Precaution against What? – The Electronic or E-authentication Frameworks of the United Kingdom, Canada and South Africa

*Mzukisi N Njotini**

Abstract

Information and communication technologies (ICTs) provide opportunities and can cause setbacks to society. On the one hand, they have revolutionised the manner in which people, businesses or governments communicate and share information. On the other hand, ICTs have, inter alia, provided opportunities for the misappropriation of information in online settings. Because ICTs have become a source from which information is kept and stored, they contribute to information becoming a public good that requires legal recognition. In addition, this acceptance has meant that measures to secure information should be introduced to avert those who may wish to access, use, alter or interfere with information using whatever means possible. These measures are called e-authentication measures. They are preventive in nature and aim to validate and corroborate certain credentials necessary for the granting of authority to access information. In this article, a comparative approach to e-authentication is followed. It looks at the e-authentication structures adopted in the United Kingdom, Canada and South Africa. This approach is selected with a view to ensure that the e-authentication agenda in South Africa responds adequately to the danger of information being misappropriated online.

* LLB LLM LLD. Associate Professor, Department of Private Law, Faculty of Law, University of Johannesburg. The author wishes to acknowledge that this research was commenced and completed while he was in the employ of the College of Law, University of South Africa.

INTRODUCTION

Information and communication technologies (ICTs)[1] are essential to society, specifically the information or knowledge society.[2] They play an influential role in doing business online. For example, they ameliorate the manner in which information is exchanged and shared online. However, ICTs also generate adverse consequences to the information society. Some of these challenges have to do with the theft or misappropriation of information online.[3] This theft arises in situations where a person assumes control of information belonging to another in a manner that deprives the latter of the exclusive benefits derived from the information.[4] The deprivation does not necessarily amount to the actual or physical control of information. This is the case because ICTs create a situation where a person could assume control of a copy of information without actually depriving another of the original thereof.[5] Simply, it has now become possible for a person to assume control of information in a manner that denies the other the exclusive use and enjoyment of information.[6] The use and enjoyment is sometimes attributed to the exclusive bond that exists between a person and a thing.[7] In view of the fact that information may be misappropriated in the manner aforementioned, ICTs achieve three purposes at once.

---

1 Examples include the world wide web or the web, the internet, interactive and multimedia communications, video conferences, virtual realities, computer-aided design, the information superhighway, and technologies of electronic or e-surveillance and consumer profiling. See Steve Woolger (ed), *Virtual Society? Technology, Cyberbole, Reality* (Oxford University Press 2002) 1.

2 This is a society where 'a high level of information intensity (exists) in the everyday lives of most citizens, in most organisations and workplaces, by the use of common or compatible technology for a wide range of personal, social, educational or business activities, and by the ability to transmit, receive and exchange digital data rapidly between places irrespective of distance.' See Shiraz Durrani, *Information and Liberation: Writings on the Politics of Information and Librarianship* (Library Juice Press 2008) 256, and Torry Manning, *Radical Strategy: How South African Companies can win against Global Competition* (Zebra Press 1997) 134.

3 Information means a 'piece of news with a meaning for the recipient; its assimilation usually causes a change within the recipient.' See Ulrich Sieber, 'The Emergence of Information Law – Object and Characteristics of a New Legal Order' in Eliezer Lederman and Ron Shapira (eds), *Law, Information and Information Technology* (Kluwer 2001)10–11. Thus, it is a resource in terms of which messages and instructions are conveyed. See Hermann Kaken, *Information and Self-Organisation: A Macroscopic Approach to Complex Systems* (3 edn, Springer-Verlag 2006) 15.

4 Jonathan Burchell, *Principles of Criminal Law* (4 edn, Juta 2013) 479. See also *S v Graham* [1975] 3 All SA 572 (A) 578, *Nissan South Africa (Pty) Limited v Marnitz No (stand 186 Aeroport (Pty) Limited intervening)* (2005) 1 SA 441 (SCA) and *S v Ndebele* (2002) 1 SACR 245 (GSJ) 248.

5 Mzukisi Njotini, 'E-Crimes and E-Authentication – A Legal Perspective' (LLD thesis, University of South Africa 2016) 109–110.

6 See Johannes Van der Walt, *Die Ontwikkeling van Houerskap* (Potchefstroom University for CHE 1985) 333–334.

7 Geoffrey Samuel, 'The Many Dimensions of Property' in Janet McLean (ed), *Property and the Constitution* (Hart 1999) 47.

First, they become instruments to perpetrate the misappropriation of information.[8] Second, these technologies become targets where attacks to information stored online are commenced.[9] Third, they are used as the machinery in terms of which misappropriated information is stored.[10] In addition, a number of reasons exists why information is appropriated. In one case, information can be appropriated in order to listen to or intercept a person's private conversations.[11] In this instance, the misappropriation of information impairs or has the effect of prejudicing a person's *dignitas*, that is, the 'inborn right to the tranquil enjoyment' of a person's life,[12] which accords to the prevailing *boni mores*.[13] In other cases, information may be appropriated in order to weaken existing information security mechanisms. Accordingly, it may amongst others, be interfered with, produced or reproduced unlawfully, sold or offered for sale, procured for use, altered for use in a manner that inhibits its authenticity and credibility.[14] Espionage, terrorism, revenge, illegal immigration or assuming a new identity in order to avoid a criminal charge are, inter alia, the list of behaviours that could be used in order to attenuate the integrity of information.[15]

The theft of information mentioned above arises because information has nowadays become a public good.[16] Specifically, institutions, governments, businesses and individuals expend time, effort and money in gathering and collating information.[17] Ultimately, these institutions, governments, businesses and individuals reasonably expect that the principles of property law will recognise their rights, for example ownership, to information.[18] Thus, it is anticipated that the ambit of the law of property will be broadened in such a manner that property rights or the objects of rights are not only

---

8 Richard Downing, 'Shoring Up the Weakest Link – What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime' in Indira Carr (ed), *Computer Crime* (Routledge 2009) 9.

9 Id 709–715.

10 Id 709.

11 See *S v A* (1971) 2 TPD 293. See also the United States of America Case of *TRW v Andrews*, 534 U.S. 19 (2001).

12 *R v Umfaan* 1908 TS 57.

13 *S v A* (n 11) 207–299.

14 Section 87(1)–(2) of the Electronic Communications and Transactions Act 25 of 2002 (hereinafter referred to as the ECT Act).

15 See Sandra Hoffman and Tracy McGinley, *Identity Theft* (Greenwood 2010) 6; John Vacca, *Identity Theft* (Prentice Hall 2003) 4–5; Daniel Solove, Marc Rotenberg and Paul Schwartz, *Privacy, Information, and Technology* (Aspen 2006) 251–253.

16 See Niva Elkin-Koren and Eli Salzberger, *Law, Economics and Cyberspace: The Effects of Cyberspace on the Economic Analysis of Law* (Edward Elgar 2004) 49–50.

