access.¹⁸

1.3 Aim, scope and methodology

The overall aim of this paper is to review the current technological and legal landscape to determine if it is necessary to introduce legislation to compel encryption technology providers to incorporate encryption backdoors into their technology. Such legislation is referred to as mandatory encryption backdoor legislation (MEBL) throughout this paper. Modern examples of draft and in force legislation that could amount to MEBL have been identified and analysed to determine how effective such legislation could be in providing LEAs with decrypted data. In addition to analysing the effectiveness of the identified draft and in force legislation, assessing the compatibility of MEBL with the right to privacy is also a focus of this paper. Determining the necessity of introducing MEBL feeds directly into assessing the compatibility of MEBL with the right to privacy.

Although the incorporation of encryption backdoors into encryption technology has the potential to impact several internationally recognised human rights,¹⁹ the right to privacy has been selected as a focal point due to the recurrence of privacy concerns when MEBL is discussed or proposed. Noting the right to privacy is interpreted and regulated differently around the world, this paper concentrates on the right to privacy as articulated in two major human rights instruments: the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR).²⁰ These instruments have been selected for their wider application in comparison to

18 Abelson and others, 'Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications' (*Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Technical Report*, 6 July 2015) <<https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8>>, 5.

19 The right to freedom of opinion and expression, the right to seek, receive and impart information and the right to freedom of peaceful assembly and association can be negatively affected by mass surveillance practices that would be possible if encryption backdoors were mandatory. See paragraph 14 of United Nations Office of the High Commissioner for Human Rights (OHCHR), 'The Right to Privacy in the Digital Age' (30 June 2014) UN Doc A/HRC/27/37.

20 International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) and Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).

other international and regional instruments, as measured by the number of state parties, and because they are applicable to several EU member states that have indicated a desire to introduce MEBL, including France and Germany.²¹ The Charter of Fundamental Rights for the European Union (Charter) also provides a right to privacy applicable in the EU, together with a closely linked right to protection of personal data. However, the Charter has been intentionally omitted from analysis in this paper to prevent duplication, noting the meaning and scope of the right to privacy provided in the Charter and the ECHR are the same.²²

A wide range of sources, including media reports, technology blogs and publications from think tanks and non-governmental organisations, have been consulted to identify statements from legislators and law enforcement officials who have indicated an intention to introduce MEBL. As a result of this research, relevant draft and in force legislation from Australia, France, the UK and the USA was identified for analysis. Despite reports that Germany was preparing a law that would force device manufacturers to incorporate encryption backdoors into their products,²³ no evidence of any draft legislation to that effect from Germany was identified for analysis in this paper.²⁴

Significant bias against MEBL was apparent in the reporting and commentary regarding the examples of MEBL identified for analysis. To address this apparent bias, this paper focuses on the original text of draft and in force legislation to

21 The ICCPR has 173 state parties and the ECHR has 47 state parties as at 1 April 2021.

22 See European Union Agency for Fundamental Rights, 'Article 7 – Respect For Private and Family Life' <<http://fra.europa.eu/en/charterpedia/article/7-respect-private-and-family-life>>. By way of Article 52(3) of the Charter, the meaning and scope of the right to privacy provided in Article 7 of the Charter is the same as the right to privacy provided in Article 8 of the ECHR. The right to privacy and the right to protection of personal data provided by the Charter have been considered together by the Court of Justice of the European Union, see *Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, paras 32-69.

23 See Catalin Cimpanu, 'Germany Preparing Law for Backdoors in Any Type of Modern Device' (*Bleeping Computer*, 5 December 2017) <www.bleepingcomputer.com/news/government/germany-preparing-law-for-backdoors-in-any-type-of-modern-device/>.

24 A report published by New America in December 2017, updated in January 2018, supports the conclusion that Germany has not (yet) proposed any legislation that could be interpreted as mandating encryption backdoors. See Bhairav Acharya and others, 'Deciphering the European Encryption Debate: Germany' (*New America*, January 2018) <https://d1y8sb8igg2f8e.cloudfront.net/documents/Transatlantic_Encryption_Germany.pdf>. Further, the authors of a brief issued by the Carnegie Endowment for International Peace in May 2019 concluded that Germany has not yet made any attempts to weaken encryption or require vendor assistance for lawful access. See Sven Herpig and Stefan Heumann, 'The Encryption Debate in Germany' (*Carnegie Endowment for International Peace*, May 2019) <https://carnegieendowment.org/files/WP_The_Encryption_Debate_in_Germany_WEB.pdf>, 6.

conduct an independent and neutral analysis. Secondary material was consulted to assist with the translation of French legislation. The example MEBL identified has been analysed to determine how it would apply to encryption technology and whether it would be effective in obtaining decrypted data for LEAs. Determining the effectiveness of the example MEBL is a difficult task and depends on the peculiarities of each jurisdiction, but some general deficiencies were identified with the ability of the example MEBL to assist LEAs to obtain decrypted data. To assess the compatibility of MEBL with the right to privacy provided in the ICCPR and ECHR, original source material from the United Nations Human Rights Committee (UNHR Committee) and judgments from the European Court of Human Rights (ECtHR) have been consulted. Recent reports from various United Nations (UN) Special Rapporteurs have also been consulted to provide current interpretations and opinions regarding the application of the right to privacy to encryption technology.

Section two of this paper provides a basic overview of modern encryption technology and identifies the problems with this technology from a law enforcement perspective, focussing on E2E encryption and encryption-enabled devices. Section two also details how often encrypted data are encountered by LEAs and what methods are currently available to LEAs to conduct investigations when encrypted data are encountered. Section three focuses on encryption regulation and commences with a brief summary of the history of encryption regulation before focussing on recent examples of draft and in force legislation that could amount to MEBL. These examples are analysed for their ability to assist LEAs to obtain decrypted data. Section four consists of an assessment of the compatibility of MEBL with the right to privacy, as articulated in the ICCPR and ECHR. Based on this assessment, the paper concludes that it is not currently necessary to introduce MEBL and, as a direct consequence of this finding, MEBL will violate the right to privacy if it is deemed to constitute an interference with the right to privacy.

2 The problem with modern encryption technology from a law enforcement perspective

As part of the so-called going dark problem, the FBI identified two distinct challenges with modern encryption practices.²⁵ The first challenge concerns access to real-time data in transit, such as telephone calls and messages sent via SMS, MMS and over-the-top (OTT) services such as email and IM applications.²⁶ The second challenge concerns access to data at rest stored on devices, including messages, photos, videos and other documents. This section details how modern encryption technology operates to limit LEA access to data in transit and data at rest, how often encrypted data are encountered by LEAs and what methods are currently available to LEAs to conduct investigations where encrypted data are encountered.

2.1 End-to-end encryption – data in transit

In simple terms, encryption is the process of rendering information unintelligible to unauthorised recipients.²⁷ Modern encryption generally involves the use of a computer to apply an algorithm to clear data (plaintext) prior to scrambling the data into an unreadable format (ciphertext).²⁸ One or more keys are incorporated into the ciphertext during this process and, without the correct key, the ciphertext cannot be decrypted back into plaintext, even if the algorithm applied to the original data is known.²⁹ Once data are encrypted, only those who have access to a decryption key are able to decrypt the data into plaintext.³⁰ There are two main types of modern encryption: symmetric and asymmetric.³¹ Symmetric encryption utilises the same key for both encryption and decryption, whereas

25 See FBI (n 15).

26 'Over-the-top' refers to 'content, services or applications that are provided to the end user over the public Internet'. See Body of European Regulators for Electronic Communications (BEREC), 'Report on OTT services' (January 2016) <http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5751-berec-report-on-ott-services_0.pdf>, 6.

27 See 'encryption' entry in Andrew Butterfield, Gerard Ekembe Ngondi and Anne Kerr (eds), *A Dictionary of Computer Science* (7th edn, Oxford University Press 2016).

28 Global Partners Digital, *Travel Guide to the Digital World: Encryption Policy for Human Rights Defenders* (Global Partners Digital 2017) 12.

29 *ibid.*

30 Information Commissioner's Office, 'Encryption' (4 April 2017) <<https://ico.org.uk/media/for-organisations/guide-to-data-protection/encryption-1-1.pdf>>, 3.

31 *ibid.*, 11.

asymmetric encryption utilises a different key for encryption (public key) and decryption (private key).³² Due to its use of a second, public key, asymmetric encryption is also known as public key encryption.³³

When the encryption applied to transmitted data is described as end-to-end, this acknowledges the relevant data are encrypted at the sender's end, remain encrypted during transmission and are then decrypted at the recipient's end. There are no intermediate stages of decryption and re-encryption during the transmission process.³⁴ E2E encryption is a form of asymmetric encryption, utilising a public key for encryption and a private key for decryption. The only parties who can view the plaintext are the sender and the receiver, as third parties are not able to access the private key required to decrypt the ciphertext.³⁵

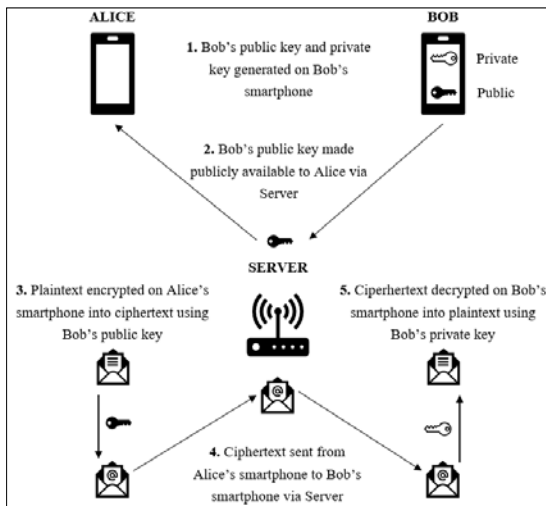


Diagram 1: How an encrypted message is sent between two smartphones utilising E2E encryption.³⁶

³² Bert-Jaap Koops, *The Crypto Controversy* (Kluwer Law International 1999), 36.

³³ *ibid.*

³⁴ See 'end-to-end encryption' entry in Butterfield, Ngondi and Kerr (n 27).

³⁵ Andy Greenberg, 'Hacker Lexicon: What is End-to-End Encryption?' (*Wired*, 25 November 2014) <www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption>.

³⁶ Diagram created by author based on images from ProtonMail, 'What is End-to-End Encryption and How Does it Work?' (*ProtonMail*, 7 March 2018) <<https://protonmail.com/blog/what-is-end-to-end-encryption/>> and Nick Evershed, 'Australia's Plan to Force Tech Giants to Give Up Encrypted Messages May Not Add Up' (*The Guardian* 14 July 2017) <www.theguardian.com/technology/2017/jul/14/forcing-facebook-google-to-give-police-access-to-encrypted-messages-doesnt-add-up>.

Both Google Play and iTunes offer several free IM applications that incorporate E2E encryption, including Facebook Messenger, Signal, Telegram and WhatsApp.³⁷ These applications can be used on a range of devices with an Internet connection, including smartphones, laptops and desktop computers. However, the applications are not interoperable for the purposes of sending E2E encrypted data, both the sender and the recipient must be using the same application for the transmitted data to be E2E encrypted. Of the applications offering E2E encryption, WhatsApp is the most popular, with an estimated 2 billion monthly active users as of January 2021.³⁸ E2E encryption is the default setting for WhatsApp and cannot be deactivated by users.³⁹ iMessage, the default messaging application for Apple products such as the iPhone and iPad, also utilises E2E encryption, but is only available on Apple products.⁴⁰

E2E encryption of emails is not as prevalent as E2E encryption of data sent via IM applications.⁴¹ The limited incorporation of E2E encryption into email platforms has been attributed to business reasons and the different expectations of email users in comparison to users of IM applications. For example, email platforms allow users to access a single email account with multiple devices, recover forgotten passwords and send emails to contacts who utilise a different email platform.⁴² The incorporation of E2E encryption into email platforms would inhibit several, if not all, of these functions.⁴³

The incorporation of E2E encryption into IM applications is both a technical feature and a sales pitch. There are several examples of providers of E2E encrypted messaging applications taking an outright stance against encryption backdoors to ensure the privacy of customer data.⁴⁴ Apple previously stated in their privacy information that they ‘refuse to add a backdoor into any of our products’.⁴⁵ This anti-backdoor stance is also advanced by Crypho, a Norwegian start-up company offering an E2E encrypted IM application. Crypho’s policy goes beyond Apple’s refusal to add backdoors and states: ‘Crypho can not [sic] grant access to anyone to read your encrypted messages or files or be forced to

37 Google Play offers applications for devices running Android OS. iTunes offers applications for devices running iOS. Signal can also be used to send SMS messages, which are not E2E encrypted.

38 Statista, ‘Most Popular Global Mobile Messenger Apps as of January 2021, Based on Number of Monthly Active Users’ (*Statista* January 2021) <www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/#statisticContainer>.

