The Apple Falling Far From the Tree? Assessing the Law of Encryption in South Africa

KC Perumalsamy and PGJ Koornhof
Department of Mercantile and Labour Law, University of the Western Cape
kperumalsamy@uwc.ac.za; pkoornhof@uwc.ac.za

This work is based on the research supported in part by the National Research Foundation of South Africa for the grant, Unique Grant No. 99180. Any opinion, finding and conclusion or recommendation expressed in this material is that of the author(s) and the NRF does not accept any liability in this regard.

Abstract

In this article we investigate the legal framework for encryption in South Africa and the instances in which it may be legitimate for a court to compel the decryption of encrypted information to protect the interests of the state. Part I introduces the problems posed by encryption and the challenges it faces today after briefly setting out its historical use. Part II will consider modern encryption, expound upon the terminology germane to encryption and its regulation under the Electronic Communications and Transactions Act 25 of 2002 and The Regulation of Interception of Communications and Provisions of Communications-Related Information Act 70 of 2002. Part III will evaluate the jurisprudence both domestic and foreign on the instances in which governments have sought to have encryption bypassed against challenges of the privilege against self-incrimination and Part IV will evaluate the domestic implications for bypassing encryption with particular regard to the constitutional privilege against self-incrimination.

Keywords

Encryption; security; right to a fair trial; right against self-incrimination

1. Introduction

The use of encryption in protecting information or data is not something that is new or dispositive to modern technological advances. There is evidence which suggests that its use stretches as far back to ancient Egypt nearly four thousand years ago where it was used to protect a variety of secretive information (Wiseman, 2015). Throughout history encryption has been used to keep religious information secret, protect military secrets, and shelter communication that is politically precarious (Wrixon, 1998).

Technological advances today have compounded its use. It covers a wider variety of interests, which often protects the ordinary individual’s security and privacy, particularly in an age where an almost inextricable link exists between technology,
our privacy and security. The proper functioning of the internet is reliant on encryption as it permits transactions which are both private and secure; it assists in preventing fraud and impersonation, and without it, it would be impossible to safely purchase and do banking over the internet (Wiseman, 2015). Yet, the efficiency of cryptography may also be used to protect illegal activity including fraud, gambling and loansharking (U.S. v Scarfo, 180 F.Supp.2d 572 [2001]). It has facilitated the construction and expansion of illicit markets for the purchasing of drugs and even hit men and has been used to conceal child pornography (Farivar, 2011; see also U.S. v Gavegnano, 205 Fed.App 954 [4th Cir 2009]). The recent dispute between Apple and the FBI has strengthened the gaze on the regulation of encryption and the circumstances under which it may be bypassed (In Re Order Requiring Apple INC to Assist In the Execution Of A Search Warrant Issued By this Court 15-MC-1902 [JO] [“Apple case”]). Additionally, mobile applications such as Whatsapp and Viber have installed end-to-end encryption, which seemingly signals a victory for privacy over security interests (Nordrum, 2016). The extent to which encryption may be bypassed has thus become the subject of significant debate. In many reported decisions, the specific issue of compelling decryption where it may assist the state with criminal investigations and proving the guilt of an accused has been dealt with against the backdrop of the privilege against self-incrimination. The Apple Case illustrates the novel problem of guarding state security where technological advancement seemingly undermines it: in contrast to the usual request for decryption the United States’ Federal Bureau of Investigation (FBI) sought to compel Apple Inc. to build software that would allow it to bypass the encryption on a mobile phone device. Both of these circumstances will be considered in respect of South Africa’s encryption regulations and likelihood of a court granting such a request in light of our encryption framework.

2. Terminology, Modern Encryption and its Regulation

Encryption is an electronic process that protects data by using a formula to transform readable data into unreadable data. An algorithm called a cipher is used to convert the readable data called the plaintext into unreadable data known as the ciphertext (Reis & Simek, 2012). The reverse process of this is known as decryption, where a key is used to transform the encrypted data back into readable data. The process of encryption may be used to protect both data at rest and data in motion. Data at rest refers to inactive data usually desktops, laptops and servers, whilst data in motion conversely relates to wired or wireless networks and the Internet (Reis & Simek, 2012).