17 See Arnold Weinrib, 'Information and Property' (1988) 38 University of Toronto LJ 117–150. Because of this, they (reasonably) expect to have real rights in or over this information. See *Thomas Marshall (Exports) Ltd v Guinle* [1978] 3 All ER 193 209–210; and Pamela Samuelson, 'Is Information Property?' (1991) 34 Communications of the ACM 15.

18 Id Samuelson 15.

'limited to land'.[19] Consequently, the widening of the law of property will lead to situations where property rights in information are possible.[20]

Because information is significant to the information society, it is then necessary to formulate measures to preserve its credibility.[21] Traditionally, the duty to establish measures to restore the integrity of information was bestowed on computer[22] scientists and engineers of ICTs. This was the case because uncovering the adeptness of these technologies 'requires long, tedious hours of solitary work in laboratories or in isolated rooms full of machines.'[23] However, it also became necessary to involve those who formally had nothing to do with the introduction of ICTs, that is, the legal practitioners, in the design and enforcement of the measures to maintain the authenticity of information. For this reason, the ambit of the law was developed in order to cover activities or facilities that were customarily viewed to be unrelated to the law. For example, the court in the case of *S v Mashiyi*[24] had to determine, amongst others, whether a computer print-out can be admitted as evidence in terms of section 34 of the Civil Proceedings Evidence Act.[25] The court stated, amongst others, that a computer is not a person within the context of the aforementioned Act.[26] Consequently, a computer printout does not amount to a statement that is a made by a person.[27] Furthermore, the accused in the case of *S v*

---

19 Matthew Chaskalson and Carole Lewis, 'Property' in Matthew Chaskalson and others, *Constitutional Law of South Africa* (Juta 1996) 31–33. See also Francis Philbrick, 'Changing Conceptions of Property in Law' (1938) 86 University of Pennsylvania LR 696–698.

20 Mzukisi Njotini, 'Evaluating the Position of Information or Data in the Law of Property' (2015) 1 Stellenbosch LR 222–228.

21 Elkin-Koren and Salzberger (n 16) 49–50.

22 The word computer comes from the Latin word *compŭto*. *Compŭto* means to reckon together, calculate or compute. See David Simpson, *Cassell's New Latin-English English-Latin Dictionary* (Cassell & Co 1959) 125. In an information society, this term denotes an electronic or e-device that stores, retrieves and processes information. See Michael Williams, 'A Preview of Things to Come – Some Remarks on the First Generation of Computers' in Raúl Rojas and Ulf Hashagen (eds), *The First Computers: History and Architectures* (The MIT Press 2002) 1–2. Furthermore, s 1(1) of the Computer Evidence Act 57 of 1983 defines a computer as, 'computer' means any device or apparatus, whether commonly called a computer or not, which by electronic, electro-mechanical, mechanical or other means is capable of receiving or absorbing data and instructions supplied to it, of processing such data according to mathematical or logical rules and in compliance with such instructions, of storing such data before or after such processing, and of producing information derived from such data as a result of such processing.

23 Edward Tiagha, 'Technology Management and Technology Transfer in Africa' in Julius Muruku Waiguchu, Edward Tiagha and Muroki Francis Mwaura (eds), *Management of Organisations in Africa: A Handbook and Reference* (Quorum Books 1999) 243.

24 *S v Mashiyi* 2002 (2) SACR 387 (Tk).

25 Civil Proceedings Evidence Act 25 of 1965.

26 *S v Mashiyi* (n 24) 390.

27 ibid.

Van den Berg[28] intercepted certain information belonging to another and used this information to electronically credit an account in Santam bank with an amount of R800.[29] The court stated that this conduct amounted to a particular form of theft of information. Specifically, the court held that the fact that a computer system was used as the means by which the theft of information was carried out does not render the appropriation lawful.[30] In arriving at this decision, the court applied and developed the common law principles of *crimen iniuria* in determining the manifestation or not of cyber fraud or cyber smearing.[31]

In this article, the measures to preserve the authenticity of information are referred to as the electronic or e-authentication measures. These measures build on the ICT regulatory theories that are propounded by, for example, Lessig,[32] Conant and Ashby,[33] Reidenberg[34] and Von Bertalanffy.[35] Simply, these theories acknowledge that *better regulation* as opposed to *less regulation* is indispensable to the governance of ICTs and the manner in which these technologies generally operate.[36] Specifically, *better regulation*

---

28 *S v Van den Berg* 1991 (1) SACR 104 (T). See also *S v Ndiki* 2008 (2) SACR 252 (Ck), *Ndlovu v Minister of Correctional Services* 2006 (4) SA 165 (W) and *S v Harper* 1981 (1) SA 88 (D).

29 *S v Van den Berg* (n 28) 106.

30 ibid.

31 ibid.

32 The regulatory theory which Lessig propagates is referred to as the theory of regulating by 'codes'. See Lawrence Lessig, *Code and Other Laws of Cyberspace* (Accessible Publishing 1999); Lawrence Lessig, 'The Laws of Cyberspace' in Richard Spinello and Herman Tavani (eds), *Readings in Cyberethics* (Jones & Bartlett 2004) 134–144; Lawrence Lessig, 'The Law of the Horse – What Cyberlaw Might Teach' (1999) 113 Harvard LR 501–549; Lawrence Lessig, 'The New Chicago School' (1998) 27 The J of Legal Studies 661–691; Lawrence Lessig, 'The Path of Cyberlaw' (1995) 104 The Yale LJ 17–46. For further interesting reading, see Mzukisi Njotini, 'Regulation by Risks – Beyond Lessig's Codes Based Theory' (2015) 36 Obiter 293–307.

33 Conant and Ashby introduced the 'Good Regulatory Theorem'. See Roger C Conant and Ross Ashby, 'Every Good Regulator of a System must be a Model of that System' (1970) 1 Intl J of Systems Science 89–90. In terms of this theorem, it is argued that 'the *pursuit* of a goal by some dynamic agent in the face of a source of obstacles places at least one particular and unavoidable *demand* on that agent, which is that the agent's behaviours *must* be executed in such reliable and predictable way that they can serve as a *representation* of that source of obstacles.' See Daniel L Scholten, 'Primer for Conant and Ashby's Good Regulator Theorem' <http://www.goodregulatorproject.org/images/A_Primer_For_Conant_And_Ashby_s_Good-Regulator_Theorem.pdf> accessed 18 January 2018.

34 See Joel R Reidenberg, '*Lex Informatica* – The Formulation of Information Policy Rules through Technology' (1998) 76 Texas LR 553–584.

35 See Ludwig von Bertalanffy, *General System Theory: Foundations, Development, Applications* (G Braziller 1968) 38–40; Ludwig von Bertalanffy, *Perspectives on General System Theory: Scientific-Philosophical Studies* (G. Braziller 1975) 88–93.

