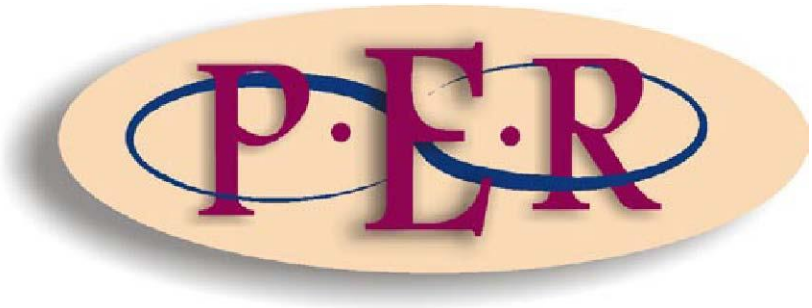
Author: D van der Merwe

A COMPARATIVE OVERVIEW OF THE (SOMETIMES UNEASY) RELATIONSHIP BETWEEN DIGITAL INFORMATION AND CERTAIN LEGAL FIELDS IN SOUTH AFRICA AND UGANDA



2014 VOLUME 17 No 1

http://dx.doi.org/10.4314/pelj.v17i1.07

A COMPARATIVE OVERVIEW OF THE (SOMETIMES UNEASY) RELATIONSHIP BETWEEN DIGITAL INFORMATION AND CERTAIN LEGAL FIELDS IN SOUTH AFRICA AND UGANDA

D Van der Merwe*

1 Introduction

Before having a look at the legal questions addressed in the present article, it might be wise to set out the facts that typically give rise to such legal questions. *Da mihi facta, dabo tibi ius*,[1] should be the slogan of every careful jurist.

Governments have traditionally spied upon their own citizens, usually in the name of "security of the state". Hermann Göring, head of the German secret police[2] during the Hitler-era, used a device to "bug" the telephones of foreign embassies as well those of its own citizens suspected of being critical of Hitler.[3] This practice was extended (with more sophisticated technology) by the secret police[4] of the former state of East Germany. It is ironic that the present chancellor of a free and democratic Germany, Angela Merkel, now finds herself being spied upon by (modern digital) technological devices used by the United States' National Security Agency (NSA) and by the United Kingdom's Government Communications Headquarters (GCHQ). Apparently she was not alone in being targeted by these two "democracies". Similar devices were also used against President Rouseff of Brazil, Ban Ki-Moen (the UN Secretary-General), the Pope and many others.[5] The activities of the United States in this regard have been exposed by whistleblower Dennis Snowden, who has had to apply for and receive political asylum from Russia (even

* Dana van der Merwe. B.Jur (UPE), LLB and LLD (Unisa). Formerly Professor in Public Law at the University of South Africa, at present Research Fellow at that institution. Email: vdmerdp@mweb.co.za.

1 "Give me the facts and I shall give you the law".

2 The Gestapo.

3 Scholtz *Beeld*.

4 The Stasi.

5 Napolitano 2013 http://reason.com/archives/2013/11/07/how-can-the-nsa-spy-on-merkel-the-pope-t.

more ironical!). What is especially shocking is that the NSA infrastructure is by now so powerful (and well-funded by the US government) that it is able to intercept literally ALL electronic communication across the world. The sifting for information out of all that data can come later.

Is the law able to provide any guidance in this struggle between governments and travellers on the "Information Highway"?

In a number of previous articles, published in various legal journals,[6] the present author has explored the convoluted relationship between information and the law. This relationship has often been problematic because of the rapidly changing nature of the technological infrastructure of the former concept and the inherent conservatism of the latter. The uneasy juxtaposition described above has also been the motivation behind both of my published works, entitled *Computers and the Law*[7] as well as (in its latest embodiment) *Information and Communications Technology Law*.[8]

Other authors, locally as well as overseas, have also engaged upon this quest. The very first book on the topic came from United Kingdom author Colin Tapper.[9] In his introduction to the work,[10] the author asks whether "there is any more need for a book on the law of computers than there is for one on the law of typewriters or tuning forks". The book then discusses the admissibility of digital documents in the law of evidence, the new problems that copyright in digital creations has brought about, the "dramatic emergence for the personal privacy of human beings" and also problems arising from the abuse of computer systems. The work is the more valuable for the fact that UK law is contrasted with US law in a comparative fashion throughout.

---

6 For instance Van der Merwe 1983 *Obiter*; Van der Merwe 1985 *SACC*; Van der Merwe 1994 *Obiter*; Van der Merwe 2007 *THRHR*.
7 Van der Merwe *Computers and the Law* 1986 and 2000.
8 Van der Merwe *et al Information and Communications Technology Law*.
9 Tapper *Computer Law*.
10 Tapper *Computer Law* xxiii.

Besides the works by van der Merwe mentioned above, other South African authors have also entered upon the digital terrain. One of the first of these works was *Cyberlaw*[11] by Hofman. Although dated in certain respects, this title still contains one of the best explanations of PKI[12] and the X.509 technical standard for creating reliable digital signatures.[13]

South Africa has also seen three editions of *Cyberlaw@SA*.[14] These works have had almost each chapter written by different authors and the contributing set of authors has also changed considerably between given editions. The chapters in the latest edition on Privacy and Data Protection,[15] Electronic Evidence[16] and "Cybercrime and the investigation of cybercrime"[17] will be dealt with as being especially relevant to the subject matter of the present article.

The last-mentioned work reveals a possible problem when dealing with ICT Law in this manner. Each of the chapters seems to have been written independently without a bird's eye-view of the field as a whole, and thus without making the cross-references required [18] The book simply reflects the idiosyncratic stance of each of the established legal disciplines with regard to the new phenomenon of digital information, for which it seems these disciplines were not yet quite ready. Each legal field seems therefore to have developed its own "coping mechanism" to try to accommodate this newborn but unruly child.