Cryptography and the breaking of codes have always been vital for military applications (Wiseman, 2015). In South Africa, the military have historically used and controlled the encryption of hardware and software by requiring a permit or licence where a product is used for military purposes in terms of the Armaments Development and Production Act of 1968 (now repealed by Act 41 of 2002) (Michalsons Attorneys, 2015). During the Second World War cryptography and the
breaking of codes played a crucial role in the victory of the Allied forces as well (Wiseman, 2015).

Today, multiple forms of cryptography exist, but almost all are exclusively dealt with through computers. It is common for most encryptions to be secured by passwords; however, other forms of cryptographic keys may be used instead of, or in addition to passwords. Usually, this is done through a keyfile, the content of which is used as part of the encryption process, and is often stored separately from the encrypted document. A user is required to identify the correct keyfile out of all the files on the device, which provides additional protection together with the password. Modern forms of encryptions can be divided into two groups: symmetric and asymmetric keys. Symmetric key encryption concerns the same key being used to encrypt and decrypt a device, whilst asymmetric key encryption (sometimes known as public key encryption) relates to two keys being created, one private and one public. In order to encrypt messages the public key is used allowing publishing and distribution to the world without undermining the private key. This allows the private key to be kept secret while decrypting files encrypted by the public key (TrueCrypt Foundation, 2012). One prevalent algorithm used for public key encryption is the RSA, which is named after Ron Rivest, Adi Shamir and Leonard Adleman. The RSA underlies a significant amount of security for Internet communications, particularly because public key encryption is integral to the functioning and security of online commerce and private communications over the Internet (Wiseman, 2015; See also Bright, 2013).

It may be possible to penetrate the encryption without the key through attacking the cryptographic system directly, usually by trial and error or by other means (Wiseman, 2015). Many modern encryption systems are however, for the most part, impenetrable because the use of force to unlock an encryption cannot be achieved within a reasonable timeframe. Another way of unlocking the encryption is by listening to the sounds emitted by the central processing unit- usually undertaken by security researchers in laboratories (Bright, 2013). Perhaps the most effective, and contentious, method of acquiring the key is to compel the holder of the key to provide it, as in the case of *U.S. v Scarfo* and many others discussed below, including, most recently, the Apple Case.

In South Africa the principle regulation for encryption is found in Chapter 5 of the Electronic Communications and Transactions Act of 2002 (ECTA). Section 29 of ECTA mandates the establishment of a register with all cryptography providers by the Director General of the Department of Communications, which records the names and addresses of all cryptography providers, a description of the type of cryptography service or product, and particulars that are necessary for the identification and location of the cryptography provider and their products or services (s 29(1)-(3), ECTA). Failure to register a cryptographic service carries the penalty of an unspecified fine or imprisonment for a maximum of two years.
There are many challenges created by the nebulous composition of Chapter 5. For example, it has been argued that the Act is unclear as to who may be a “cryptographic provider”, what constitutes a “cryptographic service” and what exactly a “cryptographic product” is (Vermuelen, 2016). It is submitted however, that the most contentious aspect of section 29, particularly for the future regulation of encryption, concerns the unclear extent of protection given towards it. Section 29 (3) provides that a cryptographic provider is not required to disclose confidential information or trade secrets in respect of their cryptography services and products. The first reported South African case to consider this aspect, albeit only tangentially, was the Diners Club case (Diners Club Pty Ltd v Singh and Another 2004 (3) SA 630 (D)). In the case it was held that witnesses were not required to give evidence before the court related to encryption services offered to the plaintiff, notwithstanding the challenge posed by the defendant that foregoing such testimony would violate their constitutional right to a fair trial through cross-examination. The judge held that not allowing the evidence could be justified on grounds of public policy and the limitation found in section 36 of the Constitution. This judgment seemingly offers authority for the argument in favour of strong encryption protections.