36 For a study of better regulation, see Robert Boyer, 'The Regulation Approach as a Theory of Capitalism – A New Derivation' in Agnes Labrousse and Jean-Daniel Weisz (eds), *Institutional Economics in France and Germany* (Springer-Verlag 2001) 50; and Robert Baldwin, 'Better Regulation in Troubled Times' (2006) 1 Health Economics, Policy and Law 204–205.

recognises that ICTs are generally evolving phenomena. For example, the internet formerly referred to as the Advanced Research Projects Agency Network (ARPANET), was a military invention.[37] Its objective was to, inter alia, conceal military information from enemy countries.[38] Following this, the internet gained prominence and it was used by certain organisations charged with securing information online.[39] Nowadays, the internet has become the 'fabric of our (daily) lives'.[40] Particularly, it has become what can be termed the 'network of computer networks'.[41] Given the evolving nature of ICTs, *better regulation* posits that a fitting regulatory method is that which establishes an ICT regulatory structure that is bound or attached to the technology.[42] The latter structure should also have the ability to progress with the progressions of ICTs.[43] E-authentication measures are one of those mechanisms to deter the misappropriation of information. Specifically, these measures support the general idea that *prevention is better than cure*.[44] Contextually, the latter notion postulates that forestalling a wrong is typically better than dwelling on and making good its 'adverse effects after the event'.[45] In studying e-authentication measures, the meaning and workings of e-authentication measures are discussed in this article. Specifically, it is illustrated that e-authentication has to do with validating and corroborating information kept in online environments. Following this discussion, a comparative study of the United Kingdom (UK), Canada and South African framework to e-authentication is made. The rationale for this investigation is to ascertain whether the scheme for e-authentication adopted and followed in South Africa conforms to the developments occurring in other jurisdictions. Thereafter, the way forward for South Africa in e-authenticating information is set out. The latter examines the importance of precaution or precautionary measures in the overall framework to maintain the e-authenticity of information. Lastly, an ephemeral summary of the facts presented in this article is demonstrated

---

37 David S Kidder and Noah D Oppenheim, *The Intellectual Devotional: American History* (TID Volumes 2007) 354.

38 ibid.

39 Matt Larson, Cricket Liu and Robbie Allen, *Mastering the Domain Name System: DNS on Windows Server 2003* (O'Reilly 2004) 1–2.

40 Manuel Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (Oxford University Press 2001) 1.

41 JR Okin, *The Internet Revolution: The Not-for-dummies Guide to the History, Technology, and Use of the Internet* (Ironbound Press 2005) 19. See also Chris Reed, *Internet Law: Text and Materials* (2 edn, Cambridge University Press 2004) 8.

42 Colin Kirkpatrick and David Parker, 'Regulatory Impact Assessment – An Overview' in *Regulatory Impact Assessment: Towards Better Regulation* (Edward Elgar 2007) 1–2.

43 ibid.

44 There are also instances where prevention may not be better than cure. For example, cutting off a person's head is not better than curing such person's headache. See Gilbert Kieth Chesterton, *Eugenics and Other Evils* (Inkling Books 1922) 55.

45 Peter Cane, *The Anatomy of Tort Law* (Hart Publishing 1997) 100.

and a conceivable approach to e-authentication is recommended for South Africa.

AUTHENTICATION

Overview

Authentication or the act of authenticating is generally an old phenomenon. Different methods long existed that were aimed at supporting and preserving the believability[46] of a person or thing, for example, a document. In most cases, the term 'credibility' is used in order to establish if this believability exists. The expression 'credible people are believable people … credible information is believable information' best captures the previously mentioned.[47] The notion of credibility, and not necessarily confidence, has everything to do with the existence of trust.[48] For example, people generally trust that their friends would be compassionate, they trust that motorists would adhere to traffic rules, and they trust that purchased goods have the quality that is commensurate with the price.[49] In this manner, authentication assists in establishing trust, for example that a person is exactly who he or she purports or claims to be.[50]

The association of authentication with trust is correspondingly supported by the International Organisation for Standardisation (ISO). ISO states that authentication has to do with verifying the identity of a person.[51] According to the ISO, this verification seeks to establish facts or evidence to demonstrate that the person is who he or she claims to be.[52] Hardin follows this idea of trust as a means to establish the authenticity of a person.[53] Specifically, Hardin developed what he calls the principle of 'encapsulated interest', and provides that:

---

46 BF Fogg and Hsiang Tseng, 'The Elements of Computer Credibility' in *Computing Systems* (International Conference on Human Factors in Computing Systems, New York, 18–20 May 1999) 80.

47 ibid.

48 Peter H Kim and others, 'Removing the Shadow of Suspicion – The Effect of Apology Versus Denial for Repairing Competence-Versus Integrity-Based Trust Violations' in Ana Cristina Costa and Neil Anderson (eds), *Trust and Social Capital Organisations* (Sage Publishing 2013) 175–177. For further interesting reading, see Timothy C Earle, Michael Siegrist and Heinz Gutscher, 'Trust, Risk Perception and the TCC Model of Cooperation' in *Trust in Risk Management: Uncertainty and the Scepticism in the Public Mind* (Routledge 2010) 4.

49 LA Selby-Bigge (ed), *A Treatise on Human Nature by David Hume* (Clarendon Press 1896) 15–18. See also, the Organisation for Economic Co-Operation and Development (OECD), 'OECD Guidelines on Measuring Trust' <http://www.oecd.org/std/oecd-guidelines-on-measuring-trust-9789264278219-en.htm> accessed 27 February 2018.

50 Jean L Camp, *The Economics of Identity Theft: Avoidance, Causes and Possible Cures* (Springer 2007) 13.

51 International Organisation for Standardisation (ISO), 'Public Key Infrastructure for Financial Services – Practices and Policy Framework' <https://www.iso.org/obp/ui/#iso:std:iso:21188:ed-1:v1:en> accessed 8 February 2018.

52 ibid.

53 Russell Hardin, *Trust and Trustworthiness* (Russell Sage Foundation 2002) 109.

> Much of our ability to trust others on ordinary matters of modest scope depends on having institutions in place that block especially destructive implications of untrustworthiness.[54]

In view of the above-mentioned, according to Hardin distrust is harder to 'unlearn when conditions change to justify trust, than is trust when conditions change to justify distrust.'[55] To illustrate this, Hardin asserts that trust ensues in situations where a person to be trusted has an 'incentive to be trustworthy because they internalise the interests of the person doing the trusting.'[56] In this instance, the interests that the person has encapsulates those that the person trusting the other also possesses.[57] Also important to the study of trust is Nannestad's rationalistic and moralistic theories of trust.[58] Generally, the theories examine, inter alia, whether trust has to be understood as a belief about others' trustworthiness (rational trust) or as a social norm in terms of which one person treats the other or others.[59] According to this, trust involves a cognitive attitude (and not belief) which is founded on concerns as opposed to certainty.[60]