In the opinion of the present author only a holistic approach to this new legal field can hope to succeed. Whether it be called "Computer Law", "CyberLaw" or "ICT

11 Hofman *Cyberlaw*.
12 Public Key Infrastructure.
13 Hofman *Cyberlaw*. 71ff. For an interesting update, especially as far as digital signatures are concerned, see Hofman "South Africa" 483.
14 The first and second editions (with Buys as editor) appeared in 1999 and 2004 respectively (Buys *Cyberlaw@SA* 1999 and 2004). The third edition (Papadopoulos and Snail *Cyberlaw@SA*) is utilised for the purposes of the present article.
15 Papadopoulos and Snail.
16 Meintjes-van der Walt.
17 Watney.
18 This is also manifest in the fact that each chapter commences with a new set of footnotes.

law", a whole set of new considerations from the digital world impinges upon a legal system based on the analogue world.[19]

The present article borrows from the US for many of its factual scenarios,[20] but then strives to apply African law to solve similar problems that might arise on this continent. It will be shown that there are three main role-players as far as information is concerned, namely the state (although it sometimes tries to be both referee and player), the public (whose right to electronic privacy needs to be protected) and the purveyors of merchandise over the Internet by means of so-called "electronic commerce".[21] The role that the law is supposed to play in this (already) difficult task of giving to each his (or her) due is complicated by the fact that some of these problems are international in nature. It is suggested that such jurisdictional problems need to be addressed urgently, for instance by multi- or bilateral treaties between countries.

2 The law of privacy

2.1 Multi-lateral treaties

As far as privacy is concerned, the entire second section of the African Union's *Draft Convention on Cyber-legislation in Africa* deals with this topic specifically. The Convention distinguishes between "Personal Data", "Sensitive Data" and "Health Data". The first concept is defined as:

> … any information relating to a physical person directly or indirectly identified or identifiable by reference to an identification number or to one or several elements relating to his/her physical, physiological, genetic, psychic, cultural, social or economic identity.[22]

---

19 Intellectual Property (IP) constitutes an uneasy "halfway" stage between traditional rights based on tangibles and the new rights based on digital "property". However, this topic falls outside the ambit of the present article.

20 As with IT, the US also seems to be the pioneer as far as IT crime is concerned.

21 Better known as "e-commerce".

22 Part II, s 1, A II-1.4 *Draft Convention on Cyber-legislation in Africa* (2012).

Of interest also is the way in which these concepts may affect and influence each other, as is expressed by the Convention's definition of "Interconnection of Personal Data":

> (A)ny connection mechanism that harmonizes processed data designed for a set goal with other data processed for goals that are identical or otherwise, or interlinked by one or several processing official(s).[23]

This would include the systematization of otherwise meaningless data into valuable information. Of course, this very process might have negative implications for the privacy of the individuals whose personal data is being processed.

Part II Section III of the Convention sets out an institutional framework for a "protection authority" to be tasked with the protection of personal data in each state of the African Union. Failure to comply with the prescribed guidelines may lead to "adversarial proceedings"[24] in order to ensure compliance.

At first glance South Africa does not seem to have become part of any supra-national privacy protection network as yet. Nonetheless it does form part of the SADC[25] grouping of states, which has issued a *Draft Model Law on Crime and Cybercrime*. Although *prima facie* this provision does not appear to have anything to do with privacy, one of its sections[26] deals with "Data Espionage". This occurs when any person unlawfully "obtains computer data which are not meant for him and which are specially protected against unauthorized access". The reference to a "person" seems to indicate that this crime is not committed by states or on behalf of states infringing upon the privacy of an individual. This has to do with a person gaining access to the forbidden fruits of government information.

---

23 Part II, s 1, A II-1.8 of the *Draft Convention on Cyber-legislation in Africa* (2012).

24 This phrase is wide enough to cover both adversarial and inquisitorial proceedings, depending on the system of procedure applicable in the state concerned.

25 Southern African Development Community.

26 S 8 of the *SADC Draft Model Law on Crime and Cybercrime* (2012).

An unsettling report entitled *Humanitarian Trends in Southern Africa: Challenges and Opportunities* has recently been drawn up by 33 researchers from the Universities of Antananarivo in Madagascar, North-West, Stellenbosch and Lesotho. According to the report the tension between "limited governance", a youthful population and increasing access to cellular technology makes for an explosive mixture in Southern Africa. Four countries, namely Angola, the Comores, Malawi and Zimbabwe are described as "fragile states" which do not comply with the expectations of their citizens. The ability to organise mass meetings rapidly by means of cell-phones constitutes a "fire hazard".[27]

Uganda already forms part of the East African Community (EAC) *Cyber-laws Framework*.[28] In contrast to South Africa, a significant part of this framework does contain legal provisions on the protection of personal privacy.[29]

Uganda's parliament would therefore have to make sure that its local legislation complies with the Community's *Cyber-laws Framework* (Phase I). Part of this Framework focuses on privacy and recognizes the "critical importance of data protection and privacy" and recommends that further work needs to carried out on this issue, to ensure that

> (a) the privacy of citizens is not eroded through the Internet;
> (b) that legislation providing for access to official information is appropriately taken into account;
> and to take into account:
> (c) the institutional implications of such reforms and
> (d) the international best practice in that area.

27 Claasen *Beeld*. The expression "fire hazard" is that of the present author.
28 This Framework includes the countries of Kenya, Uganda, Tanzania, Rwanda and Burundi.
29 S 2.5 of the *EAC Cyber-laws Framework* (2009) on "Data Protection and Privacy".

2.2 Domestic legislation - South Africa (with some reference to the USA)

Virtually the only protection against an over-inquisitive government[30] seems to lie in a constitutionally guaranteed right to privacy. South Africa is in the fortunate position of having a supreme *Constitution*,[31] which may be enforced by the Constitutional Court. Section 14(d) of the 1996 *Constitution* deals with "Privacy" as follows: "Everyone has the right to privacy, which includes the right not to have the privacy of their communications infringed."

A new Privacy Act has just been adopted by Parliament during its current session.[32] This long-awaited piece of legislation has as its stated goal the protection of the personal information of citizens of South Africa. The entire gestation project leading up to the new Act was undertaken under the aegis of the South African Law Reform Commission[33] in a project entitled "Privacy and data protection".[34] Hopefully this new law will finally make concrete the lofty ideals with regard to privacy expressed in the *Constitution*.