39 WhatsApp (n 9).

40 Like Signal, iMessage can also be used to send messages via SMS, which are not E2E encrypted.

41 Carter, Lewis and Zhang (n 10) 10.

42 *ibid.*

43 *ibid.*

44 Comey (n 16).

45 Apple (n 9). The quoted text has since been removed from the cited source.

install back doors'.⁴⁶ In providing E2E encryption, the first part of Crypho's statement is uncontroversial. Without the decryption key, Crypho is not able to obtain the data sent between Crypho users in plaintext and therefore, Crypho cannot provide the plaintext to a LEA. However, Crypho's claim that they cannot be forced to install backdoors is curious, suggesting Crypho is above the law. Perhaps intended as nothing more than marketing puff or a reflection of the Norwegian government's pro-encryption stance, Crypho does not explain how it would be able to avoid a legal obligation to incorporate an encryption backdoor in the event MEBL was introduced in Norway. If MEBL was introduced in Norway, encryption technology providers such as Crypho would be forced to incorporate encryption backdoors into their technology unless the MEBL could be successfully challenged in court or was otherwise repealed. As will be discussed later, it could be possible to challenge the validity of any such MEBL on the basis that it breaches the right to privacy.

2.1.1 What is the problem with end-to-end encryption?

The inability of a third party to access transmitted data in plaintext is the distinguishing feature of E2E encrypted IM applications in comparison to other popular forms of electronic communication, such as SMS, MMS and email.⁴⁷ When a telephone call is made or a message is sent via SMS, MMS or unencrypted email, the applicable law in the relevant jurisdiction may allow a LEA to compel the respective telephone or Internet service provider to assist with intercepting the communication in transit.⁴⁸ In addition, the telephone or Internet service provider might collect and store the content of any sent messages and associated metadata (such as the time and date a call was made or a message was sent and the phone numbers or email addresses of the parties involved). The ability of a telephone or Internet service provider to deliver the content of messages and associated metadata to a LEA depends on a combination of applicable data retention laws and the business practices of the relevant service provider. For example, legislation may require service providers to collect and store certain data for a fixed period to assist with criminal investigations.⁴⁹ In that case, a LEA equipped with an appropriate legal authority or instrument, such as a court

46 Crypho, 'Frequently Asked Questions' (Crypho 2020) <www.crypho.com/faq/>.

47 Third party is used here to refer to any party who is not the sender or the intended recipient of the encrypted data.

48 For example, Part 2 of the UK's Investigatory Powers Act 2016 authorises the interception and examination of communications in accordance with a warrant.

49 The EU's ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, as amended by Directive 2006/24/EC and Directive 2009/136/EC) includes a carve out provision in Article 15(1) to allow member states to adopt legislation requiring data retention for certain purposes (such as safeguarding national security or to assist with the 'prevention, investigation, detection and prosecution of criminal offences').

order or a warrant, could compel a telephone or Internet service provider to deliver any relevant data held, such as the content of messages and any associated metadata.⁵⁰

In contrast, when transmitted data are E2E encrypted, the provider's server 'acts as an illiterate messenger, passing along messages that it can't itself decipher'.⁵¹ Accordingly, the plaintext is not available to any service provider involved in the transmission of the data and therefore a LEA cannot compel a service provider to provide the data in plaintext, regardless of any legal authority or instrument the LEA may have. This renders ineffective many traditional investigative techniques, such as wiretapping and compelling service providers to provide content data.⁵² However, E2E encryption usually only applies to the content of the transmitted data, not the metadata.⁵³ Depending on a combination of applicable data retention laws and the business practices of any service provider involved in the transmission of E2E encrypted data, metadata *might* be available to a service provider and therefore, compellable for production by a LEA equipped with an appropriate legal authority or instrument.⁵⁴

2.2 Device encryption – data at rest

The method of encrypting data stored on a device can vary from encryption of single files or folders to encryption of an entire hard disk (full disk encryption). For the purposes of this paper, the term 'device encryption' is used to refer to the process of encrypting data stored on a device and the term 'encryption-enabled device' is used to refer to devices capable of device encryption (either manually or by default). The data stored on encryption-enabled devices, such as current generation iPhones,⁵⁵ are often encrypted when the device is off or locked and are decrypted by entering a passcode (involving a combination of alphanumeric characters), a pattern or by using a biometric reader.⁵⁶ Simply because access to

50 For example, see Part 3 of the UK's Investigatory Powers Act 2016. Section 61 allows a 'designated officer of a relevant public authority' to authorise, among other powers, the obtaining of communications data from any person or telecommunication system.

51 Greenberg (n 35).

52 Europol, *The Internet Organised Crime Threat Assessment (IOCTA 2017)* (Europol 2017) 63.

53 Information Commissioner's Office (n 30) 9.

54 Thomas Brewster, 'Forget About Backdoors, This is the Data WhatsApp Actually Hands to Cops' (*Forbes* 22 January 2017) <www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoor-government-data-request/#30be88c91030>.

55 At the time of writing, current generation iPhone models were running iOS 14.

56 For further information on Apple's device encryption process for iOS 14, see Apple, 'Apple Platform Security' (Apple February 2021) <<https://support.apple.com/guide/security/welcome/1/web>>.

a device is restricted by a passcode or a biometric reader does not mean data stored on the device are encrypted, although it is becoming more common for data stored on an encryption-enabled device to be encrypted when the device is locked or off.⁵⁷ The UK Information Commissioner's Office has claimed most modern operating systems utilise full disk encryption,⁵⁸ however, the current personal computer operating systems offered by Microsoft (Windows 10) and Apple (macOS Big Sur) require users to enable device encryption, it is not the default setting.⁵⁹ Full disk encryption is the default setting for devices running the current versions of iOS and Android OS, with the decryption process linked to any access restriction enabled on the device (such as entering a passcode, a pattern or by using a biometric reader).⁶⁰

2.2.1 What is the problem with encrypted devices?

The problem with encrypted devices from a LEA perspective is that they hold data that are difficult or impossible to obtain in plaintext. When combined with E2E encrypted IM applications, encrypted devices ensure there is only an extremely limited possibility that LEAs will ever be able to see certain data in plaintext.⁶¹ The ability of an encrypted device to inhibit a criminal investigation was demonstrated in a short-lived, yet high profile legal dispute between the United States Government (USG) and Apple in 2016. The dispute concerned a locked and encrypted iPhone 5 that belonged to Syed Farook, one of two perpetrators of a shooting in San Bernardino, California, who was subsequently killed by police.⁶² After initially requesting Apple's assistance to circumvent the security measures on the retrieved iPhone, the USG dropped its court proceedings

57 David Nield, 'Why You Should Be Encrypting Your Devices and How to Easily Do It' (*Gizmodo* 4 September 2017) <<https://gizmodo.com/why-you-should-be-encrypting-your-devices-and-how-to-ea-1798698901>>. Encryption is enabled by default in Apple's iOS and Android OS 6.0 Marshmallow or later versions.

58 Information Commissioner's Office (n 30) 6.

59 Windows 10 and macOS Big Sur both require users to manually turn on device encryption. See Microsoft, 'Turn on Device Encryption' (*Microsoft* 2020) <<https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption>> and Apple, 'Use FileVault to Encrypt the Startup Disk on Your Mac' (*Apple* 30 November 2018) <<https://support.apple.com/en-au/HT204837>>.

60 Nield (n 57).

61 An example of this limited opportunity is the infiltration of an encryption-enabled device to remotely monitor its use. See UNGA, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism' (23 September 2014) UN Doc A/69/397, 3-4, para 6.

62 Danny Yadron, 'San Bernardino iPhone: US Ends Apple Case After Accessing Data Without Assistance' (*The Guardian* 29 March 2016) <www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone>.

against Apple when it was able to successfully obtain decrypted data from the iPhone with the assistance of a third party.⁶³

It has been suggested the USG initiated the litigation against Apple to create a legal precedent to compel US-based technology companies to provide backdoor access to encrypted devices for US-based LEAs.⁶⁴ However, the fact the USG dropped the case once they had access to decrypted data from the iPhone suggests otherwise. Regardless of the motivations for litigating, the FBI, acting on behalf of the USG, is estimated to have spent US\$900,000 to obtain decrypted data from Farook's iPhone.⁶⁵ The USG's ability to obtain decrypted data from the iPhone, albeit for a significant sum of money, illustrated that device encryption does not provide absolute protection from third party access to decrypted data. It also contradicted suggestions that encryption backdoors were necessary, with supporting legislation to mandate such backdoors, to ensure LEAs could obtain decrypted data from an encrypted device. Although an encryption backdoor would have made the FBI's investigation easier and cheaper to conduct, it was, in this case at least, not necessary to have an encryption backdoor to retrieve decrypted data from the subject iPhone. It should not be presumed that well-financed LEAs will always be able to circumvent device encryption, particularly noting Farook's iPhone was an iPhone 5, which has been superseded by newer models with more secure hardware and software. However, several companies, such as Cellebrite, claim to be able to obtain decrypted data from a range of encrypted devices, including the latest iPhone models.⁶⁶

It is unclear how the third party contracted by the USG was able to circumvent the security measures on Farook's iPhone, but it is possible a brute force approach was adopted. Brute force in the context of a passcode protected encrypted device is a trial and error method utilising software to enter possible passcode combinations in rapid succession until the correct passcode is identified to unlock the device and decrypt its contents.⁶⁷ Apple has suggested it would take more than five and a half years for a brute force approach to 'try all combinations of a

63 *ibid.*

64 Kieran McCarthy, 'Did the FBI Engineer its iPhone Encryption Court Showdown with Apple to Force a Precedent? Yes and No, Say DoJ Auditors' (*The Register* 27 March 2018) <www.theregister.com/2018/03/27/fbi_encryption_showdown/>.

65 Matt Novak, 'The FBI Paid \$900,000 to Unlock the San Bernardino Terrorist's iPhone' (*Gizmodo* 8 May 2017) <<https://gizmodo.com/the-fbi-paid-900-000-to-unlock-the-san-bernardino-kill-1795010203>>.

66 Thomas Brewster, 'The Feds Can Now (Probably) Unlock Every iPhone Model in Existence – Updated' (*Forbes* 26 February 2018) <www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#59e6bc3c667a>.

67 Techopedia, 'What is a Brute Force Attack?' (*Techopedia* 1 July 2020) <www.techopedia.com/definition/18091/brute-force-attack>.

six-character alphanumeric passcode with lowercase letters and numbers'.⁶⁸ In reality, this timeframe is somewhat misleading, as this is the time required to test *all* possible combinations involving six alphanumeric characters. The default prompt on current generation iPhones with English as the operating language is for a user to enter a passcode consisting of six numbers, without using any letters.⁶⁹ This lowers the number of potential passcode combinations dramatically in comparison to a six-character alphanumeric passcode. Even if LEAs have time and money on their side, stronger protections such as forced time delays between passcode attempts and auto-erase features activated by multiple unsuccessful access attempts are making it increasingly more difficult for LEAs to obtain decrypted data from encrypted devices.⁷⁰

2.3 What is an encryption backdoor?

'Encryption backdoor' is used in this paper to describe the intentional or unintentional incorporation of a capability into encryption technology that allows a third party to decrypt encrypted data. Third party in this definition refers to a party who is not the sender or the intended recipient of encrypted data or, in the case of an encryption-enabled device, a party who is not the owner or authorised user of an encryption-enabled device. Third parties therefore include Internet service providers, device manufacturers, software developers, LEAs and hackers. Encryption backdoors are not a novel concept and have a long history of criticism.⁷¹ The concept of an encryption backdoor first came to mainstream attention via the proposed Clipper Chip in the USA in the early 1990s, which was abandoned before it could be implemented on a mass scale.⁷²

The term 'backdoor' in the context of encryption is loaded and has been said to imply 'surreptitious access and a lack of accountability'.⁷³ Due to negative connotations associated with the term, several government officials have moved to

68 Apple, 'Passcodes' (Apple 2020) <<https://support.apple.com/guide/security/passcodes-sec20230a10d/1/web/1>>.

69 Apple, 'Use a Passcode With Your iPhone, iPad, or iPod Touch' (Apple 18 March 2021) <<https://support.apple.com/en-ca/HT204060>>, see step 3 under 'Setup a passcode'.

70 Carter, Lewis and Zhang (n 10) 5-6.

71 For examples, see: A. Michael Froomkin, 'The Metaphor is the Key' (1995) 143(3) University of Pennsylvania Law Review 709, particularly 764-843; Abelson and others, 'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption' [1997] Columbia University Academic Commons; Abelson and others (n 18); and Bert-Jaap Koops and Eleni Kosta, 'Looking for Some Light Through the Lens of "Cryptowar" History: Policy Options For Law Enforcement Authorities Against "Going Dark"' (2018) 34 Computer Law and Security Review 890.

72 Global Partners Digital (n 28) 31. The Clipper Chip is discussed further in section 3.1.

73 Carter, Lewis and Zhang (n 10) 3.

distance themselves from referring to a backdoor when proposing measures to assist LEAs to obtain decrypted data. For example, Former FBI Director James Comey referred to a ‘front door’ when proposing that modern encryption technology should include interception capabilities to assist LEAs.⁷⁴ In response to suggestions that proposals in Australia regarding decryption powers amounted to a backdoor, then Department of Home Affairs secretary, Michael Pezzullo, described the term as ‘shorthand, colloquial, and in many respects, highly ill-informed shorthand’.⁷⁵ Pushed for a definition of a backdoor, former Australian Prime Minister Malcolm Turnbull is reported to have said ‘a backdoor is typically a flaw in a software program that perhaps the developer of the software program is not aware of and that somebody who knows about it can exploit’.⁷⁶ Even encryption technology itself carries negative connotations and has a history of being linked with those who are hiding criminal conduct.⁷⁷ Despite the negative connotations associated with the term, encryption backdoor is used neutrally throughout this paper without any intention of casting encryption backdoors in either a positive or negative light.