For authentication purposes, certain characteristic traits of a person are pivotal in establishing the requisite trust.[61] The most essential characters include the eyes, nose or mouth.[62] In some instances, it may also become essential to inspect or validate a person's fingerprints. This could be done by studying the distinctiveness of the structure of the fingerprints.[63] The other way to establish whether trust exists may be to corroborate the signature of a person. In this instance, one will have to examine the available principles regarding the credibility of signatures in South Africa. This is the position because signatures are generally required to be handwritten, typewritten, or be in some form of a photographic procedure.[64] In other words, a person writes his or her name 'as a signature to a document in attestation,

---

54 ibid.
55 Id 107.
56 Id 109.
57 ibid.
58 Peter Nannestad, 'What we Learned about Generalised Trust, if Anything?' (2008) 11 Annual Review of Political Science 413–436.
59 See in general, Karen Frost-Arnold, 'The Cognitive Attitude of Rational Trust' (2014) 191 Synthese 1957–1974.
60 Id 1962.
61 Massimo Tistarelli, Andrea Lagorio and Enrico Grosso, 'Understanding Iconic Image-Based Face Biometrics' in Massimo Tistarelli, Josef Bigun and Anil K Jain (eds), *Biometric Authentication* (Springer 2002) 22.
62 ibid.
63 Kenneth Nilson and Josef Bigun, 'Complex Filters Applied to Fingerprint Image Detecting Prominent Symmetry Points Used for Alignment' in Tistarelli and others (n 61) 39.
64 Roger Kerridge and Alastair HR Brierley, *Parry and Kerridge: The Law of Succession* (12 edn Sweet & Maxwell 2009) 43 and John Barlow, Lesley C King and Anthony G King, *Wills, Administration and Taxation: A Practical Guide* (8 edn Sweet & Maxwell 2003) 3.

confirmation, ratification' of certain facts.[65] Indeed, there are exceptions to this general rule. These exceptions relate to signing using thumbprints[66] and initials.[67]

For authentication purposes, a debate exists regarding whether a mark could or should be accepted as a signature. Particularly, there is a viewpoint that a mark should be in the form of a thumbprint, rubber stamp or a seal-ring impression before it can be regarded as a signature.[68] However, the latter view is rejected by some academics on the basis that a signature also includes the making of a mark.[69] Accordingly, any mark on a document made by a person for the purpose of attesting the document, or of identifying the mark as his or her act is his or her signature thereof.[70] Accordingly, the intention of a person at the time of making the mark is significant. This can be deduced from the fact that:

> Unless parties contemplate some particular form of signature, any sign or mark made with the intention of signifying assent to the document will suffice.[71]

Accordingly, the mental element, that is, whether a person intended to sign a document, is adequate.[72] The latter view seems to have been followed by the court in the case of *Jhajbhai v The Master*.[73] In this case, the court stated that the intention of a person in 'writing or signing his name is the criterion'.[74] In situations where a person 'intends his mode of writing or signing his name to represent his signature, it is effective as such.'[75] Therefore, it is sufficient if a person can be identified by means of the writing or signature and the writing or signature illustrates or can be taken to mean that a person intends to be legally bound.[76]

---

65 Reinhardt Buys (ed), *Cyberlaw @ SA: The Internet and the Law in South Africa* (Van Schaik Publishers 2000) 131. See also, *Putter v Provincial Insurance Co Ltd* 1963 (3) SA 145 (W) 148.

66 *In the Estate of Finn* (1935) 105 L.J.P. 36.

67 Section 1 of the Law of Succession Amendment Act 43 of 1992.

68 Marius Johannes de Waal and MC Schoeman-Malan, *Law of Succession* (4 edn Juta 2008) 60. See also the English cases of *In the Goods of Savoy* (1851) 15 Jur. 1042, *In the Goods of Jenkins* (1863) 3 SW & Tr. 93 and *Thorn v Dickens* [1906] W.N. 54.

69 Section 1 of the Law of Succession Amendment Act.

70 See *Putter v Provincial Insurance Co Ltd* 1963 (3) SA 145 (W) 148E.

71 Richard Hunter Christie, *The Law of Contract in South Africa* (LexisNexis 1996) 118.

72 For an opposing view to the subjective approach to signing, see the case of *Dempers v The Master* 1977 (4) SA 444 (SWA) and *Meyill v The Master* 1084 (3) SA 387 (C).

73 *Jhajbhai v The Master* 1971 (2) SA 370 (D).

74 Id 372.

75 ibid. See also the English case of *Hindmarsh v Charlton* (1861) 8 HL Cas 160 171 where it was said that 'the subscription must mean such a signature as is descriptive of the witness, whether by a mark or by initials, or by writing the full name.'

76 Stephen York, Ken Chia and Hammond Suddards (eds), *E-Commerce: A Guide to the Law of E-Business* (Butterworths 1999) 51.

E-Authentication

E-authentication is an online equivalence of offline authentication.[77] For the sake of completeness, e-authentication is distinguished from electronic or e-authorisation. E-authorisation has to do with a process of determining whether a person was subjected to the e-authentication measures and can henceforth access a particular facility or resource.[78] In this procedure, e-authorisation schemes may be used.[79] These schemes detail the steps to be followed in order to illustrate the 'formal decision, or an implied decision, concerning access to a service activity or the exercise thereof.'[80] However, e-authentication is a process in terms of which a person or legal entity verifies the believability or genuineness of information.[81] It amounts to an 'assertion of validity, such as the signing of a certificate: we authenticate what it certifies.'[82] The aforesaid arises in situations where a person or legal entity verifies the validity or genuineness of a particular piece of information.[83] In view of this, e-authentication measures are designed to promote and maintain trust in electronic or e-commerce.[84] This trust is generally achieved by ensuring that the persons who pass the e-authentication process are granted access to information and that those who fail the process are refused access to information.[85]

---

77 Scott Berinato, 'FFIEC: Second Thoughts on Second Factors' <http://www.csoonline.com/article/220784/FFIEC_Second_Thoughts_on_Second_Factors> accessed 22 April 2017.

78 Dobromir Todorov, *Mechanics of User Identification and Authentication: Fundamentals of Identity Management* (Auebach Publications 2010) 7.

79 See art 4 of Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006.

80 See art 4(6) of Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006.

81 See art 3(5) Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014.

82 Stephen Mason, *Electronic Signatures in Law* (2 edn Cambridge University Press 2007) 1.

83 ibid. See also OECD, 'OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication' (2007) <https://www.oecd.org/sti/ieconomy/38921342.pdf> accessed 30 October 2017.

84 United Nations Commission on International Trade Law (UNCITRAL), *Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication* (UN Publication 2009) 35.

85 Article 4(13) of the Commission of the European Communities, 'Proposal for a Directive of the European Parliament and of the Council on Payment Services in the Internal Market and Amending Directive 97/7/EC, 2000/12/EC and 2002/65/EC' 1 December 2001.