The authors of the work *ICT Law*[35] expressed the opinion that the provisions of the new Act would probably replace the data protection provisions contained in the existing *Electronic Communications and Transactions Act*.[36] There is a dire need for this progression, since the latter Act provides only for a voluntary regime of data protection with no sanctions attached to a failure to adopt such a regime. That said, the new Privacy Act seems to be geared more towards administrative control and oversight than towards directly criminalising deviations from the prescribed procedures and standards.

---

30 Although one would also like legal protection against nosey fellow citizens, this is not the focus of the present article.

31 An interim version was passed in 1994 and the final version in 1996.

32 *Protection of Personal Information Act* 4 of 2013, signed by President Zuma on the 19th November 2013.

33 The SALRC.

34 SALRC Privacy and Data Protection.

35 Van der Merwe *et al Information Communications Technology Law* 368.

36 *Electronic Communications and Transactions Act* 25 of 2002 (ECT Act).

The gist of the new legislation deals with the "processing" of "personal information" pertaining to a "data subject" by a "responsible party".[37] The protection of personal information already formed part of the (Roman-Dutch) common law of delict in South Africa and has since been comprehensively affirmed both by academic writing[38] as well as in decided cases.[39] The new statutory protection is to be afforded through administrative control by means of a "regulator", rather than by resorting to litigation.

If a person feels aggrieved by (what he or she believes to be) false information held by someone else, that person has another option: he (or she) may also act in terms of the *Promotion of Access to Information Act*.[40] According to the provisions of the last-mentioned Act, the respondent has to provide the requester access to the information concerned, whether such information is held in hard copy or in digital format. The requester would then be able to decide whether or not to pursue further legal redress.

Although the *National Credit Act*[41] also deals with information, and often with information that the data subject would have preferred to keep private, it has a different "flavour" to most other data protection legislation. This is because the statute now deals with information that starts off being private, but which might have to be disclosed later on because of the increasingly commercial nature of such information.[42]

Almost as a counterweight to the Privacy Act discussed above, the South African Government has now countered with its own *Protection of State Information Bill*

---

37 Van der Merwe *et al Information Communications Technology Law* 313ff; Papadopoulos and Snail *Cyberlaw@SA* 275ff.

38 Neethling and Potgieter *Law of Delict*.

39 *O'Keeffe vs Argus Printing and Publishing Co Ltd* 1954 3 SA 244 (C); *National Media Ltd v Jooste* 1996 3 SA 262 (A); *Financial Mail (Pty) Ltd vs Sage Holdings Ltd* 1993 2 SA 453 (SA); *Janit v Motor Industry Fund Administrators (Pty) Ltd* 1995 4 SA 293 (A) - this list is not comprehensive.

40 *Promotion of Access to Information Act* 2 of 2000 (PAIA).

41 *National Credit Act* 34 of 2005.

42 See Papadopoulos and Snail *Cyberlaw@SA* 298; Van der Merwe *et al Information Communications Technology Law* 364ff.

(POSI).[43] This would appear to look after the information interests of the state, as opposed to those of its citizens. The POSI Bill is supposed to deal with the classification, protection and dissemination of state information. The problem is that the government now appears to be using powers given to it for a different purpose (to act as the referee in the information game) in order to guard its own secrets (as a player in that game). This might just be an instance of *Quis custodiet custodes ipsos*?[44]

Rumour hath it that President Zuma is also about to sign into force the *General Intelligence Laws Amendment Bill* (GILA),[45] which will give the government the power to monitor and intercept "foreign" communications. For this purpose, the government proposes merging all existing intelligence organisations into an umbrella body - the overarching "State Security Agency".

Also slightly disturbing are the suggested amendments[46] to the ECT Act. Section 1 of the Bill sets out new definitions of "critical information", "critical information infrastructure" and a "critical information infrastructure administrator". Sections 53 to 58 then deal with the identification, registration, management and audit of such critical information infrastructures. Clarifying the concept of a "critical information structure" is apparently left to the discretion of the Minister of Communications:

> The Minister may by notice in the Gazette-
> (a) declare certain classes of information which is of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens to be critical information for the purposes of this Chapter; and
> (b) establish procedures to be followed in the identification of national critical information infrastructure for the purposes of this Chapter.[47]

The only hope that a citizen would have against his or her own government acting in terms of the above legislation would seem to lie in the South African *Constitution*.

---

43 Popularly known as the "Secrecy Bill".
44 "Who guards the guardians themselves"?
45 Popularly known as the "Spy Bill".
46 As published in concept form in GN 888 in GG 35821 of 28 October 2012 (*Electronic Communications and Transactions Amendment Bill*).
47 Suggested replacement for s 53 of the ECT Act.

The Constitutional Court has a right to test all forms of local legislation for compatibility with the values enshrined in the *Constitution*. If such a law has transgressed the last-mentioned values, the Court would have the power to declare null and void such provisions as are in conflict with the *Constitution*. For this reason it is very important that the judges appointed to serve in this court do not carry with them any political affiliation that might cloud their judgment. In this regard the examples of famous American Justices such as Oliver Wendell Holmes Jr. and Louis Brandeis[48] should serve as continuing inspiration for our own Constitutional Court to protect South African citizens against the ever-increasing powers of the State. Brandeis was, of course, the co-author of a seminal article on privacy, which has set the tone of the debate on this topic ever since.[49]

As may be seen from the proposed legislation discussed above, besides the commercial players in e-commerce,[50] government itself might now constitute a threat to online privacy, claiming security considerations as justification. Instead of merely being the enforcer and protector of the private rights of its citizens, the modern state has now itself become a player in the information game and its rights in this regard could, and have, come into conflict with those of its citizens as far as mutually destructive claims to information are concerned.

A source of revelation to the present author in this regard has been the work *The New Digital Age*,[51] by Eric Schmidt (the Executive Chairman of Google) and Jarred Cohen (the Director of Google Ideas). The authors speak of a "push-pull between privacy and security in the digital age" and expect things to become much worse before they become better:

> The authorities responsible for locating, monitoring and capturing dangerous individuals will require massive, highly sophisticated data-management systems to

48 See para 3.2 below for a case where these three American Judges of Appeal held that an opinion, no matter how "loathsome", deserved protection under the law unless the safety of the State itself was threatened.