Attempting to define the technical workings of an encryption backdoor is beyond the scope of this paper and, to date, there is no specific outline of LEA requirements for an encryption backdoor.⁷⁸ Section three demonstrates, in proposing MEBL, legislators have generally refrained from providing any guidance to encryption technology providers as to how they could or should go about ensuring they can provide decrypted data when requested to do so. A group of leading computer scientists noted in the ‘Keys Under Doormats’ report that one way of ensuring LEAs have access to decrypted data would be to provide LEAs with direct access to a decryption key via a key escrow system, as was the intention of the Clipper Chip. This involves the encryption of a decryption key with the public key of an escrow agent. When a LEA obtains encrypted data in transit or at rest, the help of the escrow agent can be enlisted to decrypt the relevant decryption key and provide it to the LEA, therefore allowing the LEA to decrypt the obtained data.⁷⁹ In theory, a key escrow system prevents LEAs from having unrestricted access to decryption keys. However, the authors of ‘Keys Under Doormats’ identified several technical and procedural problems inherent in a

74 Comey (n 16).

75 Chris Duckett, ‘Australian Decryption Legislation Will Not Undermine ‘Legitimate Encryption’: Home Affairs’ (ZDNet 26 February 2018) <www.zdnet.com/article/australian-decryption-legislation-will-not-undermine-legitimate-encryption-home-affairs/>.

76 Rae Johnston, ‘Everything That Went Down At Malcolm Turnbull’s Encryption Law Announcement’ (Gizmodo AU 14 July 2017) <www.gizmodo.com.au/2017/07/everything-that-went-down-at-malcolm-turnbulls-encryption-law-announcement/>.

77 Joris van Hoboken and Wolfgang Schulz, *Human Rights and Encryption* (UNESCO 2016) 29.

78 Abelson and others (n 18) 18.

79 *ibid*, 11-12.

key escrow system, such as identifying who could be trusted to hold and secure the escrowed key in a key escrow system. Encryption-enabled device manufacturers and providers of E2E encrypted messaging services have also acknowledged they would not be able to ensure the security of encryption backdoors if they were forced to incorporate them into their products and services.⁸⁰ Due to these unresolved issues, there is minimal incentive for encryption technology providers to develop a key escrow system.

2.4 How often are encrypted data encountered by law enforcement agencies?

A significant hurdle to any meaningful analysis of the necessity of introducing MEBL is a lack of comprehensive and reliable information regarding how often LEAs are faced with data rendered unrecoverable by way of encryption.⁸¹ It is a futile exercise to attempt to calculate how often data rendered unrecoverable by encryption prevent a criminal investigation from proceeding, as there is no way to know if the unrecoverable data are incriminating and would lead to a prosecution or not. The next best statistic to support or discredit a case for MEBL is how often LEAs are unable to obtain decrypted data in circumstances where they have legal authority to obtain such data.

A 2015 report from Europol suggested more than 75% of cybercrime investigations in the EU ‘encountered the use of encryption to protect data and/or frustrate forensic analysis of seized media’.⁸² Further, an assessment conducted by the Council of the EU in 2016 suggested, based on the responses from 25 EU member states and Europol, ‘encryption is encountered often or almost always in the context of criminal investigations’.⁸³ Neither the Europol report nor the assessment by the Council of the EU distinguished between encountering encryption generally and encountering encrypted data that could not be decrypted. To suggest encryption is encountered often or almost always in the

80 Article 29 Data Protection Working Party (A29WP), ‘Statement of the WP29 on Encryption and Their [sic] Impact on the Protection of Individuals With Regard to the Processing of Their Personal Data in the EU’ (A29WP 11 April 2018) <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51026> 2.

81 Carter, Lewis and Zhang (n 10) iv.

82 Europol, *The Internet Organised Crime Threat Assessment (IOCTA 2015)* (Europol 2015) 50. Subsequent annual reports from Europol published between 2016 and 2019 have not included similar statistics regarding the frequency of encountering encryption.

83 Council of the European Union, ‘Encryption: Challenges for Criminal Justice in Relation to the Use of Encryption’ (23 November 2016) Council of the European Union document number 14711/16, 3, para 7. Emphasis in original. Five delegations stated they encountered encryption rarely in the context of criminal investigations.

context of criminal investigations is little more enlightening than suggesting smartphones and computers are frequently encountered in the context of criminal investigations. Frequent encounters with encryption is not a compelling argument in favour of MEBL being necessary, particularly in the absence of further information regarding whether the encountered encrypted data were eventually decrypted and how the encrypted data impacted the relevant criminal investigation. For example, was the encrypted data the only evidence available or otherwise likely to be critical to the investigation? Did the relevant LEA have legal authority to decrypt the data in the first place? Was a conviction obtained regardless of the issues regarding access to decrypted data?

The Director of the FBI, Christopher Wray, indicated the FBI was unable to obtain decrypted data from approximately 7,800 devices in the fiscal year ending on 30 September 2017, despite the FBI possessing a proper legal authority to do so.⁸⁴ Wray described this inability to access decrypted data as an ‘urgent public safety issue’,⁸⁵ but did not elaborate on why the alleged issue was urgent or how it threatened public safety. These figures, if accurate,⁸⁶ are a slightly more compelling argument in favour of MEBL being necessary than the European encounters with encryption, as the figures from Europe did not indicate whether the encountered encrypted data were unrecoverable, nor whether a legal authority to access the decrypted data existed. As the data on the alleged 7,800 devices held by the FBI were unrecoverable, one can only guess how useful, or useless, the decrypted data would be for the purposes of crime prevention or a criminal investigation.

It has been suggested that publicly available information regarding recent terrorist attacks indicate terrorists do not appear to rely on encryption to protect their operational communications, instead opting for burner phones, couriers or pre-arranged code words to evade surveillance.⁸⁷ If this is true, the introduction of encryption backdoors appears unlikely to assist with obtaining data to prevent and prosecute terrorist acts. Where criminals actively seek to use encryption to hide their activity, imposing encryption backdoors is unlikely to

84 Dustin Volz, ‘FBI Chief Calls Unbreakable Encryption ‘Urgent Public Safety Issue’ (Reuters 9 January 2018) <www.reuters.com/article/us-usa-cyber-fbi/fbi-chief-calls-unbreakable-encryption-urgent-public-safety-issue-idUSKBN1EY1S7>.

85 *ibid.*

86 An article in The Washington Post suggested the FBI exaggerated the number of devices from which decrypted data could not be obtained, with the correct number likely to be between 1,000 and 2,000. See Devlin Barrett, ‘FBI Repeatedly Overstated Encryption Threat Figures to Congress, Public’ (The Washington Post 23 May 2018) <www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html>.

87 Carter, Lewis and Zhang (n 10) iv.

be an effective measure against such criminals as they would continue to seek out or adapt the strongest available encryption to protect any incriminating data.⁸⁸ For example, criminals could seek out encryption technology that did not include encryption backdoors or apply ‘super encryption’ (by first applying a private, uncrackable encryption method to data, then encrypting the data a second time with a government approved encryption method).⁸⁹ Further, the UN Special Rapporteur on the promotion and the protection of the right to freedom of opinion and expression has noted governments proposing MEBL ‘have not demonstrated that criminal or terrorist use of encryption serves as an insuperable barrier to law enforcement objectives’.⁹⁰ On this basis, the argument in favour of MEBL being necessary appears to be weak or unproven at best.

2.5 What methods are available for investigating crimes where encrypted data are encountered?

Issuing an individual with a forced decryption instrument is an alternative to pursuing service providers to deliver decrypted data, particularly in circumstances where the service providers do not have the means to decrypt encrypted data. Where available to LEAs, forced decryption instruments can be issued to individuals to compel the provision of a password, a decryption key or decrypted data generally, with non-compliance punishable by imprisonment or financial penalties.⁹¹ However, forced decryption instruments can trigger legal protections against self-incrimination and put the targeted individual on notice that they are under investigation.⁹² In the 2008 case of *R v S and A* in the UK, two suspects charged with a failure to comply with a notice requiring the disclosure of the password or decryption keys to encrypted files sought to rely on the privilege against self-incrimination, provided by the UK’s common law and Article 6 of the ECHR.⁹³ The privilege against self-incrimination was held not to be engaged in the circumstances ‘on the basis that the material in question had a separate existence, independent of the minds of the appellants, and in any event, that the proposed incursion into the privilege against self-incrimination (if any) was legitimate and proportionate’.⁹⁴

88 A29WP (n 80) 2.

89 Koops and Kosta (n 71) 894.

90 UNGA, ‘Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye’ (22 May 2015) UN Doc A/HRC/29/32, 14-15, para 42.

91 For example, see Regulation of Investigatory Powers Act 2000 (UK), sections 49 and 53.

92 The privilege against self-incrimination is recognised in both US and European constitutional law. Koops and Kosta (n 71) 894.

93 *R v S and A* [2008] EWCA Crim 2177, para 9.

94 *ibid*, para 15.

The opposite approach was taken in a 2012 case in the USA regarding an order to produce the unencrypted content of several encrypted laptops and external hard drives.⁹⁵ Here the defendant successfully pleaded decryption and production of the content of the devices would trigger the protection against self-incrimination provided in the Fifth Amendment to the United States Constitution. This was on the basis that the defendant's act of decryption and production would constitute providing a testimony against himself and would therefore violate the Fifth Amendment. However, in a 2017 case in the USA, the Fifth Amendment was held not to apply in response to a decryption order due to the foregone conclusion exception to the Fifth Amendment.⁹⁶ Under this exception, the government can compel a person to produce an item where the government reasonably knows the requested item exists.⁹⁷ The foregone conclusion exception can be applied as follows in the context of an encrypted hard drive: 'The government can force a person to decrypt a hard drive because it always knows that an encrypted hard drive has a corresponding unencrypted version'.⁹⁸ This reflects the approach taken by the Third Circuit in the USA in 2017. The apparent state of flux and potentially contradictory application of legal protections against self-incrimination demonstrates the use of forced decryption instruments against individuals is not always effective for obtaining decrypted data.⁹⁹ An individual can always refuse to comply with a forced decryption instrument and this may be an individual's preferred option where the maximum punishment for failing to comply with the forced decryption instrument is less than the punishment for a crime that might be revealed by decrypted data.

Beyond attempts to force either a service provider or the user of encryption technology to provide decrypted data, LEAs have a range of other investigatory tools available to collect intelligible data for the purposes of criminal investigations. Some of the abilities available to LEAs to collect intelligible data have been identified by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism:

Most States now have the capacity to intercept and monitor calls made on a landline or mobile telephone, enabling an individual's location to be determined, his or her movements to be tracked through cell site analysis and his or her text messages to be read

95 *In re Grand Jury Subpoena Duces Tecum (Doe)*, 670 F.3d 1335 (11th Cir. 2012).

96 *United States v. Apple Macpro Computer*, No. 15-3537 (3rd Cir. 2017). For further analysis of the application of the foregone conclusion exception, see Dan Terzian, 'Forced Decryption as a Foregone Conclusion' (2015) 6 California Law Review Circuit 27.

97 Terzian, *ibid*.

98 *ibid*.

99 For additional examples of decryption orders clashing with the privilege against self-incrimination and a brief discussion of forced decryption instruments in the context of devices protected by biometrics, see Koops and Kosta (n 71) 895.

and recorded. Targeted surveillance also enables intelligence and law enforcement agencies to monitor the online activity of particular individuals, to penetrate databases and cloud facilities, and to capture the information stored on them. An increasing number of States are making use of malware systems that can be used to infiltrate an individual's computer or smartphone, to override its settings and to monitor its activity. Taken together, these forms of surveillance provide a mosaic of data from multiple sources that can generate valuable intelligence about particular individuals or organizations.¹⁰⁰

In addition to this array of abilities, the metadata associated with E2E encrypted communications is usually not encrypted because it needs to remain unencrypted for systems to operate.¹⁰¹ The large volume and accessibility of metadata provides LEAs with an alternative source of useful information to assist with investigations.¹⁰² Where available, metadata can reveal the location of individuals in real-time, the frequency of their communications and the times and dates of their communications. In a particularly interesting twist on the encryption backdoor concept, a controversial proposal has emerged to suggest LEAs should seek out and exploit existing security holes or backdoors in end-user software or platforms instead of pursuing MEBL.¹⁰³ Exploiting security vulnerabilities without notifying the relevant service providers poses several ethical, legal and policy questions, but it may be preferable to forcing encryption technology providers to add more complexity and potential insecurity to existing encryption technology by mandating the incorporation of encryption backdoors. Although the investigatory powers already available to LEAs may raise separate privacy concerns, they are less controversial and more proportionate than pursuing MEBL.¹⁰⁴

¹⁰⁰ UNGA (n 61).

¹⁰¹ Zittrain and others (n 4) 3.

¹⁰² Ian Walden, "The Sky is Falling!" – Responses to the "Going Dark" Problem' (2018) 34 Computer Law and Security Review 901, 906.

¹⁰³ Steven M. Bellovin and others, 'Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet' (2014) 12(1) Northwestern Journal of Technology and Intellectual Property 1, 5.

¹⁰⁴ A29WP (n 80) 3.

