Examining the Nexus Between ICTs and Human Rights in Africa: The Case of South Africa*

Sven ABRAHAMSE**

* Prepared for an International workshop on the Nexus between ICTs and Human Rights in Africa Organized by Human Rights and Peace Centre, Faculty of Law, Makerere University, Uganda. 2nd to 4th April 2009 with assistance from the International Development Research Centre, Ottawa, Canada.

** Researcher University of Cape Town, South Africa

Understanding of the Terms of Reference

My understanding of the Terms of Reference for this Scoping Project

1. It requires a in-depth analysis of privacy issues in South Africa
2. An view of Censorship currently
3. How our Society handles the issues of Freedom of expression and Hate speech

Privacy

South African Jurisprudence draws from two major sources, the first being our constitution[1] and the common law.

The South African Constitution

South Africa has a historical basis of the security services not respecting the privacy rights of individuals during the armed struggle. Article 14 of the SA constitution guarantees a general right to privacy in South Africa. This right can be limited in terms of Article 36 of the constitution which allows for the limitation of any right by a law in a just and modern society

From a constitutional level section 14[2] of our constitution states:

> Everyone has the right to privacy which includes the right not to have
> 1. Their person or home searched
> 2. Their property searched
> 3. Their possessions searched
> 4. The privacy of their communications infringed

This should be contrasted with section 36(1)[3] of the South African constitution, which allows for limiting any right:

> "Only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and

[1] Act 101 of 1996
[2] Section 14(d) of the South African Constitution, Act 108 of 1996
[3] Section 36 of the South African Constitution, Act 108 of 1996

> democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including
> 1. The nature of the right
> 2. The importance of the purpose of the limitation
> 3. The nature and extent of the limitation
> 4. The relation between the limitation and its purpose, and
> 5. Less restrictive means to achieve the purpose"

In *Bernstein and Others v Bester and Others,*[4] Ackerman J in dicta 68 defined privacy as "Privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly".

However in *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) ltd and others,*[5] the court held

> [T]hat the right to privacy guaranteed in s 14 of the Constitution did not relate solely to the individual within his or her intimate space. When persons moved beyond this established 'intimate core', they still retained a right to privacy in the social capacities in which they acted. Thus, when people were in their offices, in their cars or on mobile telephones, they still retained a right to be left alone by the State unless certain conditions were satisfied. Wherever a person had the ability to decide what he or she wished to disclose to the public and the expectation that such a decision would be respected was reasonable, the right to privacy would come into play.

It appears that this right to privacy is further qualified and the protections granted by the constitution is not similar in its scope and application. Langa DP in *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) ltd*[5] and others at dicta 18 states the right to privacy flows from the value placed on human dignity by the constitution but since juristic persons are not bearers of human dignity it appears on the face of it that juristic persons have less protection of this under the south African constitution. He goes on to say

---

[4] BERNSTEIN AND OTHERS v BESTER AND OTHERS NNO 1996 (2) SA 751 (CC)

[5] Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others 2001 (1) SA 545 (CC).

> Exclusion of juristic persons would lead to the possibility of grave violations of privacy in our society, with serious implications for the conduct of affairs. The State might, for instance, have free license to search and seize material from any non-profit organization or corporate entity at will. This would obviously lead to grave disruptions and would undermine the very fabric of our democratic State. Juristic persons therefore do enjoy the right to privacy, although not to the same extent as natural persons. The level of justification for any particular limitation of the right will have to be judged in the light of the circumstances of each case. Relevant circumstances would include whether the subject of the limitation is a natural person or a juristic person as well as the nature and effect of the invasion of privacy.

Sachs J in *Mistry v Interim Medical and Dental Council of South Africa and others*[6] at dicta 48 makes a finding that "The first is that a right to informational privacy is covered by the broad protection of privacy guaranteed by s 13. " Sachs J refers to section 13 of the interim constitution and the privacy protection clause of section 13 was later incorporated into the current South African Constitution as section 14

Justification of the limitations clause requires proportionality between the degree of infringement of privacy and the purpose of the infringement.

Section 32 of the South African Constitution[7] guarantees Access to information

> 1. Everyone has the right of access to
> a. any information held by the state; and
> b. any information that is held by another person and that is required for the exercise or protection of any rights.
> 2. National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state.

Section 36(1) of the constitution again limits this and the limit is implemented via the Access to Information Act, Act 2 of 2000.