49 Brandeis and Warren 1890 *Harv LJ*.

50 Who disregard privacy considerations in order to perform online marketing and advertising.

51 Schmidt and Cohen *New Digital Age*.

> do so. Despite everything individuals, corporations and dedicated nonprofit groups are doing to protect privacy, these systems will inevitably include volumes of data about non-terrorist citizens - the questions are how much and where.[52]

A number of American citizens have already illustrated their protest against similar actions by these "authorities" (in the shape of the US government) by becoming conscientious offenders.[53] The first of these was one Philip Zimmermann, who had created a data-encryption programme called PGP.[54] However, the programme was classified as a "munition" in terms of US law and accordingly banned from export. Zimmermann thereupon published the source code in a book.[55] This was not subject to the same restrictions since "printed matter" is protected in terms of the First Amendment to the US *Constitution*. The popular movement that grew around this campaign has come to be known as "Wikileaks".[56]

Followers of this popular movement have repeatedly clashed with the US government.[57] Amongst these have been Aaron Swartz, aged 26, a programmer who committed suicide while awaiting trial upon a charge of hacking an academic computer at MIT. Private Bradley Manning, aged 25, was convicted for giving classified files to "Wikileaks" after being charged not only with stealing military secrets, but also in terms of the *Espionage Act* and with a charge of "aiding the enemy".[58] He may face up to 134 years in prison. Edward Snowden, aged 29, has since gained political asylum in Russia after a highly publicized flight from the US, where he worked as an intelligence analyst.

Were these prosecutions really necessary to protect the state against its own citizens or are they merely signs of a generation gap between (young) creators and (old) enforcers?

---

52 Schmidt and Cohen *New Digital Age* 173.
53 For a popular version of this conflict see Scherer 2013 *Time*.
54 An acronym for "Pretty Good Privacy".
55 Zimmermann *PGP Source Code and Internals* MIT (Massachusetts Institute for Technology) Press.
56 An obvious pun on the Internet online encyclopedia called "Wikipedia".
57 Mention of these cases will be made again below when specifically discussing criminal law.
58 See Anon 2013 *Time* 13.

2.3 Domestic legislation - Uganda

This East-African country is also in the fortunate position of having a *Constitution* that affirms the protection of privacy as a right of Ugandan citizens.[59] The relevant provision reads as follows:

> No person shall be subjected with the interference of the privacy of his home, correspondence, communications or other property.

It is interesting that the Ugandan Human Rights Commission (UHRC) has been tasked to deal with the delimitation of conflicting rights and that this matter is not left to the courts. The country also does not have a Data Protection Authority, as is the case in many other countries.[60] The UHRC would therefore be the sole body handling all complaints arising out of the abuse of rights relating to privacy.

One can only hope that members of the UHRC are not simply civil servants owing allegiance to the Executive, otherwise the separation of powers between the three arms of government would have come to naught.

3 Security, criminal law and evidential provisions pertaining thereto

3.1 Multilateral treaties

In the area of criminal law, the best-known example in this regard is probably the Council of Europe's *Convention on Cybercrime*.[61] It has classified computer crime into three categories, namely "Offences against the confidentiality, integrity and availability of computer data and systems",[62] computer-related offences,[63] content-

---

59 By means of s 27 of the *Constitution*.

60 Hopefully this will also be the situation in South Africa by the time that the present article is published.

61 *Convention on Cybercrime* (2011) drawn up in Budapest, Hungary on the 23rd of November 2011. A sufficient number of countries (also outside of Europe) have by now ratified the Convention so that it has come into force.

62 Title 1, including actions such as "hacking" and "phishing".

63 Title 2, including actions such as computer-related forgery and fraud.

related offences[64] and offences relating to infringements of copyright and related rights.

This seems to be an excellent instrument by means of which to co-operate internationally. Although South Africa apparently signed the treaty, it has not yet been able to ratify it. Even though this country complies substantively with the criminal and evidential conditions of the Act, our legislature has not yet placed the proper infrastructures and procedures in place so as to comply with all the requirements necessary to be in a position to ratify the treaty.[65]

South Africa forms part of the grouping of countries to which the Draft Southern African Development Community's *Model Law on Crime and Cybercrime* was meant to apply. The *Model Law* recommends that, besides those offences already covered in South Africa's ECT Act, new crimes should be added, such as "Illegal Remaining", Data Espionage, Identity-related crimes, Crimes relating to Racism and Xenophobia,[66] "Denial of Homicide and Crimes against Humanity", Spam, "Disclosure of details of an Investigation",[67] "Failure to permit Assistance"[68] and Electronic Harassment. The Model Law also contains important provisions with regard to evidential proof and jurisdiction.

In the author's personal view the splitting up of co-operation treaties into various disparate regions is a pity. The adoption of a single, worldwide basis for co-operation would have constituted a more significant step forward.

As stated above, Uganda is part of the East African Community (EAC) and therefore partly responsible for the UN Conference on Trade and Development's *Draft EAC*

64 Mostly relating to online child pornography.
65 Van der Merwe *et al Information Communications Technology Law* 101ff.
66 A Greek-derived word that literally means "fear of foreigners".
67 This would seem to have important implications for the freedom of the press.
68 This apparently relates to situations with regard to the search of premises (s 25of the *SADC Draft Model Law on Crime and Cybercrime* (2012)) and the production of data from a computer system or by an Internet service provider (s 27 of the *Model Law*).

Framework for Cyber-laws (Phase I).[69] This contains a suggested legal framework for electronic transactions, electronic signatures and authentication, computer crime and consumer protection, as well as data protection and privacy.

3.2 South Africa (with a comparative view regarding the USA)

In all probability, no legal field has been affected more by the arrival of the digital world than the Law of Evidence. For centuries this field had been content with distinguishing between objects of evidential value that could be classified as real[70] evidence and other objects[71] that bore marks, symbols or writing with a meaning independent from the surface they had been inscribed upon, which could be classified as documentary evidence.