3 Encryption regulation

This section provides a brief history of encryption regulation to put the current encryption debate in context. This is followed by an analysis of some proposals that could amount to MEBL to determine the potential effectiveness of such legislation in providing LEAs with decrypted data. By requiring encryption technology providers to be able to provide decrypted data on request, the development and incorporation of encryption backdoors appears to be the only option available for encryption technology providers to ensure they can comply with such requests.

3.1 A brief history of encryption regulation

Despite the long history of cryptography, dating back to Ancient Egypt and the use of hieroglyphs,¹⁰⁵ it was not until the beginning of the Cold War that encryption came to be regulated on a major scale, with the USA pioneering the regulation efforts.¹⁰⁶ Seeking to protect encryption technology from falling into the hands of foreign powers and potential enemies, the USA imposed export controls to limit the strength of the encryption methods that could be legally distributed beyond the USA.¹⁰⁷ This led to conflict regarding the ability of US-based technology companies to export products incorporating strong encryption and the freedom of American academics to publish research addressing cryptography.¹⁰⁸ This conflict marked the start of the ‘Crypto Wars’.¹⁰⁹ A combination of technology breakthroughs in cryptosystems, specifically the production of the Data Encryption Standard (DES) and the Rivest-Shamir-Aldeman algorithm (RSA), and new communication technologies, such as the fax machine and the Internet, eventually pushed encryption beyond government and military usage

105 David Kahn, *The Codebreakers: The Story of Secret Writing* (Scribner 1996) 71.

106 Nathan Saper, ‘International Cryptography Regulation and the Global Information Economy’ (2013) 11(7) *Northwestern Journal of Technology and Intellectual Property* 673, 677. For definitions and further explanation of the difference between cryptology, cryptography and cryptanalysis, see Koops (n 32) 35 and Kahn, *ibid*, xv-xviii.

107 Access Now, ‘Encryption in the U.S.: Crypto Colloquium Outcomes Report’ (*Access Now* January 2018) <www.accessnow.org/cms/assets/uploads/2018/02/Encryption-in-the-United-States-Crypto-Colloquium-Outcomes-Report.pdf> 9.

108 Abelson and others (n 18) 8.

109 *ibid*.

into the hands of the public.¹¹⁰ This led to extensive debates about the ability of the government to access and decrypt encrypted data.¹¹¹

As advanced encryption methods became available to the public and more common in communication technology, encryption increased the personal privacy of individuals while simultaneously reducing the ability of LEAs to intercept telephone calls, read electronic messages and decrypt the hard disks of electronic devices.¹¹² According to Froomkin, the fear of losing these traditional methods of conducting surveillance resulted in a three-pronged reaction from the law enforcement and intelligence communities in the USA.¹¹³ The first prong was a public relations offensive to explain the importance of electronic surveillance capabilities, the second prong involved seeking legislation to require communication technologies be designed in a way that facilitated wiretapping and the third prong was to design and support a new encryption standard, the Escrowed Encryption Standard (EES).¹¹⁴ EES was to be implemented in a device known as the Clipper Chip, which would enable the USG to keep a copy of the decryption key for all communications encrypted using EES.¹¹⁵ The push for a key escrow system was ultimately abandoned in 2000 due to a combination of pressure from industry during the 'dotcom' boom and political resistance, including resistance from the EU.¹¹⁶

The development and deployment of E2E encrypted IM applications and encryption-enabled devices by the technology industry since the Snowden revelations, and the subsequent uptake of that technology by the public, has led to a new battle over access to data, nicknamed 'Crypto Wars 2.0'.¹¹⁷ Although the issues in version 2.0 of the Crypto Wars are essentially the same as those in the original 'conflict', encryption is now deeply embedded in various aspects of everyday life, including browsing the Internet, communicating electronically and online commerce. Accordingly, any legislation that impacts encryption technology is likely to affect a much greater number of people and services than the legislative efforts in the 1990s.

110 David McClure, 'First Amendment Freedoms and the Encryption Export Battle: Deciphering the Importance of *Bernstein v. United States Department of Justice*, 176 F.3d 1132 (9th Cir. 1999)' (2000) 79(2) *Nebraska Law Review* 465, 467.

111 Zittrain and others (n 4) 5.

112 Froomkin (n 71) 715.

113 *ibid.*, 743.

114 *ibid.*

115 *ibid.* See pages 752-764 for an explanation of how the Clipper Chip was intended to work.

116 Abelson and others (n 18) 5.

117 *The Economist*, 'Crypto Wars 2.0' (*The Economist* 8 November 2014) <www.economist.com/business/2014/11/08/crypto-wars-20>.

3.2 Regulating access to encrypted data

Arguably the most important consideration in proposing MEBL is whether encryption backdoors are technically possible, and if so, whether they can be kept secure. On this point, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has previously noted:

It is a seemingly universal position among technologists that there is no special access that can be made available only to government authorities, even ones that, in principle, have the public interest in mind. In the contemporary technological environment, intentionally compromising encryption, even for arguably legitimate purposes, weakens everyone's security online.¹¹⁸

Despite the technological and procedural difficulties associated with creating a secure encryption backdoor, the introduction of MEBL remains one of the most widely discussed and controversial measures for addressing the 'going dark' problem.¹¹⁹ However, only a few countries appear to have made serious efforts to develop and implement encryption backdoors,¹²⁰ while other countries have sought to impose limits on the strength of the encryption available to the public, imposed a requirement to obtain government approval prior to using encryption or required suppliers of encryption technology to provide copies of decryption keys to the government before providing their technology to the public.¹²¹

In recent years, draft legislation targeting encryption-enabled devices has emerged in at least two states in the USA and in France. More broadly targeted draft legislation has also emerged in the USA, seeking the incorporation of encryption backdoors into all encryption-enabled devices, operating systems and IM applications.¹²² The UK's Investigatory Powers Act of 2016 (IPA), in force since November 2016, has the potential to be used to require targeted entities to incorporate an encryption backdoor into their encryption technology. Similarly, Australia's Telecommunications Act, as amended by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act (AA Act) in December 2018, has been criticised for its potential to be used to pursue encryption backdoors. The remainder of this section is dedicated to analysing

118 UNGA (n 90) 4, para 8.

119 Global Partners Digital (n 28) 31-32.

120 For example, the Clipper Chip in the USA and the National Security Certificate in Kazakhstan. See *ibid*, 31-32.

121 UNGA (n 90) 14, para 41.

122 Richard Burr and Diane Feinstein, 'Compliance with Court Orders Act 2016: Discussion Draft' (13 April 2016) <www.burr.senate.gov/imo/media/doc/BAG16460.pdf>.

these recent legislative efforts to determine if they could be effective in providing LEAs with decrypted data.

3.3 Device backdoors

Two examples of proposed legislation targeting encryption-enabled smartphones have emerged at state level in the USA, specifically in New York State and California. In the previously cited CSIS report it was suggested that device encryption on mobile devices is likely to pose more of a problem for LEAs in the USA in comparison to other countries, based on the report's estimates that 47% of all mobile devices in the USA have full disk encryption, compared to a global average of 21%.¹²³ This might explain the appetite of legislators in New York State and California to target encryption-enabled smartphones, as opposed to targeting encryption technology providers more generally. Draft legislation targeting equipment manufacturers has also emerged at the national level in France.

3.3.1 New York State Assembly Bill No. A08093

Bill No. A08093, introduced to the New York State Assembly in June 2015, sought to impose a requirement that any smartphone manufactured on or after 1 January 2017 that was sold or leased in New York State be 'capable of being decrypted and unlocked by its manufacturer or its operating system provider'.¹²⁴ With some limited exceptions, the seller or lessor of a non-compliant smartphone in New York State would be liable to a civil penalty for each infringing device sold or leased.¹²⁵ Although the bill did not directly target providers of encryption technology, if enacted, it could pressure the manufacturers and operating system providers of smartphones to incorporate an encryption backdoor into their respective devices and operating systems to ensure ongoing sales and leases in New York State. If manufacturers and operating system providers did bow to the pressure to ensure smartphones could be decrypted and unlocked, non-compliant smartphones manufactured before 1 January 2017 would still be available for sale or lease in New York State without subjecting the seller or lessor to any potential liability. In addition, individuals would be free to source non-compliant devices from outside New York State without any consequences. Accordingly, if enacted, the effectiveness of this bill in ensuring LEAs can obtain decrypted would be doubtful. Anyone seeking to obtain a non-compliant smart-

¹²³ Carter, Lewis and Zhang (n 10) 9. The figures provided should be treated with caution, as noted in section 1.1.

¹²⁴ New York State Assembly, 'A08093 Summary' <https://assembly.state.ny.us/leg/?default_fld=&bn=A08093&term=2015&Summary=Y&Actions=Y&Votes=Y&Memo=Y&Text=Y> section 2.

¹²⁵ *ibid*, section 3.

phone may not be able to purchase it in New York State from a law-abiding retail store, but non-compliant devices would still be available from out of state and the inability of LEAs to obtain decrypted data would persist. The bill appears to have stalled and has been noted as ‘held for consideration in consumer affairs and protection’ since 24 May 2016.¹²⁶ No evidence could be found to suggest the bill or similar legislation is likely to be pursued in New York State.

3.3.2 California State Assembly Bill No. 1681

California State Assembly Bill No. 1681, introduced to the California State Assembly in January 2016, targeted any smartphone sold or leased in California on or after 1 January 2017 and would subject a manufacturer or operating system provider of any such smartphone to a civil penalty ‘for each instance in which the manufacturer or operating system provider of the smartphone is unable to decrypt the contents of the smartphone pursuant to a state court order’.¹²⁷ The proposed legislation indicated a desire to shift the onus to comply with requests to provide decrypted data away from individual owners and users of smartphones and onto device manufacturers and operating system providers. This is an understandable move, noting the current state of flux regarding forced decryption orders in the USA and the application of the right against self-incrimination provided by the Fifth Amendment.¹²⁸ Pursuing a third party to provide decrypted data, rather than the owner or user of an encrypted device, removes any issues associated with legal protections against self-incrimination.

By directly targeting the manufacturers and operating system providers of smartphones and threatening a civil penalty for non-compliance, the California bill would be more likely to prompt action from the manufacturers and operating system providers of smartphones than the bill from New York State. However, the relatively low civil penalty proposed for each instance of non-compliance, being US\$2,500, may not be a sufficient incentive for a large technology company to produce a separate compliant device or operating system just for use by residents of California.¹²⁹ In addition, the limited geographic scope of the legislation would allow California residents to obtain a non-compliant smartphone from outside California and the manufacturers and operating system providers of externally sourced smartphones would not be subject to any decryption obligations or penalties for non-compliance. As the proposed finan-

¹²⁶ *ibid*, see ‘Actions’ section.

¹²⁷ California Legislative Assembly, ‘Assembly Bill No. 1681’ (Introduced by Assembly Member Cooper on 20 January 2016, amended in Assembly on 8 March 2016 and 28 March 2016) <https://leginfo.ca.gov/faces/billPdf.xhtml?bill_id=201520160AB1681&version=20150AB168197AMD> section 2(b).

¹²⁸ See section 2.5 of this paper for further discussion of the application of the Fifth Amendment.

¹²⁹ California Legislative Assembly (n 127).

cial penalty would only apply to smartphone manufacturers and operating system providers, there would be no incentive for retailers to stop selling non-compliant smartphones. Like the bill from New York State, if the bill from California were enacted, its effectiveness in ensuring LEAs have access to decrypted data would be doubtful. The bill is currently listed on the California Legislative Assembly website as ‘Inactive Bill – Died’.¹³⁰ No evidence could be found to suggest the bill or similar legislation is likely to be pursued in California. However, if the bill or similar legislation was pursued, a strong response from the local technology industry could be expected, noting California is the home of several pro-encryption market leaders in smartphone technology, including Apple and Google.¹³¹

3.3.3 French proposals

A report published by New America in July 2017 identified several attempts by French lawmakers to make amendments to the Digital Republic Act and the Organised Crime and Terrorism Act regarding encryption technology.¹³² Some of these amendments would have allegedly amounted to a backdoor mandate, requiring providers of encryption technology to also hold the decryption key for any encryption technology they offer.¹³³ An example of a proposal that could have amounted to mandating an encryption backdoor for devices was presented to the French National Assembly in January 2016. The amendment was proposed to the bill that would eventually become the Digital Republic Act and stipulated ‘[m]anufacturers of equipment must take into account in their design the need to give law enforcement authorities, in the context of a judicial inquiry and after the authorization of a judge, access to the requested materials’.¹³⁴ The proposal also sought to authorise the Council of State (Conseil d’État) to set detailed rules for the implementation of the requirement.¹³⁵ The proposed amendment was vague and was rejected shortly after its introduction to the National Assembly.¹³⁶ The ambiguity of the proposed amendment does not allow a meaningful analysis of its potential effectiveness to ensure LEAs can obtain

130 California Legislative Information ‘Status: AB-1681 Smartphones (2015–2016)’ <https://leginfo.ca.gov/faces/billStatusClient.xhtml?bill_id=201520160AB1681>.

131 Apple and Google both openly advocate the use of encryption in their technology. See Apple (n 9) and Google, ‘Online Security & Protection’ <<https://safety.google/security/>>.

132 See Bhairav Acharya and others, ‘Deciphering the European Encryption Debate: France’ (*New America* August 2017) <https://d1y8sb8igg2f8e.cloudfront.net/documents/France_Paper_8_8.pdf> 6–10.