In South Africa, electronic or e-signatures[86] are normally used for e-authentication purposes.[87] These e-signatures assist in enhancing the ability to authenticate information online.[88] This ensures that the original contents of information are protected from undesirable intrusions, modifications or alterations.[89] However, the e-signatures have to meet the requirements of section 13 of the Electronic Communications and Transactions Act 38 of 2001 (ECT Act). The first requirement is that a signature does not lose its legal force or effect merely because it is in electronic form.[90] Secondly, in cases where a signature is required for purposes of concluding an electronic or e-transaction, the requirement of signing is met in relation to a data message[91] if a method is used to identify a person and to indicate a person's approval of the information communicated.[92] Thirdly, the requirement of signing is complied with if the method to identify a person is reliable for the purpose for which the information is communicated.[93] In online settings, the aforementioned means that certain codes in general support the structure for e-authentication. The most significant of these codes or devices are passwords or pins that depend on public or private key infrastructures (PKIs), smart cards, one-time passwords (OTPs),[94] USB plug-in devices or biometric identification.[95] Passwords or codes amount to the technology that is ordinarily utilised in order to control and manage access to information. These e-authenticating codes or devices operate in

---

86 In terms of s 1 of the ECT Act, an e-signature refers to the 'data attached to, incorporated in, or logically associated with other data and which is intended to by the user to serve as a signature.' See also, art 3(10) of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 (hereinafter referred to as Regulation (EU) 910/2014); and DKY Tang and CG Weinstein, 'Electronic Commerce: American and International Proposals for Legal Structure' in *Regulation and Deregulation: Policy and Practice in the Utilities and Financial Services Industries* (Clarendon Press 1999) 333.

87 Fangguo Zhang and Yumin Wang, 'Security Fundamentals' in Weidong Kou (ed), *Payment Technologies for E-Commerce* (Springer-Verlag 1998) 24.

88 Stephen E Blythe, 'Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of the Growth in E-Commerce with Enhanced Security' (2005) 11 Richmond J of L and Technology 1.

89 ibid.

90 Section 13(2) of the ECT Act.

91 A data message is data generated, sent, received or stored by electronic means and includes voice, where the voice is used in an automated transaction; and a stored record. See s 1 of the ECT Act.

92 Section 13(3)(a) of the ECT Act.

93 Section 13(3)(b) of the ECT Act.

94 OTPs are random numbers that are required to be used when entering into, for example, e-transactions. They can only be used once and become inactive as soon as the purpose for which they were initiated and issued has been achieved.

95 Peter N Grabosky and Russel G Smith, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities* (Routledge 1998) 152. For further interesting reading, see Federal Financial Institutions Examination Council (FFIEC), 'Authentication in an Internet Banking Environment' <http://www.ffiec.gov/pdf/authentication_guidance.pdf> accessed 13 July 2013.

the same manner as a key.[96] Specifically, a password may be used in signing a document or a communication, for example an electronic or e-document. These may include any content stored in electronic form, for example, a text, sound, visual or audio-visual recording. Furthermore, PKIs may be used in order to e-authenticate information.[97] Accordingly, the first key is referred to as a symmetric key. In this case, the same key is used both for encryption (a process of making information unintelligible to other computer users) and decryption (process of transforming information into something intelligible). The second key is called an asymmetric key. In this regard, the key which is used for encryption differs from the one used for decryption.[98]

The 'Needham-Schroeder Public Key Protocol' illustrates, inter alia, the reasons why the distinction between symmetric and asymmetric keys is essential for e-authentication purposes.[99] This Protocol argues that symmetric or short keys normally are held by the person to be e-authenticated.[100] However, asymmetric or long keys are stored in an e-authentication server. A person who wishes to access information will enter the short key. Thereafter, the latter key will be matched with the long key. If a match is then established or the person completes all the validation processes, access to the information will be granted.[101]

In summary, a number of reasons exist regarding why it is necessary for information to be protected in terms of the law. The most common of these is that information has become a public good. Specifically, information is valuable to the information society and, because of this, users of information expend effort and time to gather information. Consequently, they reasonably expect that their interests or rights in this information should be protected from unlawful intrusions or interception.[102] In this article, e-authentication measures are discussed as some of the measures to protect information. These measures seek to promote trust by guaranteeing that information is only accessible to those that are entitled to the information in terms of the law. Having established the need to protect information, the section below discusses the existing frameworks to e-authenticate information. These are based on the UK, Canada and South African e-authentication frameworks. Specifically, the UK and Canadian e-authentication structures are similar to that of South Africa. They support the idea of establishing confidence

---

96 Mark Burnett and Dave Kleiman (eds), *Perfect Passwords: Selection, Protection, Authentication* (Syngress Publishing 2006) 3–4.

97 Id 13.

98 ibid.

99 See in general, Roger M Needham and Michael D Schroeder, 'Using Encryption for Authentication in Large Networks of Computers' (1978) 21 Communications of ACM 993–999.

100 Id 994.

101 Id 994–996.

102 Van der Walt (n 6) 150 and Njotini (n 5) 45.

in e-commerce. Furthermore, they postulate that risks to information generally exist. Therefore, a meaningful structure to protect information should respond to these perceived risks.

E-AUTHENTICATION FRAMEWORKS

United Kingdom

The UK framework to e-authentication is founded on a number of initiatives. These include the Electronic Communications Act,[103] Directive 2007/64/EC[104] and Regulation (EU) 910/2014. The UK initiatives seek to support the principle that 'there is no such thing as zero risks' to information.[105] Specifically, they recognise that information is susceptible to be used for purposes other than those envisaged by its holder. Therefore, it is indispensable to generate online environments where information is protected from inappropriate appropriations. The basis for this creation is to build trust in online environments.[106] More specifically, it has to do with rationalising that a lack of trust in online environments leads to legal uncertainty, and a lack of legal certainty leads to a lack of confidence in prevailing information security measures.[107] For example, the EU lists the need for building trust as one of the basic fundamentals for the information society.[108] Consequently, mechanisms are put in place to alleviate incidents wherein information is interfered with, misappropriated or misused. E-authentication measures are considered to be some of the overriding mechanisms to prevent this interference with, misappropriation or misuse of information.

Within the context of the UK, e-authentication measures refer to a 'process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.'[109] In this process, the identification information of a person is identified using electronic identification means.[110] These means can be in the form of a material or immaterial unit of identification information.[111] The measures to e-authenticate identification information are required to be proportionate, sound and adequate.[112] In other words, the risks connected

---

103 See Electronic Communications Act 2000.

104 See Directive of the European Parliament and of the Council on Payment Services in the Internal Market of 13 November 2007 (hereinafter referred to as Directive 2007/64/EC).

105 See Commission Implementing Decision (EU) 2015/1505 of 8 September 2015.

106 Preamble to Regulation (EU) 910/2014.

107 Preamble to Regulation (EU) 910/2014. See also The Office of the e-Envoy, 'E-Government – Authentication Framework' (2000) <https://ntouk.files.wordpress.com/2015/06/authentication-framework.pdf> accessed 30 October 2017.