---

[6] Mistry v Interim Medical and Dental Council of South Africa and others 1998 (4) SA 1127 (CC)

[7] Section 32 of the South African Constitution, Act 108 of 1996

The Promotion to Access to Information Act, Act 2 of 2000

The basic thrust of this act is to carry out the constitutional right to access of information with section 32 of the constitution.
Section 9(b) introduces a series of limitations including:

- Limitations aimed at reasonable protection of privacy
- Commercial confidentiality
- Effective, Efficient and good governance

The Act promotes data protection by allowing individuals access to their personal information while banning access to third parties to the information which would lead to unreasonable infringement.

The Act contains several rules about correcting personal information until the republic adopts a data protection act. This can directly be mapped back to the draft protection of personal privacy act and the privacy rules of the National Credit Act.

Access to information

The Act allows individuals access to their own data.[8] It also provides various grounds for refusing a request[9]

Mandatory protection of privacy of a third party

The act provides for compulsory protection of information about a third-party.[10] A public or private body must refuse a request for access to a record if its disclosure would involve an unreasonable disclosure of personal information about a third-party.
Epstein AJ in *Water Engineering and Construction (Pty) Ltd v Lekoa Vaal Metropolitan Council at 605 (c)* states that:

---

[8] Sections 33 -44 and 62 – 64, Act 2 of 2000
[9] Section 11 and Section 50 – also look at the definition of "personal requester" in Section 1 of the act
[10] Water Engineering and Construction (Pty) Ltd v Lekoa Vaal Metropolitan Council. 1999 (9) BCLR 1052 (W)

> In my view, it cannot be that unrestricted access was intended by the framers of the constitution. If this was so, unscrupulous persons would be able to exploit this provision for their own selfish reasons. A Balance must be achieved between the rights to access to documents and the rights to privacy entrenched in section 14 of the Constitution.

There is a two-part test to see if this protection is applicable.

- Firstly, for this ground to be applicable one has to look at whether the information is personal as defined in section one.[11]
- Secondly, a determination needs to be made around the "*unreasonable- ness*" of such a request.

The act provides some exceptions to the compulsory protection of third-party information rule.

- If an individual has consented in writing to the disclosure of his information to the requester concerned
- If the information is already publicly available
- The individual's information was given to a private or public body by an individual to whom it relates and the individual was informed the information belongs to a class of information that would be made available to the public. This amounts to implied consent
- The medical records of an individual sought by his healthcare professional of record and if the individual is under the age of 18 and or if the individual is incapable of understanding the nature of this request because of incapacity, mentally or medically.
- The information belongs to an individual who is deceased and the requester is the next of kin or is making the request with the written permission of the next of kin. This provision applies to individuals that have been dead for less than 20 years but I fail to see why this time-frame is applicable as people who are deceased do not have personality rights and therefore could not have an expectation to a right of privacy.

11

- The information belongs to a person that is or has been an official of a private or public body and the information that is sought relates to the position or job of that person.

Correction of personal information

Section 88[12] of the Act provides that if no rules exist for correcting personal information in a record held by a private or public body, *"that body must take "reasonable steps" to establish an "acceptable and proper" internal measures providing for such correction."*[13]

South African Acts that could have an influence on the general right to privacy in South Africa

Other than our constitutional framework there is other legislation that has the potential to limit the right of privacy in the context of this paper

The interception and Monitoring Prohibition Act, Act 27 of 1992

This act has as one of its general rules that make it an offence to intercept any communication that will be sent over a telephone line or a telecommunications line. It does allow for directing the judicatory by the application of a warrant based on probable cause, "that a serious offence has been committed or is being or will probably be committed, which cannot be investigated in any other manner and of which the investigation in terms of the act is necessary or that the security of the republic is threatened or the gathering of information concerning a threat to the security of the Republic is necessary

The Electronic Communications and Transaction Act, Act 25 of 2002

This act deals in principle with the content of any electronic communication in South African jurisprudence. For the first time in South African Jurisprudence

[12] The Access to Information Act , Act 2 of 2000
[13] The implementation of the data protection provisions of the NCA , act 23 of 2005 now provides in law for such a mechanism

this act creates a doctrine of functional equivalence. This allows for all actions except for of two (contracts of sale of property and contracts if marriage) will be equivalent to its real world action. Therefore e-mail which is a fast medium now has the same weight in law as a document and came be used with the same evidentiary value as a document.

Data Protection in the ECT Act

Protecting personal information in the ECT act applies only to:

- Natural Persons,[14]
- Information that has been obtained via electronic means,[15]
- After the introduction of this act

The ECT act does not regulate access to information. The act also does not impose legally binding duties on data controllers but creates a voluntary framework that data controllers may subscribe to and the act adds the subscriber either completely subscribes to the act or not[16]

The data subject and the data controller must reach an agreement to the rights and duties of the breach of the principles.[17]

This framework has several principles of data protection and section 51 of the act lists the 9 principles the data controller must subscribe to. These principles can directly be mapped back to both the OECD framework and the Council of Europe's framework.