133 *ibid.*, 6.

134 *ibid.* The original French text of the proposed amendment is available at Assemblée nationale, ‘République Numérique (No 3318) – Amendement No CL92’ (*Assemblée nationale* 4 January 2016) <www.assemblee-nationale.fr/14/amendements/3318/CIION_LOIS/CL92.pdf>.

135 Acharya and others (n 132).

136 *ibid.*, 7.

decrypted data to be conducted, beyond noting individuals would be free to source non-compliant equipment from outside France without penalty if they wanted to continue to utilise strong encryption to protect their privacy. No evidence could be found to suggest similar amendments are likely to be pursued in France in the immediate future.

3.4 A backdoor for all encryption

The Burr-Feinstein bill, drafted with a working title of the ‘Compliance with Court Orders Act 2016’, takes its name from the two USG Senators who co-authored the bill, Senators Richard Burr (Republican) and Dianne Feinstein (Democrat).¹³⁷ Despite the bill having bipartisan support, it never developed past the point of a discussion draft and was never introduced to Congress.¹³⁸ The key legal obligation of the bill is set out in section 3 and requires:

a covered entity that receives a court order from a government for information or data shall-

(A) provide such information or data to such government in an intelligible format; or

(B) provide such technical assistance as is necessary to obtain such information or data in an intelligible format or to achieve the purpose of the court order.¹³⁹

A covered entity is defined broadly in the bill as ‘a device manufacturer, a software manufacturer, an electronic communication service, a remote computing service, a provider of wire or electronic communication service, a provider of a remote computing service, or any person who provides a product or method to facilitate a communication or the processing or storage of data’.¹⁴⁰ On receipt of a court order, a covered entity would be ‘responsible only for providing data in an intelligible format if such data has been made unintelligible by a feature, product, or service owned, controlled, created, or provided, by the covered entity or by a third party on behalf of the covered entity’.¹⁴¹

The bill refers to the provision of technical assistance as is *necessary* to obtain data in an intelligible format, as opposed to the provision of *reasonable* assistance. This would require covered entities to assist beyond what is deemed rea-

137 Burr and Feinstein (n 122).

138 Patrick Howell O’Neill, ‘Sen. Dianne Feinstein Wants to Bring Back Bill That Bans Strong Encryption’ (Cyberscoop 10 November 2017) <www.cyberscoop.com/dianne-feinstein-encryption-bill-fbi-apple/>.

139 Burr and Feinstein (n 122) section 3(a)(1).

140 *ibid*, section 4(4).

141 *ibid*, section 3(a)(2).

sonable and fails to consider the technical challenges that covered entities might face in attempting to provide data in an intelligible format.¹⁴² If the targeted data were E2E encrypted, a covered entity would not be able to comply with the court order unless an encryption backdoor was incorporated into the applicable encryption technology. If an encryption backdoor was included in an encrypted IM application, it would not be accurate to describe the application as truly E2E encrypted, as the encryption backdoor would introduce the possibility for a third party to view transmitted data in plaintext. Accordingly, if enacted, the bill would effectively prohibit true E2E encrypted communications.

The bill omitted any details regarding consequences for failing to comply with a court order to supply information or data, so it is unclear if civil or criminal penalties were intended for non-compliance. If the bill were enacted and covered entities took technical steps to ensure they could comply with its terms, perhaps in fear of severe penalties, this would have wide-ranging repercussions for commercially available encryption technology. Given the wide definition of covered entity and noting the bill was proposed at a federal level, the bill has potential to be effective in ensuring LEAs throughout the USA have access to decrypted data. However, individuals would still be able to obtain non-compliant devices and software from outside the USA if they wanted to continue to utilise strong encryption to conceal data from third parties.

In May 2016 Reuters reported the support from legislators in the USA to require technology companies to provide encryption backdoors was ‘gone’ and the push for associated legislation was ‘dead’, based on information from sources in the Obama administration, congressional offices and the technology sector.¹⁴³ However, in late 2017, Senator Feinstein indicated it was time to revisit the Burr-Feinstein bill.¹⁴⁴ Further, a renewed interest in regulating encryption technology at a federal level in the USA has recently been demonstrated by the introduction to Congress of the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (EARN IT Act). Although the EARN IT Act appears to be generally focussed on reducing the sharing of child sexual exploitation material, it would have significant implications for companies who offer E2E encrypted services if it were passed into law in the form it was submitted to Congress in

142 Rob Price, ‘Here’s How the US Government Plans to Break the Encryption on Your Smartphone’ (*Business Insider* 8 April 2016) <<https://www.businessinsider.in/Here-how-the-US-government-plans-to-break-the-encryption-on-your-smartphone/articleshow/51742351.cms>>.

143 Dustin Volz, Mark Hosenball and Joseph Menn, ‘Push for Encryption Law Falters Despite Apple Case Spotlight’ (*Reuters* 27 May 2016) <www.reuters.com/article/usa-encryption-legislation-idUSL2N18O0BM>.

144 O’Neill (n 138).

March 2020.¹⁴⁵ Following the elections in the USA in November 2020, it is not yet clear how the Biden administration and new look Congress will pursue the EARN IT Act or any other legislation that seeks to limit how encryption technology is currently used.

3.5 Investigatory Powers Act 2016 (UK)

The IPA received royal assent on 29 November 2016 and authorises various investigatory powers for UK LEAs, such as interception of communications, interference with communication equipment and the acquisition of communication data.¹⁴⁶ The initial bill that eventually became the IPA drew criticism from Facebook, Google, Microsoft, Twitter and Yahoo for its lack of clarity regarding potential obligations regarding encryption technology. These companies suggested the bill should have expressly stated that nothing in it ‘should be construed to require a company to weaken or defeat its security measures’.¹⁴⁷ No such statement was included in the IPA as enacted, leaving the potential implications of the IPA on encryption technology open for interpretation. The IPA is in force and does not on its face require providers of encryption technology to incorporate encryption backdoors. However, there is a complicated path available under the IPA that could be followed to impose mandatory encryption backdoors.

Section 253 of the IPA enables the government, via the Secretary of State (SoS) and with the approval of a Judicial Commissioner (JC), to issue a relevant operator with a technical capability notice requiring the operator to, among other things, remove ‘electronic protection applied by or on behalf of that operator to any communications or data’.¹⁴⁸ In issuing a technical capability notice, the SoS must consider the notice is ‘necessary for securing that the operator has the capability’ to provide assistance and also ‘that the conduct required by the notice is proportionate to what is sought to be achieved by that conduct’.¹⁴⁹ The definition of relevant operator includes a telecommunications operator, which is defined as a person who offers or provides a telecommunications service to per-

145 Lily Hay Newman, ‘The EARN IT Act Is a Sneak Attack on Encryption’ (*Wired* 5 March 2020) <<https://www.wired.com/story/earn-it-act-sneak-attack-on-encryption/>>. Due to time and space constraints, it was not possible to go into further detail in this paper about the specific implications of the EARN IT Act on encryption technology in the USA.

146 IPA, introductory text.

147 Facebook and others, ‘Written Evidence (IPB0116)’ (21 December 2015) <<http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26367.html>>.

148 IPA, section 253(5)(c).

149 *ibid*, section 253(1)(b).

sons in the UK, or controls or provides a telecommunications system which is in the UK or controlled from the UK.¹⁵⁰ The definition of a telecommunications operator has a wide scope and, according to a Code of Practice issued by the UK Home Office (UKHO), it includes Internet-based services such as web-based email, IM applications and cloud-based services, together with application and website providers (to the extent they are providing a telecommunications service).¹⁵¹ Telecommunications operators may also include anyone who provides services where customers, guests or members of the public are provided with access to communications services (for example, free WiFi), such as hotels, airport lounges and public transport operators.¹⁵² The IPA allows technical capability notices to be issued to operators located outside the UK.¹⁵³

Providers of E2E encrypted IM applications fall within the definition of a telecommunications operator under the IPA, based on the UKHO's Code of Practice, and can be issued with a technical capability notice requiring them to remove electronic protection applied by or on their behalf. This raises questions about who applies encryption to E2E encrypted data. When a user of an E2E encrypted IM application sends a message from a device, it is not clear whether the encryption would be deemed to be applied by the IM application provider, the provider of the device's operating system, the device manufacturer or by the user.¹⁵⁴ If the encryption was deemed to be applied by an entity falling outside the definition of a relevant operator, such as the user of an application, a technical capability notice would not be able to be used to remove the protection offered by the encryption.

Further complicating the path towards imposing mandatory encryption backdoors under the IPA, in issuing a technical capability notice requiring the removal of electronic protection the SoS 'must in particular take into account the technical feasibility, and likely cost, of complying with those obligations'.¹⁵⁵ Accordingly, the SoS would need to be convinced that it is both technically feasible and cost effective for encryption to be removed from encrypted data before issuing a technical capability notice to a relevant operator seeking the removal of the protection offered by encryption. It would not be technically feasible for an operator who provides an E2E encrypted IM application to remove the

150 *ibid*, sections 253(3)(b) and 261(10).

151 UKHO, *Equipment Interference Code of Practice* (UKHO March 2018) 9, paras 2.12 and 2.13.

152 *ibid*, para 2.14.

153 IPA, section 253(8).

154 Graham Smith, 'Investigatory Powers Act: Back Doors, Black Boxes, and Tech Capability Regs' (*Ars Technica* 8 May 2017) <<https://arstechnica.com/tech-policy/2017/05/investigatory-powers-act-legal-analysis/?comments=1>>.

155 IPA, section 255(4).

encryption on the basis the operator does not have, and cannot obtain, the decryption key.¹⁵⁶ It is unclear if the requirement to consider the likely costs of removing electronic protection refers to the likely costs for the UK government, the relevant operator, or both. The SoS is also obliged to ensure operators receive an appropriate contribution for the costs incurred, or likely to be incurred, in complying with the IPA, as considered appropriate by the SoS.¹⁵⁷ In theory, this could extend to paying operators for the costs associated with amending their encryption technology to incorporate an encryption backdoor.

In the Investigatory Powers (Technical Capability) Regulations 2018, published in March 2018, the SoS set out the obligations deemed reasonable to impose on relevant operators via technical capability notices. In relation to obligations imposed by a technical capability notice on telecommunications operators to remove electronic protection, the Regulations specify telecommunications operators would be required to provide and maintain the capability to remove electronic protection ‘where reasonably practicable’.¹⁵⁸ According to the UKHO’s Code of Practice, ‘[a] decision regarding what is reasonably practicable will depend on the particular circumstances of the case, recognising that what is reasonably practicable for one telecommunications operator may not be for another’.¹⁵⁹ Whether the UK courts would deem it reasonably practicable to require an encryption technology provider to incorporate an encryption backdoor into encryption technology is untested, however, UK courts have interpreted ‘reasonably practicable’ to have a narrower meaning than simply being physically possible.¹⁶⁰ The physical possibility of incorporating an encryption backdoor into encryption technology will therefore not be enough to satisfy the requirement to be reasonably practicable.

If the SoS decides, after making all of the relevant considerations regarding necessity, proportionality and reasonable practicability, it is appropriate to issue a technical capability notice, the notice must be approved by a JC.¹⁶¹ In deciding whether to give this approval, a JC must review the SoS’ conclusions as to the necessity of issuing the notice and whether the conduct sought is proportionate to the aim sought by that conduct.¹⁶² The JC’s review must also consider a list of general duties in relation to privacy articulated in section 2 of the IPA. Noting

156 Smith (n 154).

157 IPA, sections 249(1) and (2).

158 See Investigatory Powers (Technical Capability) Regulations 2018 Schedule 1 Part 1 8(b), Schedule 2 Part 1 9(b) and Schedule 3 6(b).

159 UKHO (n 151) 93, para 8.7.

160 *Edwards v National Coal Board* [1949] KB 704.

161 IPA, section 253(1)(c).

162 *ibid*, section 254(2).

the various definition and interpretation hurdles to be considered when issuing a technical capability notice and the veto power afforded to JCs, the SoS can expect a complicated path, featuring legal challenges, if they seek to force an entity to remove the protection offered by encryption via a technical capability notice. If this path could be successfully navigated, the requirement to issue a separate technical capability notice to each relevant operator could restrict the effectiveness of the IPA to ensure LEAs can obtain decrypted data. In addition, attempting to enforce technical capability notices against operators based outside the UK could introduce jurisdictional issues.

3.6 Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)

The AA Act received royal assent on 9 December 2018 and amended numerous Australian laws ‘to introduce measures to better deal with the challenges posed by ubiquitous encryption’.¹⁶³ The content and timing of the initial bill (AA Bill) that would later become the AA Act was broadly criticised by technology companies, civil liberties organisations and privacy advocates, with over 100 submissions received as part of a review process of the bill conducted by the Parliamentary Joint Committee on Intelligence and Security (PJCIS).¹⁶⁴ The PJCIS review of the AA Bill was cut short following intervention by the Australian Home Affairs Minister, Peter Dutton, on the basis that Australian LEAs required additional investigatory powers before the Christmas break.¹⁶⁵ Shortly after this intervention, the AA Act passed through the Australian Parliament on the last parliamentary sitting day of 2018.¹⁶⁶ The changes introduced via the AA Act do not compel providers of encryption technology to incorporate encryption backdoors into their technology, but the changes introduce a framework to allow Australian LEAs to request or compel industry assistance to remove electronic protection. However, section 317ZG of the Telecommunications Act, introduced via the AA Act, explicitly states that providers ‘must not be requested or required

163 The Parliament of the Commonwealth of Australia Senate, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 Revised Explanatory Memorandum* (6 December 2018) 2, para 1.