108 See Commission Implementation Decision (EU) 2015/1505 of 8 September 2015.

109 Article 3(5) of Regulation (EU) 910/2014.

110 Article 3(1) of Regulation (EU) 910/2014.

111 Article 3(2) Regulation (EU) 910/2014.

112 Article 5(e) of Directive 2007/64/EC.

to the misappropriation of information should be identified, assessed and managed. The aforementioned has to be done in a manner that is reasonable, fair and efficient. More specifically, e-authentication technologies must already exist that are able to respond sufficiently to the identified risks. These technologies have to promote the ideal that e-authentication measures should be commenced during the time when, for example, a person uses or wishes to rely on the payment systems[113] offered by a payment institution. The rationale for this ought to be to permit such a person to start a payment transaction or transactions.[114] Importantly, a unique identifier in the form of a code, pin or password constitutes the most important piece of information to initiate a transaction or transactions. With this information, the person indicates his or her intention to carry out a payment transaction or transactions.[115] Following this, a payment institution relies on this information to identify and validate the information of a person. It uses signature-verification data for the latter-mentioned purposes. This data can be a code or public cryptographic key[116] or a combination of letters, numbers or symbols.[117] Therefore, it is essential that the identified information ought to be directed at 'establishing the authenticity and integrity of the communication or data.'[118]

Article 2(2) of the Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 lists the number of possibilities available to validate information online. These are that the validation process must allow for the validation of e-signatures,[119] it ought to be indicated in the signed document, in the e-signature or e-document[120] and it has to confirm the validity of an advanced e-signature. The last-mentioned view is in line with the idea that the e-signature verification process should generally support the structure for advanced e-signatures.[121] This is so because these e-signatures are the enhanced forms of e-signatures. Specifically, they are required to meet the extensive requirements of Article 26 of Regulation (EU) 910/2014.[122] In one instance, they may be used in order to establish with precision the identity of a person (signatory).[123] In other instances, they may be depended

---

113 A payment system is a fund-transfer system where payment transactions are processed, cleared and settled. See art 4(6) of Directive 2007/64/EC.

114 A payment transaction refers to acts of placing, transferring or withdrawal of funds, irrespective of any underlying obligations between the payer and the payee that are initiated by the payer or payee. See art 4(5) of Directive 2007/64/EC.

115 Article 54 of Directive 2007/64/EC.

116 Article 2(7) Directive 1999/93/EC.

117 Article 4(21) of Directive 2007/64/EC.

118 S 7(3) of the Communications Act.

119 Article 2(2)(a) of the Commission Implementation Decision (EU) 2015/1505 of 8 September 2015.

120 ibid.

121 Article 3(1) Regulation (EU) 910/2014.

122 These requirements are discussed in the section below.

123 Caroline M Laborde, *Electronic Signatures in International Contracts* (Peter Lang 2010) 70.

upon in order to guarantee the integrity of an e-document[124] or information contained in an e-document.[125] An e-signature with a PKI is frequently the most important example of an advanced e-signature.[126] Simply, PKIs are the electronic signature creation data.[127] They include the unique information, for example, codes or passwords, that is used by the signatory.[128]

It was already stated above that the e-signature verification process should generally promote the structure for advanced e-signatures. However, the prevailing question is what does this really mean to the process to e-authenticate information? The answer can be abstracted from, inter alia, Article 26 of Regulation (EU) No 910/2014. This article lists a number of requirements that an advanced e-signature should comply with. These requirements are that an e-signature, for e-authentication purposes, must be uniquely connected to a particular signatory, that is, the holder of the information to be subjected to e-authentication; the e-signature must be capable of identifying the signatory; the e-signature must be created using e-signature creation information, for example, codes or passwords, that the signatory can, with a high level of confidence, use under his sole control; and the e-signature must be linked to the information signed therewith in such a manner that any subsequent change in the information is easily detectable.[129]

Generally, advanced e-signatures should achieve a number of purposes. First, they should ensure that the data used to create the e-signature is the same as the data used or to be used to validate the e-signature.[130] Second, they must guarantee the individuality of the e-signature in a manner that restores the credibility of the signed data.[131] Third, they must be undertaken in a technology neutral environment.[132] In other words, the use and validation of advanced e-signatures must not be specific to particular technology. However, it should be carried out using technologies.[133]

Canada

In Canada, certain principles for secure information are fundamental to the structure for e-authentication. On the one hand, the principles provide for the performing of diverse responsibilities, for example, the provisions of

---

124 This may include any content stored in electronic form, in a particular text or sound visual or audiovisual recording. See art 3(35) of Regulation (EU) 910/2014.

125 Laborde (n 123) 70.

126 Aashish Srivastava, *Electronic Signatures for B2B Contracts: Evidence from Australia* (Springer 2013) 38.

127 Article 3(13) of Regulation (EU) 910/2014.

128 ibid.

129 Article 26(a)–(d) of Regulation (EU) No 910/2014.

130 Article 32(1)(c) of Regulation (EU) No 910/2014.

131 Article 32(1)(d)–(g) of Regulation (EU) No 910/2014.

132 Blythe (n 88) 9.

133 ibid.

risk control and management, security of information, confidentiality of information, and the requirements for recovery plans in circumstances where information is or was interfered with or misused.[134] On the other hand, the principles promote an appropriate appreciation of the risks regarding the misappropriation of information. This acceptance helps in the design and structuring of e-authentication measures.[135] In this context, a number of features are used with a view to support the e-authentication process. First, the risks to information are identified and assessed. Second, the identified risks are categorised according to the degree and extent of the threat that they have or are likely to have to information. Third, information security measures are established that seek to respond to existing and potential risks.

For e-authentication purposes, the Personal Information Protection and Electronic Documents Act[136] is significant. Part 2 of this Act applies to the regulation of, amongst others, e-signatures, for example, letters, characters, numbers or symbols.[137] Therefore, e-authentication measures, within the context of this Act, are some of the processes that support the creation of a secure e-signature framework in Canada. For example, the secure e-signature framework has relations to the presentation of the hash-function to the identified information. By a hash-function is meant an electronic one-way mathematical process.[138] Included in the aforesaid process is a multitude of information that is recorded into the system, for example, a computer. Furthermore, the secure e-signature framework contains piecemeal information that is engendered into a system as an output.[139] Subsequently, the information contained therein may be converted into a message digest or digests.[140] The information in the form of a digest or digests ought to be unique to each digest or digests.[141] To facilitate this exclusivity, algorithms may be allocated to each digest. Lastly, the secure e-signature framework has to be connected to a particular key applied or allocated for application to encrypt the message digest. This key can be a pin, username or password.