Some commentators have argued for the creation of an entirely new field of evidence that could stand independently, apart from the traditional distinction between things and documentary evidence.[72] This question becomes particularly acute with regard to documentary evidence because of the latter's possible hearsay nature and the attendant matters of reliability (both of the machine and of its operator) and the weight to be accorded such evidence. Some South African courts have treated computer-based evidence as real evidence and other courts have seen it as documentary evidence.[73]

The present author has already recommended[74] that a deeper distinction be adopted in the above regard. It is based on a work by Eastlake and Niles entitled *Secure XML: The New Syntax for Signatures and Encryption*. The authors distinguish

---

69 *Draft EAC Framework for Cyber-laws* (Phase I) (2008). Phase II deals mainly with intellectual property issues and although of great commercial interest, falls outside the scope of the present article.

70 Originating from the Latin word *res*, meaning a thing.

71 Usually "paper" from the Egyptian *papyrus* plant. Even though the substance later changed to wood pulp, the name remained the same.

72 See Schmidt and Rademeyer *Bewysreg* 358ff.

73 Schmidt and Rademeyer *Bewysreg* 366 and cases such as *S v De Villiers* 1993 1 SACR 574 (Nm); *S v Harper* 1981 1 SA 88 (D); *S v Howard* (Johannesburg Regional Magistrates Court) unreported case number 41/258/02.

74 In Van der Merwe *et al Information Communications Technology Law* 128.

between the so-called "paper" and "protocol"-approaches[75]. The former approach attempts to squeeze digital documents into the traditional paper mould, with so-called "originals" being admissible as evidence and "copies" probably not admissible, as being less reliable. The problem is, of course, that nowadays 99% of all documents are produced by a digital computer and the only way to produce a true original would be to have a human sign one of the many printouts possible from the data stored on the computer. The signatory would also have to do so by means of a "wet" signature,[76] because of the suspicion with which digital signatures are still viewed by many businessmen, despite the fact that such signatures may be made almost foolproof.

The latter so-called "protocol" approach takes a much more revolutionary approach. The authors describe this approach as follows:

> PROTOCOL: What is important are bits on the wire generated and consumed by computer protocol processes. The bits are marshaled into composite messages that can have a rich multilevel structure. No person ever sees the full message, as such; rather it is viewed as a whole only by a 'geek'[77] when debugging – even then he or she sees some translated visible form. If you ever have to demonstrate something about such a message in a court or to a third party, there isn't any way to avoid having experts interpret it. Sometimes proponents of the protocol orientation forget that pieces of such messages are actually included in or influence data displayed to a person.[78]

Depending on the answer given to the above matters, entirely different approaches have to be followed by the litigating parties and entirely different skills might be needed to evaluate such evidence. The emphasis on experts in the above quotation seems to show clearly that we are dealing with real and not documentary evidence.

It is also significant that the whole exercise as described above is to ensure that documentary evidence in electronic format is acceptable as evidence and also to ensure that proper evidential weight is given to such evidence. In this regard, new

---

75 Eastlake and *Niles Secure XML* 469.
76 In other words, one produced by the use of an old-fashioned pen and ink.
77 One whose interests lie exclusively in IT, (almost) to the exclusion of everything else.
78 Eastlake and *Niles Secure XML* 470.

data formats such as XML[79] and XBRL[80] not only provide more security with regard to electronic signatures, but also provide criteria by means of which the evidential weight of such evidence may be weighed.

ICT security involves a careful evaluation of the security risks to the user's ICT assets, resources and activities and involves the formulation and quantification of countermeasures.[81] The latter should be embodied in an enterprise-wide IT security policy and the Human Resources Division concerned should see to it that acceptance of the obligations in terms of such a policy forms part of an employee's conditions of service.

Standards are of the greatest importance in achieving adequate IT security, and in this regard ISO[82] 17799 plays a pivotal role. At the same time adherence to such standards may also help provide reliable proof in disputed matters.[83] It is also important that the procedures in creating electronic signatures be accredited by an authoritative body. The South African Accreditation Authority (SAAA) has now accredited a procedure by means of regulation.[84]

Coming to Criminal Law - this legal field usually constitutes the last resort to desperate data "owners" when security measures have proved to be insufficient. When surveying the panoply of legislation in this era the question arises as to exactly what public interest is being protected by a particular statute.

---

79 eXtensible Markup Language. See Van der Merwe 2010 *THRHR*.

80 eXtensible Business Resources Language. See Van der Merwe 2011 *THRHR*.

81 See Van der Merwe *et al Information Communications Technology Law* 64 and the sources quoted.

82 International Standards Organisation.

83 If such a standard is an international one, it would also address problems of jurisdiction and proof where overseas parties are involved.

84 GN 504 in GG 29995 of 20 July 2007 (*Regulations relating to Authentication Service Providers*). See also Papadopoulos and Snail *Cyberlaw@SA* 123; Van der Merwe *et al Information Communications Technology Law* 127. A Centurion-based South African firm has recently implemented the standard successfully and obtained permission from the Department of Communications to advertise their advanced digital signatures as ECT-compliant.

Normally the criminal law allows the state to intervene against one of its citizens who has proved to be a danger to his (or her) fellow citizens and needs to be removed from society for a while. This would serve a number of purposes at the same time. In the first place the individual would (hopefully) be deterred by the punishment from ever transgressing again in the future.[85] In the second place society, when taking note of the punishment imposed, would be satisfied that justice has been done and would not be tempted to take the law into its own hands.[86] Thirdly, members of that society would normally decide that "crime does not pay" and refrain from embarking upon a similar course of criminal conduct.[87] Finally, since the convicted accused is languishing in prison while serving, for instance, "three life sentences",[88] he is prevented from committing any further crimes (at least outside of prison).

It seems, therefore, that the protection of its citizens against crime should be the main aim and justification of state-imposed punishment. Applying this principle to the field of information implies that the state should criminalise acts such as hacking into someone's computer, or obtaining money from duped Internet users who think they are helping a Nigerian user obtain a sum of money allegedly owed to him by the government, an unemployment insurance fund or a legacy from some long-forgotten relation.

The present article does not intend to focus on financial crimes in general, however, but specifically on crimes where information is obtained in an unauthorized manner. A good example would be the action described as "phishing", where the criminal's aim is not so much to obtain money directly, but to obtain information that would enable him (or her) to gain access to the victim's Internet accounts at a later stage.