164 For a list of submissions received by the PJCIS, see Appendix A of Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Commonwealth of Australia December 2018).

165 Ariel Bogle, ‘Encryption Laws Developed After Little Consultation with Australian Tech Companies’ (ABC News 9 July 2019) <www.abc.net.au/news/science/2019-07-10/dutton-encryption-laws-australian-tech-sector-not-consulted-foi/11283864>.

166 *ibid.*

to implement or build a systemic weakness or systemic vulnerability' into a form of electronic protection.¹⁶⁷

Of particular relevance to encryption technology, the AA Act amended the Telecommunications Act to include a new Part 15 regarding industry assistance.¹⁶⁸ The new Part 15 authorises the issuing of technical assistance requests, technical assistance notices and technical capability notices to designated communications providers in certain circumstances, requesting or requiring the providers to do certain acts or things. The acts or things envisaged by these instruments include the removal of one or more forms of electronic protection (which includes encryption) that are or were applied by, or on behalf of, the provider.¹⁶⁹ The term designated communications providers is very broadly defined and is intended to include 'the full range of participants in the global communications supply chain, from carriers to over-the-top messaging providers'.¹⁷⁰ Almost any entity or individual that provides communications services or systems to a person located in Australia, regardless of the geographic location of that provider, appears to be captured by the definition of designated communications providers.¹⁷¹ Accordingly, technical assistance requests, technical assistance notices and technical capability notices can be issued beyond the borders of Australia.

A technical assistance request can be issued by a Director-General of a specified government agency or the chief officer of an interception agency to request a designated communications provider 'to do acts or things on a voluntary basis that are directed towards ensuring that the provider is capable of giving certain types of help'.¹⁷² Compliance with a technical assistance request is voluntary and providers are immune from civil liability for anything done in accordance with such a request.¹⁷³ A technical assistance notice can be issued by the Director General of Security or the chief officer of an interception agency to require (as opposed to request) a designated communications provider 'to do acts or things by way of giving certain types of help'.¹⁷⁴ A technical capability notice is more onerous than a technical assistance request or a technical assistance notice and can only be issued by the Attorney-General, representing the highest level of the

167 Telecommunications Act 1997 (Cth), section 317ZG.

168 AA Act Schedule 1.

169 Telecommunications Act 1997 (Cth), sections 317E and 317B.

170 The Parliament of the Commonwealth of Australia Senate (n 163) 39, para 208.

171 Australian Privacy Foundation, 'International Implications of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018' (*Australian Privacy Foundation* 4 June 2019) <https://privacy.org.au/wp-content/uploads/2020/05/APF_AAAct_FINAL_040619.pdf> 11.

172 Telecommunications Act 1997 (Cth), sections 317A and 317G(1)(a).

173 *ibid*, section 317G.

174 *ibid*, sections 317A and 317L.

Australian executive.¹⁷⁵ The Attorney-General can only issue a technical capability notice after being requested to do so by the Director-General of Security or the chief officer of an interception agency and the giving of the technical capability notice must be approved by the Minister for Communications.¹⁷⁶ This notice can be used to require a designated communications provider to ‘do acts or things directed towards ensuring that the provider is capable of giving certain types of help’.¹⁷⁷ Failure to comply with a technical assistance notice or a technical capability notice can attract civil penalties of over 10 million Australian dollars.¹⁷⁸

The authorisation to issue a technical assistance request, technical assistance notice or a technical capability notice involves limited judicial oversight as there is no requirement to seek the independent review or approval of a judge before issuing such a request or notice.¹⁷⁹ However, the instruments generally cannot be used to request or require a designated communications provider to do an act or thing that would otherwise require a warrant.¹⁸⁰ With limited exceptions, recipients of these instruments are bound by non-disclosure obligations and could face up to five years imprisonment if they disclose information regarding the existence, receipt, or content of such a request or notice.¹⁸¹

A technical assistance request, technical assistance notice or technical capability notice can only be issued if the person issuing the instrument is satisfied that certain decision-making criteria have been satisfied. A common element of the decision-making criteria for each of these instruments is a requirement for the issuer to be satisfied that the request or the requirement is reasonable and proportionate and that compliance with the request or requirement is practical and technically feasible.¹⁸² In considering whether a request or requirement is reasonable and proportionate, the relevant decision makers are required to have regard to certain matters, including: the interests of national security; the interests of law enforcement; the availability of other means to achieve the objectives; whether the request or requirement, when compared to forms of known industry assistance, is the least intrusive form of industry assistance; necessity; and the legitimate expectations of the Australian community regarding privacy and

175 The Parliament of the Commonwealth of Australia Senate (n 163) 12, para 56.

176 Telecommunications Act 1997 (Cth), section 317TAAA(1).

177 *ibid*, sections 317A and 317T.

178 *ibid*, section 317ZB(1).

179 Australian Privacy Foundation (n 171) 2.

180 Telecommunications Act 1997 (Cth), section 317ZH

181 *ibid*, section 317ZF

182 *ibid*, sections 317JAA, 317P and 317V.

cybersecurity.¹⁸³ The Telecommunications Act does not provide guidance regarding the process for determining whether a request or requirement is practical or feasible. However, an explanatory memorandum for the AA Bill notes that ‘if a decision-maker cannot be satisfied that it is technically feasible to remove a form of electronic protection due to the technical aspects of how that electronic protection is deployed, the decision-maker could not issue a notice containing such a requirement’.¹⁸⁴

Beyond meeting the thresholds of reasonableness, proportionality, practicality and feasibility, there is a prohibition in section 317ZG of the Telecommunications Act against requesting or requiring a designated communications provider to implement or build a systemic weakness or systemic vulnerability into a form of electronic protection.¹⁸⁵ Systemic weaknesses and vulnerabilities are defined in the Telecommunications Act as a vulnerability or a weakness ‘that affects a whole class of technology’, but the definition does not include a vulnerability or weakness ‘that is selectively introduced to one or more target technologies that are connected with a particular person’ (regardless of whether the person can be identified).¹⁸⁶ According to an explanatory memorandum issued in relation to the AA Bill, the restrictions on requesting or requiring a designated communications provider to implement or build a systemic weakness or systemic vulnerability ‘do not prevent the building of a capability that is able to be deployed selectively to weaken the electronic protection of a particular service, device or item of software’.¹⁸⁷ The explanatory memorandum also notes that a notice will be prohibited if it includes requirements to make a whole set of items within a class of technology, such as mobile operating systems or mobile devices, more vulnerable.¹⁸⁸

Any attempt by an Australian LEA to pursue broad encryption backdoors in relation to an entire E2E encrypted IM application or encryption-enabled devices would be prohibited by section 317ZG of the Telecommunications Act. Based on the discussion of encryption backdoors in section 2.3 of this paper, it would be very difficult, if not technically impossible, to pursue an encryption backdoor that could be selectively introduced to remove the encryption applied by an E2E encrypted IM application or encryption-enabled device in connection with a particular person without introducing a systemic weakness or systemic vulnerability. Due to the requirements to meet certain decision-making

183 *ibid*, sections 317JC, 317RA and 317ZAA.

184 The Parliament of the Commonwealth of Australia Senate (n 163) 68–69, para 393.

185 Telecommunications Act 1997 (Cth), section 317ZG.

186 *ibid*, section 317B.

187 The Parliament of the Commonwealth of Australia Senate (n 163) 13, para 58.

188 *ibid*, 36–37, para 206.

criteria and the prohibition against requesting or requiring the implementation or building of a systemic weakness or systemic vulnerability, Australian LEAs are in a similar position to their British counterparts working within the scope of the IPA when pursuing access to decrypted data. Seeking to encourage or force a designated communications provider to remove the protection offered by encryption is likely to be a complicated and lengthy process, potentially leading to a legal challenge by the designated communications provider regarding the technical feasibility of the measure being pursued or a dispute regarding the concept of systemic weaknesses and systemic vulnerabilities. If these issues could be successfully managed, the ability of Australian LEAs to obtain decrypted data would be severely restricted by the requirement to issue a request or notice to each relevant designated communications provider. Noting the number and geographic spread of the entities providing encryption technology to Australians, Australian LEAs will also face jurisdictional difficulties in seeking to enforce technical assistance notices and technical capability notices against foreign entities.

3.7 Anti-backdoor pressure from the EU

There is currently no EU-level legislation requiring technology companies to disclose decryption keys to LEAs or to decrypt data at the request of a member state government.¹⁸⁹ Instead, electronic surveillance conducted by national LEAs in criminal investigations and the cooperation of communication service providers to allow access to communications is regulated at the member state level in the EU.¹⁹⁰ Although the governments of France, Germany and the UK have all indicated an intent to introduce MEBL, there has generally been an anti-backdoor stance within various organs of the EU that has potential to persuade member states against pursuing MEBL.

The European Parliament's Committee on the Internal Market and Consumer Protection (IMCO) issued an opinion in September 2017 suggesting amendments to the proposed Electronic Communications Code to specifically address E2E encryption and encryption backdoors. The amendments proposed a new recital be added to the Electronic Communications Code as follows:

¹⁸⁹ The Law Library of Congress, 'Government Access to Encrypted Communications' (*The Law Library of Congress, Global Research Center* May 2016) <www.loc.gov/law/help/encrypted-communications/gov-access.pdf>, 2. Although this report was published in May 2016, its conclusions regarding the absence of EU legislation imposing decryption key disclosure or decryption requirements on technology companies appear to be accurate as at April 2021.

¹⁹⁰ *ibid*, 27 and Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) 2012 OJ C 326/47, Article 4(2)(j).

In order to safeguard the security and integrity of networks and services, the use of end-to-end encryption should be promoted and, where necessary, be mandatory in accordance with the principles of security and privacy by design; in particular, Member States should not impose any obligation to encryption providers, providers of electronic communications services and all other organisations (at all levels of the supply chain) that would result in the weakening of the security of their networks and services, such as the allowing or facilitation of ‘backdoors’.¹⁹¹

Shortly after the release of IMCO’s opinion, the European Commissioner for the Security of the Union, Julian King, told a press briefing that: ‘The Commission’s position is very clear – we are not in favour of so-called backdoors, the utilisation of systematic vulnerabilities, because it weakens the overall security of our cyberspace, which we rely upon’.¹⁹²

The former Article 29 Data Protection Working Party (A29WP), consisting of a representative from the data protection authority of each EU member state, issued a statement in April 2018 that strongly advocated against any obligations aimed at reducing the effectiveness of encryption in order to allow LEAs to access decrypted data.¹⁹³ With regard to encryption backdoors, the A29WP noted ‘the mathematical foundation of cryptology does not provide the basis for a secure backdoor, and numerous examples in history have shown that master keys and backdoors cannot be kept secure, even by major law enforcement agencies or by companies specialized in key management’.¹⁹⁴ However, the Council of the European Union’s Resolution on Encryption of November 2020 and the European Commission’s proposal in September 2020 for a temporary derogation from certain provisions of the ePrivacy Directive may be indicative of a more nuanced approach to regulating the use of encrypted communications

191 European Parliament Committee on the Internal Market and Consumer Protection (IMCO), ‘Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Industry, Research and Energy on the Proposal for a Directive of the European Parliament and of the Council Establishing the European Electronic Commissions Code’ (8 September 2018) 2016/0288(COD), 17-18, Amendment 14.

192 Rebecca Hill, ‘EU: No Encryption Backdoors but, eh, Let’s Help Each Other Crack that Crypto, Oui? Ja?’ (*The Register* 19 October 2017) <www.theregister.com/2017/10/19/eu_crypto_cracking/>.

193 A29WP (n 80) 1. The A29WP was replaced by the European Data Protection Board in May 2018 via the General Data Protection Regulation.

194 *ibid.*

being adopted by EU organisations.¹⁹⁵ Both of these documents indicate that EU organisations may be open to considering legislative measures that would impact the use of encryption technology within the EU. If EU member states independently pursue MEBL, this could provoke the introduction of EU-level legislation to clarify the preferred position on the use of encryption and MEBL specifically within the EU. The EU is co-credited with the technology industry for the USG's eventual abandoning of the Clipper Chip in 2000 and the influence of EU policy on the encryption debate should not be underestimated.¹⁹⁶

195 See Council of the European Union, 'Council Resolution on Encryption – Security through encryption and security despite encryption' (24 November 2020) Council of the European Union document number 13084/1/20; and European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online' (10 September 2020) 2020/0259 (COD).