Having regard to the above-mentioned, the question is what does this really mean to the structure to e-authenticate information in Canada? Section 48(2) of the Personal Information Protection and Electronic Documents Act

---

134 Industry Canada, 'Principles for Electronic Authentication – A Canadian Framework' (12–23 May 2004) <https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/Authentication.pdf/$file/Authentication.pdf.> accessed 30 June 2018.

135 Treasury Board of Canada Secretariat, 'Framework for the Management of Risk' <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422> accessed 13 June 2017.

136 Personal Information Protection and Electronic Documents Act 2000.

137 Section 31(1) of the Personal Information Protection and Electronic Documents Act.

138 Section 1 of the Secure Electronic Signature Regulations 2005.

139 Daniel J Rogers, *Broadband Quantum Cryptography* (Morgan & Claypool Publishers 2010) 41; and Cristian Radu, *Implementing Electronic Card Payment Systems* (Artech House 2003) 376–377.

140 Section 1 of the Secure Electronic Signature Regulations.

141 ibid.

provides some assistance. This section details a number of characteristics of the e-authentication process. First, it provides that available ICTs have to be used to create e-signatures.[142] Second, it states that the e-signatures have to be exclusive to a person, that is, the holder of the information that is the subject of the e-authentication process.[143] Third, it enunciates that e-signatures must be incorporated into, attached or associated with an e-document.[144] Fourth, it argues that the e-signatures must be under or subject to the individual control of a person.[145] Fifth, it provides that the e-signatures must identify a person and be able to corroborate his or her information.[146] Sixth, it states that the e-signatures must be created in such a manner that it can be clearly established whether they have been changed since their incorporation, attachment or association with the e-document.[147]

South Africa

The overall agenda to secure ICTs and the activities that transpire through the use of ICTs in South Africa is regulated in the ECT Act and National Cybersecurity Policy Framework for South Africa of 4 December 2015 (Cybersecurity Policy). The Cybersecurity Policy is not necessarily law. Simply, it sets out the plans of action that are essential to safeguard activities that take place in these technologies or through the use of ICTs. Specifically, the Cybersecurity Policy came about pursuant to the pronouncement by the Department of Justice to 'battle crime using technology-based solutions and partnerships.'[148] Furthermore, it is designed to create a secure, dependable, reliable and trustworthy ICT environment in South Africa.[149] The Cybersecurity Policy seeks to carry out all this by, inter alia, guaranteeing confidence and trust in the secure use of ICTs.[150] In this regard, the following principles are fundamental to the realisation of this requisite confidence and trust:

> Promote a Cybersecurity culture and demand compliance with minimum security standards; strengthen intelligence collection, investigation, prosecution and judicial processes, in respect of preventing and addressing cybercrime, cyber terrorism and cyber warfare and other cyber ills; establish public-private

---

142 Section 48(2)*(a)* of the Personal Information Protection and Electronic Documents Act.
143 ibid.
144 Section 48(2)*(b)* of the Personal Information Protection and Electronic Documents Act.
145 ibid.
146 Section 48(2)*(c)* of the Personal Information Protection and Electronic Documents Act.
147 Section 48(2)*(d)* of the Personal Information Protection and Electronic Documents Act.
148 Guy Martin, 'Cyber Security Policy will go before Cabinet for Approval this Year' <http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=13783> accessed 1 November 2017.
149 The Cybersecurity Policy 14.
150 ibid.

> partnerships for national and international action plans; ensure the protection of National Critical Information Infrastructure; and promote and ensure a comprehensive legal framework governing cyberspace.[151]

Within the context of the Cybersecurity Policy, the term 'cybersecurity' is defined very broadly. It refers to a number of activities which have to do with the collection of tools, policies, security concepts, safeguards and guidelines, risk management approaches, actions, training, best practices, assurances and technologies that are essential to the protection of online environments in South Africa.[152]

For e-authentication purposes, sections 37 and 38 of the ECT Act are indispensable. However, it is essential to note that the aforesaid sections do not specifically provide for a system of e-authentication. On the one hand, section 37 of the ECT Act regulates the accreditation[153] of authentication products or services.[154] The manner in which the accreditation of authentication products or services is done is dealt with in the section below. Suffice it to say that authentication products or services refer to the products or services designed to identify the holder of an e-signature to other persons.[155] Examples of these products and services include facilities, for example, software or hardware, that are used or intended for use in order to authenticate information. The facilities intended to be used to e-authenticate information are the signature creation data and the signature verification data.[156] Accordingly, it is mandatory that the signature creation data must be a unique number.[157] This indicates that the number serves or should serve as a secret code or key that is exclusive to a person and must be capable of being used to create an e-signature.[158] Generally, the signature verification data can be in the form of any other data.[159] However, it is essential for this data to be able to authenticate the e-signature that is exclusive to a computer user.[160] On the other hand, section 38 of the

---

151 The Cybersecurity Policy 12.

152 Id 6.

153 Accreditation refers to the recognition of authentication products or services by an Accreditation Authority. See s 33 of the ECT Act.

154 See s 37(1) of the ECT Act. Notice 1537 of 2004 and Chapter II of GN 8701 GG 29995 (20 June 2007) (hereinafter referred to as the Accreditation Regulations). This section deals with the application for accreditation, the manner of applying for accreditation, the information to be disclosed in such application, the submission of the application, the granting of the application, the publication of accreditation and the refusal of the application for accreditation.

155 Section 1 of the ECT Act.

156 Section 1 of the Accreditation Regulations.

157 ibid.

158 ibid; and *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 (21 November 2014) 12 (also cited as 2015 (2) SA 118 (SCA)).

159 Section 1 of the Accreditation Regulations.

160 ibid.

ECT Act lists the factors that should be taken into account before the authentication products or services are accredited. These factors have to do with the financial and human resources of the authentication products or services, including its assets; the quality of the hardware and software systems used by the authentication products or services; the procedures for processing of products or services; the availability of information to third parties relying on the authentication products or services and the regularity and extent of audits by an independent body.[161]

The accreditation of authentication products or services must be done in a manner that supports a structure for advanced e-signatures. Advanced e-signatures, within the context of the ECT Act, are the e-signatures that result or have the propensity to result from a process which has been accredited by the Accreditation Authority in terms of section 37 of the ECT Act.[162] In the main, they facilitate the identification of information.[163] Furthermore, they assist in guaranteeing the integrity and credibility of information.[164] This is carried out with a view to ensure that the e-signature to which the authentication product or service relates is inimitably connected to its holder; is capable of identifying its holder; is generated using the means that can be maintained under the exclusive control of its holder; is attached to the data or data message to which the e-signature relates in such a manner that any consequent alteration of the information or data message is detectable, and is based on the face-to-face identification of its holder.[165]

THE WAY FORWARD FOR SOUTH AFRICA

Overview

The UK, Canada and South African approaches to e-authentication support the structure for advanced e-signatures. This structure requires that an e-signature should be generated that belongs to the person who wishes to access information, the e-signature must be exclusive to such a person, the e-signature must be created using e-signature creation information, for example, codes or e-authentication keys, the e-signature must be incorporated or attached to an e-document in a manner that enables it to identify such a person and the e-signature must be generated using methods that can be maintained under the control of the person to whom it belongs. In the UK and Canada, the structure for advanced e-signatures should adequately respond to the risks relating to the misappropriation of information. Specifically, it is accepted that inadequate measures to secure information can result in a lack of trust regarding the integrity of information or information security mechanisms. Therefore, the UK and Canada requires the measures

---

161 Section 38(2)*(a)–(d)* of the ECT Act.
162 Section 1 of the ECT Act.
163 Laborde (n 123) 70.
164 ibid.
165 Section 38(1)*(a)–(e)* of the ECT Act.

to e-authenticate information to be proportionate, sound and reasonable. Particularly, they ought to provide for risk control and supervision; security and privacy of information and certain recovery strategies in the event of loss of or damage to information.