The Regulation of Interception of Communications and Provisions of Communications-Related Information Act 70 of 2002 (RICA) makes provision for an application to be made to a Court in which the decryption key holder is required to disclose the decryption key or to provide assistance in respect of encrypted information (ss 1 and 21 RICA). This is known as a “decryption directive” which a judge may issue provided s/he is satisfied that any indirect communication relating to an interception direction, in whole or in part, concerns encrypted information; that the person specified in the application to the court is in possession of the encrypted information and has the decryption key thereto, and that it is not reasonably possible for the person authorised to execute the interception direction to obtain possession of the encrypted information in intelligible form without a decryption directive (s 21(4)(a)(i-iv) RICA). The wording of section 21 creates a numerus clausus on the considerations over which a decryption directive may be issued. This is evident by the use of the word “only” in outlining the instances in which it may be issued. Section 21(b) additionally appears to bolster encryption protections by providing that the designated judge must consider the nature of the encrypted information and whether there would be an adverse effect in issuing the decryption directive against the business of the decryption holder or against the decryption holder him or herself. Section 21 read together with section 29(3) of ECTA, which provides that a cryptography provider may not be compelled to disclose confidential information or trade secrets in respect of its cryptography products seemingly offers proficient support for encryption protections.

What then would be the effect of these provisions when the state seeks a decryption directive for the purposes of criminal investigations, where the holder claims that such a directive would violate the privilege against self-incrimination? Additionally, would RICA and ECTA preclude requests not just to decrypt but to build a mechanism that would allow for decryption as in the Apple Case? Section 29 of
RICA sets out the degree of assistance that must be provided by the holder of the decryption key. Ordinarily, this section provides that the decryption key holder must disclose the decryption key or provide assistance in disclosing the decryption key (s 29 (1)(a) and(b) RICA). Section 29 goes on to provide that the holder of the key need not provide any other information not covered by the decryption direction (s 29(2)(c) RICA), but section 29(5) provides an interesting proviso where the person to whom the decryption key is addressed is not in possession of the key or information relating thereto. This section provides that such a person, to whom the directive is addressed, must ‘endeavour to comply to the best of his or her ability with the decryption direction’. Thus, it would stand to reason that if the state makes a request to formulate a mechanism for decryption, and such an instruction is ignored it may appear on its face to be in contravention of section 29(5) of RICA.

3. Bypassing Encryptions under Court Scrutiny

The recent dispute between Apple and the FBI, has made requests for decryptions a focal point in the debate on encryption protections. This dispute, however, is not the first time requests for encryptions have been considered by a Court in the United States. One differentiating aspect between the Apple Case and the majority of other cases which consider decryption requests is that for the first time a request not just to decrypt but to build software that would allow passcodes to be bypassed was made by the FBI. Apple, who has assisted the government before on many occasions where a lawful Court order was made to do so, objected this time on the grounds that the effect of the FBI’s request would be tantamount to building a master key that would unlock any device, and, that in any event, it does not have the capabilities of doing so (Apple case).

The government’s request failed on the grounds that it fell short of one of the three requirements of its main authority, the All Writs Act. A party wishing to invoke the All Writs Act to persuade a court to make a competent order based on the powers conferred on the Courts through the Act - in this case, to make an order requiring Apple Inc. to build software that would allow decryption for an important interest of the state - must show that such request is (a) in aid of the Court’s jurisdiction; (b) necessary or proper and (c) agreeable to the usages and principles of the law. Whilst the court accepted that the first two requirements were satisfied it rejected that it was agreeable to the usages and principles of the law on the basis of an interpretive absurdity and possible constitutional invalidity rendered by the FBI’s submissions on instructive legislation (Apple case). A provision akin to that of section 29(5) of RICA would have invariably been of greater assistance to the FBI in the relief it sought, rather than relying on general authority permitting courts to make competent orders where it sees fit. The importance of drawing this distinction is that in South Africa, a direct challenge may be launched where the directive is issued to a person. Even if they are unable to decrypt the information, they are under an obligation to assist the authorities to the best of their ability, which may include assistance at a future date when they are able to construct the technological ability to do so.
Scrubbed of requests for encryptions has largely been done through the prism of the right against self-incrimination in the United States, where the vast majority of authority on encryptions exists. The Fifth Amendment in the United States’ constitution provides protection against the abuse by officials to extort a confession and upholds the accusatorial system of justice rather than an inquisitorial one, through recognising the right of an accused person not to incriminate themselves (Wiseman, 2015). It has also been argued that the right provides a degree of protection for an accused’s dignity and privacy (Dann, 1970). The effect of this right is that it prevents the accused from having to choose between perjury, contempt or providing evidence against him or her (Amae & Lettow, 1995). The majority of judicial opinion on this subject appears to be out of sync on the circumstances in which forced decryptions may occur.