---

85 The aim of Individual Deterrence.

86 The aim of Retribution.

87 The aim of General Deterrence.

88 It seems that the abolition of the death penalty in South Africa has led to inflation as far as prison terms are concerned. One often hears of a "double" or "triple" life sentence being imposed by courts. In practice, however, prisoners usually serve only a fraction of their prison terms behind bars, mostly being released on an early parole.

Inadequate passwords or password procedures play a major role in the type of crime presently under discussion.

Suppose, however, that an incursion is made not so much for the purposes of pecuniary gain but in order to obtain information that might be valuable for an entirely different purpose. Mention has already been made above to the case of Mr Snowden, who broke through the security systems of American government departments and thus obtained strategic government information that he then made openly available on the Internet. The almost hysterical reaction from the government makes one wonder whether this matter really turned on normal law enforcement with a view to protecting American citizens, or whether the state was annoyed and discomfited because its own "strategic" and secret information had been accessed. Throughout this drama, Snowden claimed that it would be to the public benefit to know what kind of personal information the government was storing for its own benefit, not for that of its citizens.

The conclusion seems inescapable that the real "victims" of Snowden's "crimes" were not the individual citizens of the United States, but powerful government officials (some of them quite high up in the hierarchy) who did not want to be exposed to the glare of open, constitutional, public scrutiny.

Similarly, Bradley Manning has been convicted in connection with a breach of military and diplomatic secrets. In 2010 Manning, a 22-year old army intelligence analyst serving in Iraq, had sent thousands of documents that had been classified as secret by the American military to the website "Wikileaks", which had published them electronically. Manning did not believe that he had been acting unlawfully, writing that "Information should be free", before his later capture.[89]

[89] Quoted in Scherer 2013 *Time* 18ff.

Aaron Swartz, a computer programmer, was to be charged for downloading academic papers from MIT and JSTOR.[90] However, the 26-year old committed suicide before he could be brought to trial.[91] Again, Swartz seemed to be more of a "conscientious objector" than a common criminal - he had downloaded and released publicly millions of federal court documents in protest of a per-page fee for access to such documents, a tariff that would make research much more expensive.

It is significant that these three "criminals" were all still in their 20s and probably did not believe that they were doing wrong - or at any rate, that the end justified the means. In South Africa "political or other not ignoble motives" may serve as an extenuating circumstance. Nonetheless, the young offenders described above all faced "having the book thrown at them" as far as their sentences were concerned. *Time* magazine[92] states that according to a poll recently conducted by the magazine, 53% of respondents were of the opinion that Snowden should be prosecuted, compared to a mere 28% who thought that he should just be "sent on his way". However, once the responses are limited to Snowden's own age group (of 18 to 34-year olds), 43% felt that he should not be prosecuted.

In commentary published with the above *Time* article,[93] mention is made of a shift in judicial views as far as weighing up security against privacy considerations is concerned. During the First World War the *Espionage Act* of 1917 was enacted in the United States and President Woodrow Wilson called for this law to be used in order to suppress criticism of the country's participation in this war.

The majority of the Supreme Court gave effect to this appeal from the Executive and convicted several antiwar critics in terms of the Act. However, in the case of *Abrams*

---

90 Short for "Journal Storage" - a digital library of academic articles, books and other primary sources - see JSTOR 2014 http://www.jstor.org.

91 Scherer 2013 *Time* 22.

92 Scherer 2013 *Time* 22.

93 Scherer 2013 *Time* 24. The author is Jeffrey Rosen, the president and CEO of the National Constitution Centre.

*v United S*tates,[94] Justices Oliver Wendell Holmes Jr, and Louis Brandeis upheld a different minority view, saying that even loathsome opinions should not be suppressed unless these are so threatening that they should be checked in order to save the country. The latter opinion finally won the day in 1969 in the case of *Brandenburg v Ohio,*[95] where the court decided that there had to be both the intention to bring about as well as a likelihood of imminent violence before free speech could be suppressed.

In a follow-up on the same point discussed in the previous paragraphs, a later *Time* magazine article[96] delivered the following insightful commentary:

> The motivations of Manning and Snowden fall under the Ideology/Identification subset of the FBI's insider-threat category: "a desire to help an '"underdog"' or a particular cause". That cause is open government, and to its champions, Manning and Snowden are heroes whose leaks are a public service. What matters next may have less to do with the punishment that is meted out than with how many people with security clearances decide to follow in their footsteps.

The failure of a dispute resolution between two major United States software providers, Microsoft and Google,[97] on the one hand, and the American government on the other, has again highlighted the double role that a government might have to play in similar cases. On the one hand, it has the administrative power to weigh up interests and to see to it that justice is done to all. On the other hand, it might be a player itself in the information game, capable of misusing the position of trust that has been given to it. The excuse of protecting the security and safety of its citizens may be valid in some instances, but should not serve to hide extreme actions behind a veil of administrative obscurity.

A civil suit will now reportedly be brought by the two software houses against an order forcing them to comply with secret requests by the American government (in

---

94 *Abrams v United States* 250 US (1919) 616.
95 *Brandenburg v Ohio* 395 US (1969) 444.
96 Anon 2013 *Time* 13.
97 Anon 2013 http://www.news24.com/Technology/News/Microsoft-joins-Google-in-US-spying-suit-20130831.

terms of the *Foreign Intelligence Survey Act*) for private user data. The plaintiffs want "to be able to provide users with better insight into what information the government gets its hands on". On the other hand, the government insists that such requests are perfectly lawful and "have helped thwart dozens of terrorist attacks".

3.3 Uganda

In a spate of new internet-related legislation during 2011, Uganda passed a *Computer Misuse Act*,[98] an *Electronic Signatures Act*[99] and an *Electronic Commerce Act*.[100] These new Acts should bring the country into the age of electronic commerce, provided that the necessary training is done and the legislation is properly enforced.