196 Abelson and others (n 18) 5.

4 Is mandatory encryption backdoor legislation compatible with the right to privacy?

In proposing the need for legislative reform regarding encryption technology, former Australian Prime Minister Malcolm Turnbull indicated public safety was more important than privacy, stating: ‘The privacy of a terrorist can never be more important than public safety – never’.¹⁹⁷ Advancing a similar point of view, the former Prime Minister of the UK, David Cameron, said: ‘In extremis, it has been possible to read someone’s letter, to listen to someone’s call, to mobile communications ... The question remains: are we going to allow a means of communications where it simply is not possible to do that? My answer to that question is: no, we must not. The first duty of any government is to keep our country and our people safe’.¹⁹⁸

The sentiment that privacy is inferior to public safety and national security, expressed by Turnbull and Cameron, is reflected to some degree in international and regional human rights law. Article 17 of the ICCPR and Article 8 of the ECHR both provide a non-absolute right to privacy, allowing interferences with the right to privacy in certain circumstances. This section analyses if MEBL is compatible with the right to privacy provided in Article 17 of the ICCPR and Article 8 of the ECHR. For the purposes of progressing this analysis, some hypothesising is required. MEBL is used throughout this section to refer to a hypothetical piece of domestic legislation requiring all encryption technology providers (including providers of E2E encrypted IM applications and manufacturers and operating system providers of encryption-enabled devices) be capable of providing decrypted data when issued with a court order to do so. In the absence of any alternative method of satisfying this requirement, MEBL is assumed to require encryption technology providers to incorporate an encryption backdoor into their technology. In addition, it is assumed the MEBL is:

- being pursued to assist LEAs to conduct criminal investigations by ensuring LEAs can access decrypted data;

197 Reuters Staff, ‘“Five Eyes” Talks to Focus on Encryption: Australian PM’ (*Reuters* 13 June 2017) <www.reuters.com/article/us-australia-security/five-eyes-talks-to-focus-on-encryption-australian-pm-idUSKBN1940JY>. The statement was made in June 2017.

198 Nicholas Watt, Rowena Mason and Ian Traynor, ‘David Cameron Pledges Anti-Terror Law for Internet After Paris Attacks’ (*The Guardian* 12 January 2015). The statement was made in January 2015.

- has been adopted through standard legislative or executive procedures; and
- has been published in a publicly available register.

The following analysis focuses on the negative obligation of state parties not to interfere with the right to privacy, as opposed to the positive obligation of state parties to protect the right to privacy.

4.1 Article 17 of the ICCPR

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.¹⁹⁹

4.1.1 Interference

The first step in determining if MEBL is compliant with Article 17 is to determine if there has been an interference with one of the interests articulated in Article 17(1). MEBL is not considered to be an unlawful attack on honour or reputation and therefore this analysis focuses on the first four interests articulated in Article 17(1).

As the oversight body for the implementation of the ICCPR, the UNHR Committee provided an authoritative, yet non-binding, interpretation of the scope of Article 17 in its General Comment 16 (GC16), adopted in 1988.²⁰⁰ GC16 does not include a definition of interference, but the UNHR Committee has to date interpreted interference broadly to include measures that directly or indirectly infringe on an individual's privacy interests.²⁰¹ Regarding correspondence, the UNHR Committee noted:

Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise

¹⁹⁹ ICCPR, Article 17.

²⁰⁰ Further commentary on the status of General Comments and the role of the UNHR Committee is provided in Lee A. Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press 2014), 84 and the references cited therein.

²⁰¹ American Civil Liberties Union (ACLU), 'Privacy Rights in the Digital Age' (ACLU Foundation March 2014) <www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf> 19.

read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.²⁰²

Although GC16 is now 30 years old and predates many current methods of electronic communications, the reference to telephonic, telegraphic and other forms of communication is sufficiently future proof to apply to E2E encrypted communications sent via the Internet and messages stored as data on an encrypted hard disk.

Viewing an encryption backdoor through the lens and the language of GC16, the incorporation of an encryption backdoor into encryption technology is analogous to installing a wiretap capability in a telephone system to enable interception and surveillance. MEBL would force providers of encryption technology to tweak their technology to enable interference with encrypted correspondence to occur. A requirement to incorporate an encryption backdoor into all encrypted IM applications would effectively prohibit true E2E encrypted communications, as the encryption backdoor would introduce a technical possibility for a third party to view the transmitted data in plaintext.

From the example legislation analysed in section three, legislators do not appear to be seeking direct access to encryption backdoors when pursuing MEBL. Instead, legislators are seeking to ensure encryption technology providers can always provide decrypted data when requested to do so. However, noting Diffie and Landau's summary of personal privacy invasions by the USG since the 1940s,²⁰³ the various mass surveillance cases that have been considered by the ECtHR and the actions of the NSA and GCHQ revealed by Edward Snowden, it seems inevitable that governments will interfere with privacy when enabled to do so.²⁰⁴ Given the widespread use of E2E encrypted IM applications and encryption-enabled devices, incorporating encryption backdoors into encryption technology enables governments and other third parties to interfere with privacy on a large scale. Even if MEBL were not enforced, the UNHR Committee has previously determined the existence of a challenged law continued to inter-

202 UN Human Rights Committee (UNHR Committee), 'CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (Adopted at the Thirty-second Session of the Human Rights Committee on 8 April 1988) para 8.

203 Whitfield Diffie and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (The MIT Press 2010) 169.

204 *ibid.* For examples of mass surveillance cases considered by the ECtHR, see *Klass and Others v Germany* [1978] ECHR 4, *Roman Zakharov v Russia* [2015] ECHR 1065, *Kennedy v The United Kingdom* [2010] ECHR 682 and *Weber and Saravia v Germany* [2006] ECHR 1173, among others.

fere directly with privacy despite the fact the challenged law had not been enforced for several years.²⁰⁵ Simply the knowledge that the government *may* have the technical ability to obtain and decrypt encrypted data, regardless of whether they have the legal authority to do so, could create the perception that encrypted communications are not private.²⁰⁶ This would be the case even if the majority of encrypted communications were never decrypted and read by LEAs.²⁰⁷

On the basis that encryption backdoors enable interference with encrypted communications to occur and noting the UNHR Committee has interpreted interference with the right to privacy broadly, MEBL is likely to constitute an interference with Article 17. The authors of a 2016 report published by UNESCO support this reasoning and suggested a ‘restriction of the availability and effectiveness of encryption as such constitutes an interference with the freedom of expression and the right to privacy as it protects private life and correspondence’.²⁰⁸ Additional support for this view is provided in a report from the Office of the United Nations High Commissioner for Human Rights (OHCHR), which stated ‘the mere possibility of communications information being captured creates an interference with privacy’.²⁰⁹ If the UNHR Committee were not convinced by this line of reasoning and did not consider MEBL to constitute an interference with the interests articulated in Article 17(1), no further assessment of MEBL would be necessary and MEBL would be considered compliant with Article 17. For example, the UNHR Committee might determine MEBL is not an interference with the interests articulated in Article 17(1) on the basis that merely enabling interference with the right to privacy to occur does not, of itself, constitute interference with the right. However, this argument contradicts existing jurisprudence and the broad interpretation of interference adopted by the UNHR Committee to date.

4.1.2 Lawful and non-arbitrary

Assuming MEBL would be deemed to constitute an interference with one or more of the interests articulated in Article 17(1), the next step in assessing compliance with Article 17 is determining if the interference is unlawful or arbitrary. Guidance on the meaning of unlawful and arbitrary has been provided by the UNHR Committee in GC16. Unlawful means ‘no interference can take place except in cases envisaged by the law. Interference authorised by States can only

205 *Toonen v Australia*, Communication Number 488/1992, UN Doc CCPR/C/50/D/488/1992 (1994), para 8.2.

206 Diffie and Landau (n 203) 236.

207 *ibid.*

208 Van Hoboken and Schulz (n 77) 55.

209 OHCHR (n 19) 7, para 20.

take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant'.²¹⁰ As for arbitrary interference, this can extend to interference authorised by law: 'The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances'.²¹¹ The ICCPR does not include a list of permissible limitations on the right to privacy and, to date, the UNHR Committee has given states a wide margin of appreciation regarding such limitations.²¹²

From parsing GC16, the practice of the UNHR Committee and reports from UN Special Rapporteurs and the OHCHR, the tests for determining if an interference with the right to privacy under Article 17 is lawful and non-arbitrary can be summarised as follows.

To be lawful, an interference must be:

- consistent with the provisions, aims and objectives of the ICCPR;
- pursuant to domestic and international law;
- accessible and foreseeable; and
- precise, specific and clearly defined.²¹³

To be non-arbitrary, an interference must:

- pursue a legitimate aim;
- be necessary and in proportion to the aim pursued; and
- be the least intrusive option available.²¹⁴

Assuming the MEBL is consistent with the provisions, aims and objectives of the ICCPR, as a legislative instrument, the MEBL is pursuant to law, thus satisfying the requirement to be authorised by domestic and international law. Noting the hypothetical MEBL is publicly available and is not hidden in an unpublished or secret executive order, it would satisfy the requirement to be accessible and foreseeable. From the legislation analysed in section three, the potential ability for the IPA or the amendments introduced by the AA Act to be used to

210 UNHR Committee (n 202) para 3.

211 *ibid*, para 4.

212 Icelandic Human Rights Centre, 'Interference with the Right to Privacy' <www.humanrights.is/en/human-rights-education-project/comparative-analysis-of-selected-case-law-achpr-iachr-echr-hrc/the-right-to-respect-for-private-and-family-life/interference-with-the-right-to-privacy>.

213 The lawfulness test is based on a proposal from the American Civil Liberties Union (ACLU), see ACLU (n 201) 20.

214 The non-arbitrary test is based on a summary of authoritative sources provided in OHCHR (n 19) 7-8, paras 22-23.

introduce encryption backdoors by way of technical capability notices could fail the accessibility and foreseeability requirements. The IPA prohibits recipients of technical capability notices from disclosing the existence or contents of a technical capability notice without permission.²¹⁵ Similarly, the amendments introduced by the AA Act impose non-disclosure obligations on recipients of technical assistance requests, technical assistance notices and technical capability notices.²¹⁶ The secrecy surrounding these instruments would prevent individuals from knowing if the encryption technology they are using is subject to an encryption backdoor, thus restricting the foreseeability of interference with their correspondence. As for the requirement to be precise, specific and clearly defined, this is unlikely to be satisfied by vaguely drafted legislation such as the French proposal noted in section 3.3.3. In addition, leaving encryption technology providers to figure out a way to incorporate encryption backdoors, without providing any technical or procedural guidance, may fail the requirement to be precise, specific and clearly defined. However, openly available legislation that clearly identifies the entities required to incorporate encryption backdoors could, in theory, satisfy the lawfulness test.

In assessing if MEBL is an arbitrary interference, noting the hypothetical MEBL is being pursued to assist LEAs to conduct criminal investigations, MEBL would satisfy the requirement to be in pursuit of a legitimate aim.²¹⁷ Establishing whether MEBL is necessary and in proportion to the aim pursued is a more difficult task. The hypothetical MEBL applies to all providers of encryption technology and therefore has the potential to affect the privacy of all users of encryption technology by prohibiting true E2E encrypted communications and setting the scene for third parties, beyond just LEAs, to seek out and exploit the mandated encryption backdoors. As demonstrated in section 2.4, based on the information currently available regarding the frequency of LEAs encountering encryption during criminal investigations and the lack of any compelling evidence that encryption is an insuperable barrier to law enforcement objectives, the argument in favour of MEBL being necessary is not strong. Similarly, compromising the security of all E2E encrypted communications for the purpose of providing LEAs with the ability to obtain decrypted data is considered 'highly disproportionate to the confidentiality of communications and protection of rights of individuals'.²¹⁸ This view is shared by the UN Special Rapporteur on the right to privacy, who described the breaking of encryption as disproportionate

215 IPA, section 255(8).

216 Telecommunications Act 1999 (Cth), section 317ZF.

217 The 'prevention of disorder and crime' is specifically identified in ECHR Article 8(2) as a legitimate aim and the UNHR Committee could be expected to agree that this constitutes a legitimate aim.

218 Koops and Kosta (n 71) 891.

and privacy intrusive.²¹⁹ Based on the difficulties associated with establishing that MEBL is necessary or proportionate, it would be difficult for a state seeking to defend MEBL to demonstrate that it is non-arbitrary. To uphold the validity of MEBL the UNHR Committee would need to be convinced that it is necessary and proportionate to prohibit true E2E encryption to assist LEAs to conduct criminal investigations, despite the availability of other less intrusive measures to obtain intelligible data. The wide margin of appreciation given to states by the UNHR Committee to date is unlikely to be cast wide enough to protect legislation that would effectively prohibit true E2E encryption and interfere with the privacy of all users of encryption technology.

4.1.3 Violation assessment

On the basis MEBL would enable broad-ranging interference with encrypted correspondence to occur, MEBL is likely to constitute an interference with the right to privacy under Article 17. Accordingly, a state seeking to defend MEBL would need to demonstrate MEBL is both lawful and non-arbitrary for it to be deemed compliant with Article 17. MEBL should, in theory, be able to satisfy the requirement to be lawful. However, it would be difficult to argue that MEBL is non-arbitrary, given the identified issues with demonstrating MEBL is necessary and that MEBL would disproportionately undermine the privacy protections provided by encryption technology in the hope of obtaining incriminating data. On this basis of these issues, MEBL appears to violate the right to privacy in Article 17.

4.2 Article 8 of the ECHR

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.²²⁰

219 UNGA, 'Report of the Special Rapporteur on the Right to Privacy' (24 November 2016) UN Doc A/HRC/31/64, 20, para 58.

220 ECHR, Article 8.

Like the right to privacy provided in Article 17 of the ICCPR, the right provided in Article 8 of the ECHR is not absolute and allows interferences in certain circumstances. However, unlike Article 17 of the ICCPR, the ECHR lists the reasons for permissible interference with the right to privacy in Article 8(2).