Written Consent

The express written consent of the data subject is needed. Inferred consent therefore is not allowed. Electronic consent (by clicking a website as an

[14] This should be contrasted with the provisions of the AIA (Natural persons/ Private versus public bodies)
[15] This should be contrasted this with the AIA and its provisions to apply to all types of records
[16] Section 50(3) of the ECT Act 25 of 2002
[17] Section 50(4) of the ECT Act 25 of 2002

example) would qualify as written consent. Consent is however not needed if the data controller must by law process the information.

Lawful purpose

Personal information may only be processed for the lawful purpose for which it is needed. This principle is directly mapped back to the principles of purpose specification and minimalism of the APEC, OECD and EU frameworks.

Disclosure in Writing

The data controller must disclose in writing to the data subject the specific purpose for which the personal information is being sought. This is to enable the data subject to see if the data processing was lawful. That is whether a legitimate interest is being protected and whether processing the data was necessary. This again maps directly back to the principle of specific purpose.

No Secondary use

The data controller may not use the collected data for any secondary purpose without the express written permission of the data subject or unless it is needed to do so by law.

Record Keeping

The data controller must keep a record of all personal information and the purpose for which it was collected for as long as the information is used and for 12 months after the last use of the data.

Record keeping of third party request

This principle is directly linked to the previous one in the controller must keep a record of any third-party to whom personal information was disclosed, what information was disclosed, and the purpose for which it was disclosed. The ECT act does not create a mechanism for correcting inaccurate information. This is corrected in the data protection rules of the NCA act.

Non – Disclosure

A data controller may not disclose any personal information to any third-party, unless needed or allowed by law or if the data subject specifically allows the disclosure in writing. This requirement maps directly to the limitations of disclosure of the OECD's framework.

The Regulation of Interception of Communications and Provision of Communication Related Information Act, Act 70 of 2002 (RICA)

This Act regulates the interception of communications, monitoring radio signals and radio-frequency spectrums and providing communication related information. The Act contains a general prohibition[18] against the interception of any communications. It also regulates the application for interception of communications and provision of communication- related information under certain circumstances. It regulates applications for interception and it regulates law enforcement where interception of communications is involved. Structurally RICA is not limited to the rules of the Act itself but supplemented by a directive, a schedule and four proclamations.

The Directive prescribes the technical and security needs related to the interception and routing of communications.

Schedule A deals with fixed line telecommunications operators

Schedule B & C deal with mobile cellular providers and Internet service providers respectively.

There are several classes of exceptions that could be raised against implementing this Act, namely

[18] Section 2 of the act states "No person may intentionally intercept or attempt to intercept or authorize or procure any other person to intercept or attempt to intercept at any place in the republic any communication in the course of its occurrence or transmission"

Section 2 of the Act states "*No person may intentionally intercept or attempt to intercept or authorize or procure any other person to intercept or attempt to intercept at any place in the republic any communication in the course of its occurrence or transmission."*

General Exception

- The approved person who carries out an intercept direction or aid with the execution of it may intercept any communication, to which such interception direction relates,[19]
- Any communication may be intercepted by one of the parties of that communication provided such communication is not intercepted for committing an offence,
- Any person may intercept any communication if one of the parties to the communication has given their prior consent to such interception in writing,[20]
- Any person may intercept any indirect communication in the course of carrying on a business provided that certain requirements are met.[21]

Business Exception

The Business exception allows employers to intercept communications of their employees without having to get their permission first. The act defines several conditions that needs to be met for the interception to be considered "lawful"

Sec 6(1) of the Act allows for indirect communication to be intercepted if:

- It relates to transaction being entered into in the normal course of the business
- It otherwise relates to the business
- It otherwise takes place in the course of that business

[19] Sec 3 (a) and (b) if The Regulation of Interception of Communications and Provision of Communication – Related Information Act (RICA), Act 70 of 2002

[20] Section 5(1) of The Regulation of Interception of Communications and Provision of Communication – Related Information Act (RICA), Act 70 of 2002

[21] Sec 6(1) and (2) of The Regulation of Interception of Communications and Provision of Communication – Related Information Act (RICA), Act 70 of 2002