However, there are currently no express provisions for a risk-sensitive based e-authentication framework in South Africa. Given this state of affairs, a precautionary method of e-authentication is discussed in this article. Specifically, it is argued that this e-authentication method is the most progressive for South Africa. This is the position because it conforms to the principles of natural justice.[166] Specifically, it requires, amongst others, that regulatory measures should generally be procedurally fair.[167] Accordingly, the precautionary method of e-authentication promotes foresight or prudence in relation to the manner of designing regulatory mechanisms.[168] For this purpose, it is equated with the doctrine of *in dubio pro natura*.[169] This doctrine implies that in circumstances where there is uncertainty regarding the existence of risks, the protection of nature should be preferred.[170] In other words, 'careful forward planning, [and] blocking the flow of potentially harmful activities' should prevent prevailing risks.[171]

In practical terms, the precautionary method of e-authentication should conform to a particular regulatory structure. First, it has to be based on a technology-neutral framework. This means that available technologies must be instrumental to the initiation of the e-authentication process. Second, it must promote equity, that is, good governance, accountability, objectivity, transparency, appropriate expertise and effectiveness.[172] This means that the e-authentication process must appropriately and reasonably respond to the danger that information may be misappropriated. Furthermore, the precautionary method of e-authentication has to promote an investigation of the intrinsic characteristics, for example, the online behaviour, of the person accessing information. It must also provide for the control and management of the identified risks. In addition, the method has to promote the provision of a general awareness of or education relating to the risks and dangers associated to the misappropriation of information. Accordingly, awareness programmes that are designed to inform and teach the public can

---

166 *Bridgetown Greenbushes Friends of the Forest Inc v Executive Director of the Department of Conservation and Land Management* 2000 SOL Case 673, 1 December 2000 118.

167 *Mohr v Great Barrier Reef Marine Park Authority* [1998] AATA 805 124.

168 MJ Williams, *NATO, Security, and Risk Management: From Kosovo to Kandahar* (Routledge 2009) 97.

169 Arie Trouwborst, *Precautionary Rights and Duties of States* (Koninklijke Brill 2006) 2.

170 David R Boyd, *The Environmental Rights Revolution: A Global Study of Constitutions, Human Rights and the Environment* (UBC Press 2012) 224.

171 Joel Tickner and Carolyn Raffensperger, *The Precautionary Principle in Action: A Handbook* (Science and Environmental Health Network 1991) 2.

172 Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy, and Practice* (Oxford University Press 1999) 76.

be introduced. The basis may be to demonstrate to the public the available e-authentication measures and the areas where these mechanisms have proved to be inadequate in the past. Lastly, the precautionary method of e-authentication has to provide for the monitoring and evaluation of the identified risks to information. Therefore, a determination has to be made regarding the seriousness of the misappropriation or situations where the misappropriation is so pernicious that postponing e-authentication measures would be undesirable.[173]

CONCLUSION

Information has become a public good. Specifically, it is depended upon by governments, institutions, and business to communicate and do business online. Because of this, governments, institutions or businesses expend time, effort and financial resources in order to preserve their integrity and image to the public. Information, having become a public good, has also become a sought-after resource by criminals. In this article, theft or misappropriation of information is identified as one of the ways in which information may be interfered with or damaged online. Espionage, terrorism, revenge, illegal immigration or assuming a new identity in order to evade a trial are, inter alia, some of the factors that contribute to the theft or misappropriation of information in online environments.

Given the fact that information is in danger of misappropriation, e-authentication measures are discussed. These measures are designed to restore the integrity of and trust to information. They require a verification of the validity or believability of certain credentials of the person seeking to access information. These credentials can be in the form of codes, devices or a number of symmetric or asymmetric keys. The rationale for this is to ensure that the persons that pass the e-authentication process are granted access to information and that those who fail or do not possess the required code, device or key are refused access. Following the general discussion of e-authentication measures, a comparative study of the UK, Canada and South African approaches to e-authentication is investigated. It is noteworthy that these countries agree that the e-authentication process should support the structure for advanced signature. In other words, the process should provide that an e-signature be generated for the person who wishes to access information; the e-signature must be exclusive to a person; the e-signature must be created using e-signature creation information, for example, codes or e-authentication keys; the e-signature must be incorporated or attached to an e-document in a manner that enables it to identify the person; and the e-signature must be generated using methods that can be maintained under the control of the person to whom it belongs. It is also worth noting that the

---

[173] Steve Rayner and Robin Cantor, 'How Fair is Safe Enough? – The Cultural Approach to Societal Technology Choice' 1987 (7) Intl Jl of Risk Analysis 3–9.

UK and Canada requires the above-mentioned structure to be risk-sensitive based. Specifically, it has recognised that 'there is no such thing as zero risks' to information.[174] Therefore, proportionate, sound and reasonable e-authentication measures should be designed that respond adequately to the risks. Available e-authentication technologies should be used in order to effect the e-authentication process. These technologies should be bendable enough to deal with novel ways of misappropriating information in online settings.

Given the fact that risk-sensitive based e-authentication measures are not expressly provided for in South Africa, a precautionary method of e-authentication is recommended. This method operates within the parameters of the existing e-authentication agenda envisaged in sections 37 and 38 of the ECT. It requires that foresight in planning should be present during the e-authentication process. In addition, it advocates that e-authentication measures should have regard to the available technologies or the developments in existing technologies. In doing so, risk-sensitive based e-authentication measures requires the process of e-authentication to be proportionate to the risks of information being misappropriated online. In the latter regard, the online behaviour of persons accessing information have to be studied, the risks to information must be identified, controlled and managed and the general public ought to be made aware or educated of the risk relating to the interference with, damage to or destruction of information using recent forms of ICTs. Therefore, sections 37 and 38 of the ECT Act will have to be developed in order to give effect to the risk-sensitive based e-authentication measures. Alternatively, supplementary provisions can be introduced through the current Cybersecurity Policy that speak to the necessity for the risk-sensitive based e-authentication measures.

[174] See in general, Preamble to Regulation (EU) 910/2014.