The ECtHR Directorate of the Jurisconsult prepared a comprehensive guide on Article 8 of the ECHR in 2017, most recently updated in August 2020.²²¹ Although the Guide is non-binding, it provides a thorough summary of how the ECtHR has interpreted Article 8 and identifies supporting case law.²²² The Guide notes the right to respect for correspondence under Article 8(1) ‘aims to protect the confidentiality of communications in a wide range of different situations’.²²³ Correspondence has been held by the ECtHR to include technologies developed after the coming into force of the ECHR, such as electronic messages (emails), Internet use and data stored on computer servers, including hard drives and floppy disks.²²⁴ It follows from the ECtHR’s reasoning in *Copland v The United Kingdom* and *Petri Sallinen and Others v Finland* that messages sent electronically via E2E encrypted messaging applications and data stored on an encrypted hard disk would fall within the broad scope of correspondence under Article 8(1).²²⁵

4.2.1 Interference

The first step in determining compliance with Article 8 is to determine if there has been an interference with one or more of the privacy interests articulated in Article 8(1). Applying the same reasoning from the analysis in section 4.1.1, MEBL is likely to constitute interference with Article 8 of the ECHR on the basis that it enables interference with the right to privacy to occur. Forcing encryption technology providers to incorporate encryption backdoors is contrary to the aim of Article 8(1) to protect the confidentiality of communications.²²⁶ Encryption is an important enabler of confidentiality and weakening encryption by way of mandating the incorporation of an encryption backdoor directly impacts the ability of individuals to ensure their communications remain confidential.

221 See Council of Europe and European Court of Human Rights, ‘Guide on Article 8 of the European Convention on Human Rights’ (Council of Europe/European Court of Human Rights 31 August 2020) <https://www.echr.coe.int/documents/guide_art_8_eng.pdf>.

222 The ECtHR was established under Article 19 of the ECHR and has responsibility for ensuring observance of the ECHR by the signatories.

223 Council of Europe and European Court of Human Rights (n 221) 105, para 483.

224 *ibid*, 66, paras 337-338.

225 *Copland v The United Kingdom* [2007] ECHR 253, para 42 and *Petri Sallinen and Others v Finland* [2005] ECHR 643, para 71.

226 Council of Europe and European Court of Human Rights (n 221) 105, para 483.

The proposal that MEBL constitutes an interference with Article 8 can also be advanced by examining some of the ECtHR's decisions. In *Roman Zakharov v Russia* the ECtHR found a violation of Article 8 had occurred in circumstances where the Russian Ministry of Communications had issued orders requiring equipment installed by communication service providers must meet certain technical requirements, including a capability to conduct surveillance.²²⁷ A significant issue with the technical requirements imposed by the orders in the *Zakharov* case was that they provided Russian LEAs with 'direct access to all mobile telephone communications of all users'.²²⁸ In addition, the system in place enabled the Russian secret services and police to 'intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else'.²²⁹

The direct access provided to the Russian secret services and police in the *Zakharov* case by way of the installation of certain equipment is far beyond anything proposed in the legislation examples analysed in section three or the hypothetical MEBL. However, the requirement to incorporate encryption backdoors into encryption technology is analogous to the technical requirements imposed on communication service providers in *Zakharov*. In the domestic court cases prior to *Zakharov* applying to the ECtHR, the Russian district and city courts held the installation of equipment, pursuant to a ministerial order, to enable surveillance to occur did not in itself interfere with the privacy of *Zakharov's* communications.²³⁰ However, the ECtHR did not indicate whether they agreed with the Russian domestic courts on this point and therefore the decision in *Zakharov* does not provide a clear precedent to indicate if the ECtHR would consider a law imposing technical requirements that enable interference to occur itself constitutes an interference with the right to privacy. The facts of *Zakharov* nevertheless demonstrate the potential for the imposition of technical requirements by law on communications service providers to enable a public authority to interfere with the right to privacy.

In *Klass and Others v Germany* the ECtHR noted the mere existence of the legislation challenged in the proceedings involved a 'menace of surveillance', with the menace striking at the freedom of communication between users of postal and telecommunications services and thereby constituting an interference by a public authority with the right to privacy in Article 8.²³¹ Building on this reason-

227 *Roman Zakharov v Russia* [2015] ECHR 1065, paras 115-116.

228 *ibid*, para 241.

229 *ibid*, para 270.

230 *ibid*, para 299.

231 *Klass and Others v Germany* [1978] ECHR 4, para 41.

ing, the mere existence of legislation requiring encryption backdoors be incorporated into encryption technology could be seen as constituting a similar menace of surveillance, striking at the freedom of communication between users of encryption technology. This supports the proposal that MEBL is likely to constitute an interference with the right to privacy in Article 8.

Like the assessment of interference under Article 17 of the ICCPR, it is possible the ECtHR might be convinced that MEBL is not an interference with Article 8 of the ECHR on the basis that merely enabling interference to occur does not, of itself, constitute interference. If no interference was established, no further assessment would be necessary and MEBL would be considered compliant with Article 8 of the ECHR. However, if interference was established, which seems likely, Article 8(2) sets out a three-step test for determining whether the interference is justified.

To be justified, the interference must:

- be in accordance with the law;
- pursue one or more of the aims listed in Article 8(2); and
- be necessary in a democratic society.

4.2.2 In accordance with the law

To be in accordance with the law, the MEBL must be clear, foreseeable and adequately accessible.²³² As a piece of legislation that has been adopted through standard legislative or executive procedures and made available publicly, on its face, the hypothetical MEBL satisfies the requirement to be in accordance with the law.

4.2.3 Pursues a legitimate aim

Article 8(2) identifies the legitimate aims which may justify an interference with the interests articulated in Article 8(1). Noting the MEBL is being pursued to assist LEAs to conduct criminal investigations, this falls directly within the prevention of disorder or crime identified in Article 8(2). Accordingly, MEBL should have no issues with satisfying the requirement to be in pursuit of a legitimate aim.

4.2.4 Necessary in a democratic society

Determining if the mandatory encryption backdoor legislation is necessary in a democratic society requires a balancing of the interests of the applicant against the interests of the state.²³³ According to the ECtHR, necessity:

²³² Council of Europe and European Court of Human Rights (n 221) 10, para 15.

²³³ *ibid*, 12, para 26.

implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued; in determining whether an interference is “necessary in a democratic society”, the Court will take into account that a margin of appreciation is left to the national authorities, whose decision remains subject to review by the Court for conformity with the requirements of the Convention. The margin of appreciation to be accorded to the competent national authorities will vary in accordance with the nature of the issues and the importance of the interests at stake.²³⁴

The ECtHR has confirmed it is the duty of the state to demonstrate the existence of a pressing social need to justify an interference with the right to privacy.²³⁵ The ‘going dark’ problem could be advanced by a state as a pressing social need to justify the interference imposed by MEBL, noting E2E encrypted messaging applications and encrypted devices have made it increasingly difficult for LEAs to obtain decrypted data. If a state could demonstrate that encryption technology regularly obfuscates criminal investigations, is commonly used by criminals, was preventing LEAs from prosecuting criminals and there were no effective alternative investigative measures available, this would weigh in favour of MEBL being deemed necessary.

In interpreting the reference to ‘necessary’ in Article 10 of the ECHR, the ECtHR has noted that necessary means something more than useful, reasonable or desirable and it is assumed the ECtHR would adopt a similar approach to the concept of necessity when interpreting Article 8.²³⁶ To demonstrate that MEBL was necessary, a state would need to show ‘publicly and transparently, that other less intrusive means are unavailable or have failed and that only broadly intrusive measures, such as backdoors, would achieve the legitimate aim’.²³⁷ MEBL may be useful, reasonable and desirable for assisting LEAs to obtain decrypted data, but noting the weak argument in favour of the necessity of MEBL identified in section 2.4 and the other methods available to LEAs to investigate crimes where encrypted data are encountered identified in section 2.5, it would be difficult for a state to establish that MEBL is necessary in a democratic society.

Significantly more intrusive legislation than MEBL has previously been held by the ECtHR to be necessary in a democratic society. For example, in the *Klass* case, the ECtHR accepted that the existence of legislation allowing secret surveillance may be ‘under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or

234 *Pretty v The United Kingdom* [2002] ECHR 427, para 70.

235 *Piechowicz v Poland* [2012] ECHR 689, para 212.

236 *The Sunday Times v The United Kingdom (No 1)* [1979] ECHR 1, para 59.

237 UNGA (n 90) 15, para 43.

crime’.²³⁸ However, the legislation at issue in the *Klass* case included various conditions to be satisfied before surveillance could be conducted on identified individuals, included oversight mechanisms and only allowed surveillance to occur on a temporary basis.²³⁹ In contrast, MEBL would permanently impact encryption technology and all individuals who use encryption technology, making all encrypted communication susceptible to interference.

4.2.5 Violation assessment

Provided the ECtHR could be convinced MEBL constitutes an interference with Article 8, there are no obvious impediments to MEBL satisfying the requirement to be in accordance with the law or the requirement to be in pursuit of a legitimate aim. However, there are significant obstacles in the way of demonstrating that MEBL is necessary in a democratic society. In the absence of evidence that criminal use of encryption serves as an insuperable barrier to law enforcement objectives, it would be difficult to demonstrate that MEBL is necessary or proportionate. Accordingly, by failing to satisfy the requirement to be necessary in a democratic society, MEBL appears to violate the right to privacy provided in Article 8 of the ECHR.

4.3 Remedies under the ICCPR and ECHR

Pursuing a human rights violation claim under either the ICCPR or ECHR is a last resort measure after seeking redress at a national level. The First Optional Protocol to the ICCPR allows individuals who claim that any of their rights articulated in the ICCPR have been violated to submit a written communication to the UNHR Committee for consideration, but only after exhausting all available domestic remedies.²⁴⁰ Only individuals who are subject to the jurisdiction of a state party to the First Optional Protocol of the ICCPR can submit a written communication to the UNHR Committee for consideration.²⁴¹ Of the current 173 state parties to the ICCPR, 116 are state parties to the First Optional Protocol.²⁴² The ECtHR can receive applications from individuals, non-governmental organisations or groups of individuals claiming to be the victim of a violation of the ECHR.²⁴³ Article 25 of the ECHR requires an applicant should claim to have

238 *Klass and Others v Germany* [1978] ECHR 4, para 48.

239 *ibid*, paras 51-52.

240 Optional Protocol to the International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (First Optional Protocol to the ICCPR), Article 2.

241 *ibid*, Article 1.

242 Figures are accurate as of 1 April 2021.

243 ECHR, Article 43.

been actually affected by the alleged violation and does not permit individuals to complain *in abstracto* on the basis they feel a law may constitute a violation of the ECHR.²⁴⁴ Any individual or legal entity can submit an application under the ECHR, but the violation complained of must have been committed by one of the parties to the ECHR.²⁴⁵ Similar to the requirements for pursuing a claim under the ICCPR, all domestic remedies must be exhausted prior to submitting an application to the ECtHR.²⁴⁶

If a victim was able to choose between progressing a claim under the ICCPR or the ECHR, the enforcement mechanisms available under the ECHR are stronger than those under the ICCPR.²⁴⁷ Unlike the ICCPR, the ECHR is overseen by a court with the ability to issue binding judgments and to award damages.²⁴⁸ Were MEBL enacted and local remedies to challenge its legality exhausted, the analysis in this section indicates it would be possible to successfully challenge MEBL on the basis that it violates Article 17 of the ICCPR and Article 8 of the ECHR (assuming a victim could establish standing to submit a claim under either the ICCPR or the ECHR).

244 *Klass and Others v Germany* [1978] ECHR 4, para 33.

245 Fair Trials International, 'A Guide to Applying to the European Court of Human Rights When Fair Trial Rights Have Been Violated' (*Fair Trials International* October 2012) <www.fairtrials.org/wp-content/uploads/2012/10/YDN-ECtHR-guide.pdf>, 3 and ECHR, Article 34.

246 ECHR, Article 35.

247 Lee A. Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6(3) *International Journal of Law and Information Technology* 247, 249.

248 ECHR, Articles 41 and 46.

5 Conclusion

Without introducing encryption backdoors into encryption technology, LEAs may never be able to obtain certain data in an intelligible format. However, the current resistance to encryption backdoors from major technology companies, security experts, privacy advocates and certain organs of the EU indicates that it is highly unlikely encryption backdoors will be intentionally incorporated into encryption technology without legislative intervention. Although various governments have proposed such legislative intervention in the form of MEBL, a mosaic of intelligible data is already available to LEAs to prevent crime and prosecute criminals. Based on the information made publicly available by LEAs to date, the legal necessity of introducing MEBL has not been satisfactorily established. In addition, the technical feasibility of creating an encryption backdoor without severely compromising the security of the targeted encryption technology in the process is yet to be demonstrated. The conclusion that MEBL is not necessary is based on a combination of the likely limited effectiveness of MEBL in assisting LEAs to obtain decrypted data, a scarcity of evidence to suggest encryption poses an insuperable barrier to criminal investigations and the range of investigative methods currently available to LEAs when faced with encrypted data. In arguing that MEBL is not necessary, MEBL is also likely to violate the right to privacy articulated in both the ICCPR and the ECHR. This conclusion is unlikely to prevent states from pursuing MEBL, yet it serves as a reminder that privacy is not always inferior to the pursuit of public safety and national security.