Taken in isolation not much fault can be found with the new trio of laws, but a fair amount of mutual overlap seem to exist between them. Thus Part V - (Miscellaneous) of the *Electronic Commerce Act* contains a number of provisions that create offences, which should perhaps rather have been enacted under the *Computer Misuse Act*.[101]

In turn, the latter Act contains a number of evidential and procedural provisions in Part III (Investigations and Procedures) and Part V (Miscellaneous). Seeing that Part V contains some really important provisions concerning criminal procedure and evidential admissibility, these other provisions are probably not correctly placed under this heading.

Part IV of the Act (Computer Misuse Offences) sets out the statutory offences and follows the pattern of the South African Act, but only up to a point. It then proceeds

98 *Computer Misuse Act* 2 of 2011.
99 *Electronic Signatures Act* 7 of 2011.
100 *Electronic Commerce Act* 8 of 2011.
101 Alternatively the E-commerce enactment could have contained the necessary crime provisions, as with South Africa's ECT Act.

to criminalise actions such as involvement in child pornography,[102] "cyber harassment", "offensive communication" and "cyber stalking".

While most of the above seem to be progress in the right direction, the Act also contains a more controversial Section 20 on "Enhanced Punishment for offences involving protected computers". This section places the onus on an accused to prove that he or she did not know that the computer concerned was "protected". Subsection 20(2) defines this type of machine as follows:

> For the purposes of subsection (1), a computer is treated as a "protected computer" if the person committing the offence knows or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for-
> (a) the security, defence or international relations of Uganda;
> (b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;
> (c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities or public key infrastructure; or
> (d) the protection of public safety including systems related to
> essential emergency services such as police, civil defence and medical services.

In connection with the onus of proof, subsection 20(3) provides as follows:

> For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2).

With all due respect, the above section seems to load the dice too heavily in favour of the State. Not only does the accused bear the full onus of proof with regard to his (or her) own innocence, but *culpa*[103] seems to be sufficient for a conviction. By including data used in connection with "public utilities" in the enhanced punishment-provision, a court may now "throw the book" at sleepy employees of municipal or state utilities - hardly the targets of such a drastic "spy" provision.

---

102 Which South Africa deals with in separate legislation.
103 "Ought reasonably to have known".

The *Electronic Signatures Act* introduces the PKI-infrastructure as the prescribed method of encryption. This is a standard that has been accepted all over the world and not much can be criticised about the standard itself. Again the only concern seems to be if Uganda possesses the necessary skilled manpower and sophisticated hardware in order to obtain the necessary qualified expert evidence regarding findings made after using such systems.

4 Conclusion

The survey done above on the international legal position (especially in the United States) as well as on certain areas of South African and Ugandan law is not yet complete. The thoughtful reader would, however, have perceived already how the arrival of digital information has changed the entire background against which the law has to operate. The Internet is not only a new global marketplace, but digital police ought to be patrolling the precinct to prevent digital crime. On the other hand, it would be very easy for the State to overreach its powers in this regard and to start using this new medium as a useful spying tool.[104] The traditional, finely tuned balance between the powers of government and those of its citizens are being shaken and should be addressed by visionary law making and enforcement. A third force that the present article has not had the time to dissect and analyse properly is the power of the digital marketplace. Citizens might not mind giving up their right to privacy, provided that they get paid for doing so.

Even though academics might have time to study and carefully dissect the changes brought about by the information revolution, most practitioners simply do not have the time to study these quantum changes that are taking place in the field of IT, and to think through their full implications for the law.

[104] Here one thinks of "Big Brother" (the over-active government) in works such as George Orwell's *1984*.

In this regard, not only universities but also the government, the organised legal profession[105] and the security and IT industries ought to sit down together and decide on the way forward as far as the interface between digital information and the law is concerned. An overhaul and consolidation of existing legislation is needed, but the legislature should also be enabled to react much quicker to the fast-moving digital world.[106] Not only legal practitioners should be involved in this collaboration, but also experts from the security and IT industries. Part of the programme should concern the planning and financing of the necessary training. Standards need to be agreed upon, especially to provide reliable proof in highly technical cases.

One strategic advantage locally is that overseas countries, some of them much further along the digital path than Africa, have been confronted with exactly the same problems, but for a much longer time than we have. The world has become a much smaller place and this continent may learn a lot from its overseas neighbours as far as best practices are concerned. Comparative research would therefore also be of the utmost importance in this regard.

Speaking from an international perspective, however, traditional legal solutions for problems with regard to jurisdiction on the Internet, for instance, are badly in need of a rethink. International standards and treaties between countries could go some way towards addressing this problem. We should start thinking outside of traditional boundaries in more ways than one.

As for citizens' tussle with their own governments with regard to their personal information - the old aphorism might still hold some truth: "If ye sup with the devil, use a long spoon."

---

105 Here one thinks of the Bar and Sidebar, Justice Training etc.

106 The over-long process attendant on the promulgation of South Africa's privacy legislation constitutes a prime example.

BIBLIOGRAPHY

Literature

Anon 2013 *Time*

Anon "Blown Whistle: What the Manning Verdict Means" 2013 *Time* 12 Aug 13

Brandeis and Warren 1890 *Harv LJ*

Brandeis L and Warren S "The Right to Privacy" 1890 *Harv LJ* 193 (downloaded from http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html on 4 September 2013)

Buys *Cyberlaw@SA* 1999

Buys R (ed) *Cyberlaw@SA* (Van Schaiks Pretoria 1999)

Buys *Cyberlaw@SA* 2004

Buys R (ed) *Cyberlaw@SA* 2nd ed (Van Schaiks Pretoria 2004)

Claasen *Beeld*

Claasen C "'Selfone kan tot Groot Oproer Lei'" *Beeld* (10 November 2013) http://www.beeld.com/nuus/2013-11-10-selfone-kan-tot-groot-oproer-lei accessed 17 February 2014

Eastlake and Niles *Secure XML*

Eastlake DE and Niles K *Secure XML: The New Syntax for Signature and Encryption* (Addison-Wesley Boston 2003)

Hofman *Cyberlaw*

Hofman J *Cyberlaw* (Ampersand Press Cape Town 1999)

Hofman "South Africa"

Hofman J "South Africa" in Mason S *Electronic Evidence: Disclosure, Discovery and Admissibility* (LexisNexis/Butterworths London 2007) 483