In Re Grand Jury Subpoena Duces Tecum it was held that the right against self-incrimination under the Fifth Amendment protected the right to refuse to decrypt one’s hard drives. During a child pornography investigation, law enforcement officials seized a number of digital media from the accused’s hotel room, but were unable to decrypt them after making several attempts. They applied to a Court requesting an order to compel the accused to decrypt the hard drives. In deciding the matter the Eleventh Circuit expressed that Fifth Amendment is ignited when there is compulsion for a testimonial communication or act, which is incriminatory. Additionally, it held that the files in question were testimonial in nature. In order for evidence to be considered testimonial in nature it must “require the use of the contents of [one’s] mind and cannot be fairly characterised as a physical act” (In Re Grand Jury Subpoena Duces Tecum 670 F.3d). This is distinguishable from physical acts which are not afforded the protections of the Fifth Amendment as in the case where a Court may compel blood samples be taken without consent, or compelling an individual to provide handwriting samples for analysis (see Gilbert v California 388 U.S. 263 (1967) and Schmerber v California 388 U.S. 757 (1966)). Additionally, even communications, which are testimonial in nature, may be compelled when they form part of what is considered to be a “foregone conclusion”. In terms of this doctrine, when the government already knows of the existence of the evidence in question, where it is stored and can show the authenticity of the documents through means other than the testimony of the accused, then such testimonial evidence may be admitted irrespective of the Fifth Amendment (Fisher v The United States 425 U.S. 391 (1976)).

In Re Boucher, decided four years before Duces Tecum, the District Court of Vermont had to decide whether the Fifth Amendment would exclude evidence of child pornography on the accused’s computer. Sebastian Boucher’s laptop had been inspected whilst crossing into the United States from Canada. The officer had found files on his computer, which at the time did not require a password or the removal of any encryption to access it, with names that suggested child pornography (In re Boucher No.2 D. Vt. Feb 19, 2009). After further investigation by another officer, more files had been found, however, when the evidence was re-evaluated it was found that portion of the hard drives which contained the incriminating files were
encrypted. The encrypted files were nearly impossible to penetrate by specialists, and access was impossible without the password. Boucher was accordingly subpoenaed to decrypt the encrypted files. On appeal to the district court, he sought to quash the subpoena based on the Fifth Amendment. The district court observed that the contents of the laptop are not testimonial; however, there are circumstances in which producing documents may be testimonial even when the documents themselves are not testimonial. This is true because the act of production implies that the files do exist, that the producer had control over them and that they were in some sense authentic. The Fifth Amendment could offer protection to the production of such material because it applies to actions, which directly imply an incriminating fact. However, since the foregone conclusion doctrine may compel a defendant to produce files where the government already knows of its existence and location, the request to quash the subpoena was accordingly denied (See also Doe v U.S. 487 U.S. 201 (1988); Fisher v The United States 425 U.S. 391 (1976); U.S. v Hubbell 530 U.S. 27 (2000)). Four years later, in the Friscosu case, the government had seized six computers from Friscosu’s house in the execution of a search warrant (U.S. v Friscosu 841 F.Supp. 2nd 1232 (2012). Having failed in its efforts to decrypt the computer without the assistance of the defendant, the government then recorded a conversation between Friscosu and his wife, which provided evidence for the fact that the incriminating information on the laptop was password protected. The government sought a writ requiring Friscosu to assist it following a warrant requiring him to produce an unencrypted version of the files. In accordance with the logic in Boucher the Court concluded that Friscosu was either the owner of the computer, or failing that, the primary user of it, and that he had access to the encrypted data on the computer. Additionally, the fact that the government knew of the location and existence of the files on the computer was also seen as relevant. (U.S. v Friscosu 841 F.Supp. 2nd 1232 (2012))