Neethling and Potgieter *Law of Delict*

Neethling J and Potgieter JM *Law of Delict* 6th ed (LexisNexis Durban 2010)

Papadopoulos and Snail *Cyberlaw@SA*

Papadopoulos S and Snail S (eds) *Cyberlaw@SA* 3rd ed (Van Schaik Pretoria 2012)

SALRC *Privacy and Data Protection*

SALRC *Privacy and Data Protection - Discussion Paper 109, Project 124* (The Commission Pretoria 2005)

Scherer 2013 *Time*

Scherer M "Geeks who Leak" 2013 *Time* 24 Jun 18-25

Schmidt and Rademeyer *Bewysreg*

Schmidt C and Rademeyer H *Bewysreg* 4th ed (Butterworths Durban 2000)

Schmidt and Cohen *New Digital A*ge

Schmidt E and Cohen J *The New Digital A*ge (John Murray London 2013)

Scholtz 2013 *Beeld*

Scholtz L "Erger as die KGB - VSA breek eie reëls" *Beeld* 2013 8 November

Tapper *Computer Law*

Tapper C *Computer Law* (Longman London 1978)

Van der Merwe 1983 *Obiter*

Van der Merwe DP "Computer Crime" 1983 *Obiter* 124-133

Van der Merwe 1985 *SACC*

Van der Merwe DP "Diefstal van onliggaamlike sake met spesifieke verwysing na rekenaars" 1985 *SACC* 129-141

Van der Merwe *Computers and the Law* 1986

Van der Merwe DP *Computers and the Law* (Juta Cape Town 1986)

Van der Merwe 1994 *Obiter*

Van der Merwe DP "Documentary evidence (with specific reference to the Internet)" 1994 *Obiter* 64-84

Van der Merwe *Computers and the Law* 2000

Van der Merwe DP *Computers and the Law* 2nd ed (Juta Cape Town 2000)

Van der Merwe 2007 *THRHR*

Van der Merwe DP "Information technology crime - a new paradigm is needed" 2007 *THRHR* 309-319

Van der Merwe *et al Information Communications Technology Law*

Van der Merwe DP *et al Information Communications Technology Law* (LexisNexis Durban 2008)

Van der Merwe 2010 *THRHR*

Van der Merwe DP "The current position regarding digital evidence and XML as a possible solution" 2010 *THRHR* 81-92

Van der Merwe 2011 *THRHR*

Van der Merwe DP "XBRL and the law: the legal implications of mark-up languages" 2011 *THRHR* 418-431

Zimmermann *PGP Source Code and Internals*

Zimmermann P *PGP Source Code and Internals* (MIT (Massachusetts Institute for Technology) Press 1995)

Case law

Abrams v United States 250 US (1919)

Brandenburg v Ohio 395 US (1969)

Financial Mail (Pty) Ltd v Sage Holdings Ltd 1993 2 SA 453 (SA)

Janit v Motor Industry Fund Administrators (Pty) Ltd 1995 4 SA 293 (A)

National Media Ltd v Jooste 1996 3 SA 262 (A)

O'Keefe v Argus Printing and Publishing Co Ltd 1954 3 SA 244 (C)

S v De Villiers 1993 1)SACR 574 (Nm)

S v Harper 1981 1)SA 88 (D)

S v Howard (Johannesburg Regional Magistrates Court) unreported case number 41/258/02

Legislation

South Africa

Constitution of the Republic of South Africa, 1996

Electronic Communications and Transactions Act 25 of 2002

National Credit Act 34 of 2005

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

Uganda

Computer Misuse Act 2 of 2011

Electronic Commerce Act 8 of 2011

Electronic Signatures Act 7 of 2011

Government publications

GN 504 in GG 29995 of 20 July 2007 (*Regulations relating to Authentication Service Providers*)

GN 888 in GG 35821 of 28 October 2012 (*Electronic Communications and Transactions Amendment Bill*)

General Intelligence Laws Amendment Bill, 2011 [B25-2011]

Protection of State Information Bill, 2010 [B6-2010]

International instruments

Convention on Cybercrime (2011)

Draft Convention on Cyber-legislation in Africa (2012)

Draft EAC Framework for Cyber-laws (Phase I) (2008)

EAC Cyber-laws Framework (2009)

SADC Draft Model Law on Crime and Cybercrime (2012)

Internet sources

Anon 2013 http://www.news24.com/Technology/News/Microsoft-joins-Google-in-US-spying-suit-20130831

Anonymous 2013 *Microsoft Joins Google in Spying Suit* http://www.news24.com/Technology/News/Microsoft-joins-Google-in-US-spying-suit-20130831 accessed 4 September 2013

JSTOR 2014 http://www.jstor.org

JSTOR 2014 *JSTOR Home Page* http://www.jstor.org accessed 28 February 2014

Napolitano 2013 http://reason.com/archives/2013/11/07/how-can-the-nsa-spy-on-merkel-the-pope-t

Napolitano A 2013 *How can the NSA Spy on Merkel, the Pope, the UN and the Rest of Us?* http://reason.com/archives/2013/11/07/how-can-the-nsa-spy-on-merkel-the-pope-t accessed 7 November 2013

LIST OF ABBREVIATIONS

EAC	East African Community
ECT	Electronic Communications and Transactions Act
FBI	Federal Bureau of Investigation
GCHQ	United Kingdom's Government Communications Headquarters
GILA	General Intelligence Laws Amendment Bill
Harv LJ	Harvard Law Journal
ICT	Information and Communications Technology
IP	Intellectual Property
ISO	International Standards Organisation
JSTOR	Journal Storage
MIT	Massachusetts Institute for Technology
NSA	United States' National Security Agency
PKI	Public Key Infrastructure
PGP	Pretty Good Privacy
POSI	Protection of State Information (Bill)
SAAA	South African Accreditation Authority
SACC	South African Journal of Criminal Law and Criminology
SADC	South African Development Community
SALRC	South African Law Reform Commission
THRHR	Tydskrif vir die Hedendaagse Romeins-Hollandse Reg
UHRC	Ugandan Human Rights Commission
XBRL	(e)Xtensible Business Reporting Language
XML	(e)Xtensible Markup Language