Despite the varied outcomes apparent in decisions to decrypt before courts in the USA, an ostensible link exists between all of the cases mentioned above. Where the evidence in question reveals new testimonial facts to the state, the decryption of such information may not be compelled, as it would affront the Fifth Amendment. A recent example confirming this is the case of Commonwealth v. Gelfgatt where it was held that knowledge of computers being used for fraudulent activities does not warrant the protection of the Fifth Amendment as it does not reveal new testimonial facts (Commonwealth v. Gelfgatt, 468 Mass. 512 (Mass. Sup. Ct., 2014)). This also explains the rationale for the exception created by the foregone conclusion doctrine, to evidence that would, on the face of it, have the protection of the privilege against self-incrimination. In South Africa, it is submitted that unlike our American counterparts, considerations on the exclusion of evidence which potentially undermines the privilege against self-incrimination, is not contingent on whether it would reveal new testimonial facts to the state but whether the admission of such evidence would render the trial unfair or otherwise be detrimental to the administration of justice. Even though it may reasonably be argued that the broader South African standard could include such aspects as the negative effect of revealing new testimonial facts to the state, it will be shown that this is unlikely to merit the
exclusion of evidence when balancing competing considerations. A narrower standard, such as the American one is thus more likely to provide greater protection to encrypted information. Before considering this standard in light of the South African privilege against self-incrimination, it is first necessary to consider the constitutional implications of the right to privacy in respect of decryption directives.

4. Comparative Assessment between Foreign Approaches and the South African Approach to Self-Incrimination

Prior to the adoption of our Interim Constitution, the position on the admissibility of evidence was governed solely by its relevance. This position comes from our English law tradition which makes relevance the only consideration notwithstanding that such evidence may have been obtained illegally (Hogg, 2005). The American position occupies the opposite of the spectrum when compared to the position under English law. The exclusionary rule as developed by American Courts has held that evidence acquired in violation of its Bill of Rights is to be considered inadmissible and thus excluded (Mapp v Ohio (1961) 367 U.S. 643). Many common law jurisdictions such as Canada, New Zealand, Australia, Ireland and South Africa approach admissibility with considerations of both the American and English extremes to reach a middle ground approach. In South Africa, similar to the approach taken in Canada, the rule governing the admission of evidence that violates a right in the Bill of Rights is that it must be excluded where it would render the trial unfair or otherwise be detrimental to the administration of justice (s 35(5) Constitution of the Republic of South Africa, 1996).

In Zuma v The State, Kentridge AJ recognised the exclusion embraced in section 35(5) (then section 25 (3) of the interim Constitution) as one that comports with notions of “substantive fairness” (Zuma v The State 1995 (2) 642 (CC)). In doing so, he contrasts the previous position reflected in precedent with the one to be taken now. In S v Rudman and Another; S v Mthwana the Appellate Division held that the function of the Court in criminal matters was to enquire into whether there was an irregularity which departs from the formal rules and principles of procedure, without considering whether the trial was unfair in accordance with the notions of basic fairness and justice (S v Rudman and Another; S v Mthwana 1992 (1) SA 343 (A)). The Constitution requires an assessment of whether the admission of evidence would undermine the right of an accused to have a fair trial, and whether the administration of justice would be detrimental should the evidence be admitted (Qozoleni v Minister of Law and Order 1994 (1) BCLR 75 (E)).

Accordingly, the way American courts would approach forced decryption against the privilege against self-incrimination is fundamentally different to the South African approach, due to the divergent standards on the admission of evidence. The American approach may be summarised as follows: there are three requirements for the operation of the Fifth Amendment. When a statement or action of the individual is compelled, testimonial and incriminating it would be considered objectionable on the grounds of the Fifth Amendment (Fisher v U.S. 423 U.S. 391 (1976)). A great
A deal of attention has been paid to what constitutes “testimonial evidence” by American Courts. This is because a court may compel physical acts for the purposes of investigations but not evidence that is testimonial in nature (Duces Tecum case). Accordingly, the Supreme Court has found that a blood sample may be taken without consent (Schmerber v. California 348 U.S. 757 (1966)), that an individual may be compelled to turn over a key to a strongbox (U.S. v. Hubbell, 539 U.S. 27 (2000)) and that an accused may be compelled to provide handwriting samples for analysis (Gilbert v. California, 388 U.S. 263). Thus, once considered to be testimonial in nature, the Fifth Amendment protects it (Fisher case). In Doe Tecum, the court held that (in the context of decryption) the evidence in question would be considered testimonial in nature, where it would “require the use and contents of Doe’s mind and could not fairly be characterised as a physical act, and it would reveal his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives, and of his capabilities to decrypt the files.” The court went on to say that it is precisely when an act of production requires the individual to use the contents of his own mind to provide a statement of fact that it becomes testimonial (Doe). There are however instances, as outlined in the discussion in Section III above, where even evidence that is testimonial in nature may be admitted against considerations of the Fifth Amendment. This is where the “foregone conclusion” doctrine applies (Fisher case).

Where the government already knows of the existence of the evidence in question, where it is being stored and can show the authenticity of the documents through means other than the testimony of the accused, then such evidence will be admitted (Wiseman, 2015).

In the Canadian case of R v Collins, Lamer J too draws a distinction between real and testimonial evidence (R v Collins [1987] 1 SCR 265). This distinction has since been deemed unnecessary in a number of decisions (R v Burlington (1995) 28 CRR (2d) 244; R v Ross (1989) 37 CRR 369). It is submitted that the distinction is without value as the real consideration is whether the admission of the evidence would bring the administration of justice into disrepute. For purposes of section 35(5), it would be unnecessary for that distinction to be drawn because the primary concern of this section is to consider whether the admission of the evidence in question would either render the trial unfair or would otherwise be detrimental to the administration of justice. It is common cause, as was recognised in S v Tandwa and Others that where the admission of evidence renders the trial unfair it would also be detrimental to the administration of justice (S v Tandwa and Others 2008 (1) SACR 613 (SCA)).

Where it is claimed that a decryption directive would violate the privilege against self-incrimination, the first inquiry is to establish whether compelling the decryption would render the trial unfair. If this leg is satisfied, then the second inquiry on whether it would be detrimental to the administration of justice need not be fulfilled. In Tandwa it was held that when considering whether the admission of evidence would render the trial unfair, the court must take into account competing social interests. The court must exercise its discretion by weighing the competing concerns of society on the one hand to ensure that the guilty are brought to book against the
protections afforded to the accused in terms of the constitution. The standard of the community was considered in Canadian precedent but has since been done away with because of its subjectivity and uncertainty in application (Hogg, 2005). In Rothman v. Queen it was held that where the admission of evidence would shock the community, it must be excluded (Rothman v. Queen [1981] 2 S.C.R. 640). The case of Collins has done away with this standard on the basis that section 24(2) of the Canadian Charter, which recognises the exclusion of evidence that would be detrimental to the administration of justice, requires a lower standard because the section recognises that a violation of a fundamental right has already occurred (R v Collins [1987] 1 S.C.R. 265).

The more nebulous standard of bringing the administration of justice into disrepute requires greater scrutiny as what may be detrimental to the administration of justice may be a matter of great subjectivity. For example, Professor Peter Hogg, commenting on the case of Collins, opines that a consideration of disrepute differs between people: what could bring the administration of justice into disrepute could differ between a police officer and a law professor (Hogg, 2005). Nevertheless, the majority of the Court in Collins found that the standard in question concerns disrepute to the community at large. Instead of indicating what a Court should look at when reaching this conclusion, the notion of a reasonable person was proposed by Lamer J. Thus, a trial Court would have to consider what, in the eyes of a reasonable person of the community, would bring the administration of justice into disrepute.

As regards what informs the definition of “disrepute”, three factors were weighed up by a Court: (1) the nature of the evidence; (2) the nature of the conduct by it was obtained and (3) the effect on the system of justice of excluding the evidence. Aspects such as the unreliability of evidence, the methods in which evidence was discovered and other rights violations, will inform the nature thereof. Other aspects such as the deliberate violations, the absence or presence of good faith and other extenuating circumstances will inform the nature of the officials conduct (Hogg, 2005). In South Africa, we have accepted the standard set out in Collins (Pillay v The State [2011] ZASCA 111).

Despite the general acceptance of the standard of disrepute in Collins by our courts, it has been overturned in Canada by R v Grant. Grant established three new factors to be considered: (1) The seriousness of the Charter-infringing State Conduct, which places the focus on the severity of the state conduct which caused the Charter breach; (2) The Impact on the Charter-Protected Interests of the Accused which focuses on the effect of the violation on the accused person because of the State’s conduct, including inquiries into the intrusion into an individual’s privacy and the direct impact on the right not to be forced to incriminate oneself, and the effect on human dignity; (3) Society’s interest in an Adjudication on the Merits, which focuses on the reliability of the evidence in light of the Charter breach (R v Grant [2009] 2 S.C.R. 353). It is submitted that the approach taken in Grant is a more satisfactory standard that places equal weight in consideration of the rights of the accused against the
interests of the community, and, accordingly, is the more appropriate constitutional inquiry in terms of s 35(5).

In summation, when a court issues a decryption directive in terms of section 21 of RICA, and the directive is challenged on the grounds of the privilege against self-incrimination, it will likely require forced decryption where the interests of the state are concerned, even when the state does not have prior knowledge of evidence concerned. This highlights the distinction we, along with countries such as New Zealand, Canada and Ireland, follow against the strict exclusion of evidence in contravention of a right followed by America.

5. Conclusion

This article has sought to consider two instances in which decryption may be compelled by a court in order to further the interests of the state. The first concerns the question posed in the Apple Case on whether a company may be required to build a mechanism that allows the state to decrypt information. In this decision it was held that the instructing legislation does not grant the state such a right based on its incorrect interpretation of the All Writs Act relied upon by the FBI. In South Africa, a more direct provision exists in respect of the assistance required by the decryption key holder. Here the decryption key holder is required to assist the state to the best of its abilities even where they are not in possession of a decryption key. A national security interest may induce the application of this section possibly requiring the creation of such a mechanism. Admittedly, the chances of this arising are doubtful, yet the legal authority for this is more certain than that of our American counterparts.

The second consideration evaluates the extent to which the privilege against self-incrimination acts as a bulwark against forced decryptions by a court. The narrow American approach has certainly seen the exclusion of evidence based on the Fifth Amendment that would probably not occur under the South African construction. This is because the exception of prior knowledge of evidence in the American legal system is irrelevant to the South African standard which concerns whether the admission of evidence would render the trial unfair or would otherwise be detrimental to the administration of justice. In all of the cases before American courts on encryption, concerning the concealment of files with fraudulent activities and child pornography, it is submitted that our courts would admit such evidence as it does not thwart the thresholds in rendering a trial unfair or destructing the administration of justice.

6. References

Books

SBN/ISSN/Product Number 20797095
F Wrixon Codes, Ciphers & Other Cryptic & Clandestine Communication: Making and
Breraking Secret Messages From Hieroglyphs to the Internet (Black Dog & Leventhal Publishers, New York 1998) ISBN/ISSN/Product Number 1579120407
ISBN/ISSN/Product Number 0409061247, 9780409061246
PW Hogg, Constitutional Law of Canada (Thomson Canada Lrd, Ontario 2005)
ISBN/ISSN/Product Number: 978-0-7798-1337-7

South African Case Law

Bernstein v Bester NO 1996 (2) SA 751 (CC)
Diners Club Pty Ltd v Singh and Another 2004 (3) SA 630 (D)
Hyundai Motor Distributors Pty (Ltd) v Smut NO 2001 (1) SA 485 (C)
J Pillay v The State [2011] ZASCA 111
Magwaza v The State [2015] ZASCA 36
Mistry v Interim National Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC)
National Coalition for Gay and Lesbian Equality v Minister of Justice 1999 (1) SA 6 (CC)
Qozoleni v Minister of Law and Order 1994 (1) BCLR 75 (E)
S v Mayekio en Andere 1996 (2) SACR 298 (C)
S v Rudman and Another; S v Mthwana 1992 (1) SA 343 (A).
S v Tandwa and Others 2008 (1) SACR 613 (SCA).
Zuma v The State 1995 (2) 642 (CC)

Foreign Case law

Census decision 65. BVerfGE. 1 (1983)
Fisher v The United States 425 U.S. 391 (1976)
Gilbert v California 388 U.S. 263 (1967)
In Re Grand Jury Subpoena Duces Tecum 670 F.3d
In Re Order Requiring Apple INC to Assist In the Execution Of A Search Warrant Issued By this Court 15-MC-1902 (JO)
R v Burlington (1995) 28 CRR (2d) 244
R v Ross (1989) 37 CRR 369
Schmerber v California 384 U.S. 757 (1966)

Journal Articles


Online Articles


Legislation
Criminal Procedure Act 51 of 1977
Electronic Communications and Transactions Act 25 of 2002
Regulation of Interception of Communications and Provisions of Communication-Related Information Act 70 of 2002
The Armaments Development and Production Act, 57 of 1968