Section 6(2) makes the interception of the indirect communication "lawful" if

- The system controller gave his consent or his implied consent,[22]
- The communication is intercepted for a legitimate purpose with is limited to
- The Establishing existing facts
- Investigating the unauthorized uses of the telecommunication system
- Securing effective operation of the system
- The use of the telecommunication system concerned is provided for wholly or partly in connection with that business[23]
- If the system controller made reasonable efforts to inform individuals in advance that their indirect communications may be intercepted or if such indirect communication[24] is intercepted with the express or implied consent of the person who uses the system

The National Strategic Intelligence Act as Amended, Act 39 of 1994

This Act defines the functions about intelligence gathering. The Act provided for the "gathering, correlation, evaluation and analysis of domestic, foreign crime and foreign military intelligence by the NIA, SASS, SAPS and SANDF". These are carried out to "identify any threat or potential threat to the security of the Republic or its people". Section 5 (2) of the Act allows for a judge to issue a warrant to collect information that has a bearing on national strategic intelligence.

The National Prosecuting Authority Amendment act, Act 61 of 2000

This Act allows the directorate of special operations to intercept and monitor communications. This is a limited authority in section 28(1) of the National Prosecuting Authority Amendment Act 61 of 2000.

---

[22] Sec 6(2)(a) of the Regulation of Interception of Communications and Provision of Communication – Related Information Act (RICA), Act 70 of 2002
[23] Sec 6(2)(c) of the Regulation of Interception of Communications and Provision of Communication – Related Information Act (RICA), Act 70 of 2002
[24] Sec 6(2)(d) of the Regulation of Interception of Communications and Provision of Communication – Related Information Act (RICA), Act 70 of 2002

The directorate has to be able to show a judge that reasonable ground such as suspicion of an offence and that monitoring is the last resort.

The Interception and Monitoring Prohibition Act, Act 27 of 1992

This Act has as one of its general provisions that make it an offence to intercept any communication that will be transmitted over a telephone line or a telecommunications line. It does allow for the direction of the judicatory by way of the application of a warrant based on probable cause, "that a serious offence has been committed or is being or will probably be committed", which cannot be investigated in any other manner and of which the investigation in terms of the Act is necessary or that the security of the republic is threatened or the gathering of information concerning a threat to the security of the Republic is necessary

The Electronic Communications Act, Act 36 of 2005

Chapter 13, Section 76 (4) Electronic communications network service licensees and electronic communications service licensees must—
(a) Carry communications to 112 Emergency Centres and from 112 Emergency Centres to emergency organisations; and
(b) Make automatic number identity, such as caller line identity, and automatic location identity available to 112 Emergency Centres.

Directs licensees and service providers to supply personal information to the 112 emergency centre in contravention of any other legislation and
Chapter 13, Section 76 (5) the obligation imposed on licensees in terms of subsection (4) (b) supersedes any request by a subscriber to withhold their identity or location, which may be permitted under any applicable law or licence condition.

Chapter 13, Section 76 (6) Licensees are exempted from liability for all claims arising out of acts done in meeting their obligation under subsection (4) (b)
- Exempts the service provider from any legal liability in this matter.

The National Credit Act, Act 34 of 2005

The National Credit Act is in essence a consumer protection act, which aims to regulate the market in consumer credit principally by regulating access to credit and preventing unfair business practices.

Section 68, Chapter 4, Part B of the National Credit Act provides:

1. "Any person who, in terms of this Act, receives, compiles, retains or reports any confidential information pertaining to a consumer or prospective consumer must protect the confidentiality of that information, and in particular, must—
a. Use that information only for a purpose permitted or required in terms of this Act, other national legislation or applicable provincial legislation; and
b. Report or release that information only to the consumer or prospective consumer, or to another person—
i. to the extent permitted or required by this Act, other national legislation or applicable provincial legislation; or
ii. as directed by—
1. the instructions of the consumer or prospective consumer; or
2. an order of a court or the Tribunal.
2. Failure by a credit bureau to comply with a notice issued in terms of section 55, in relation to this section, is an offence"

The Act creates a right to confidential treatment "confidential information"[25] received or retained in terms of the act.

This confidentiality must be protected by its holder and must be used only for its lawful purpose and must be disclosed only to the person to whom it relates or to a third party as ordered by a competent court.

The Regulation of Credit Bureau information is the second part of the privacy protections of the Act.
Sections 70 – 73 imposes a number of obligations on a credit bureau in relation to "consumer Credit information"

[25] "Confidential information" means personal information that belongs to a person and is not generally available to or known by others; - line 40 the National Credit Act definitions, Act 34 of 2005

- A Bureau is needed to allow consumers free access to their credit information for purposes of verifying and challenging it.
- Credit Bureaus have a duty imposed by the act to take reasonable steps to verify the accuracy of consumer credit information[26]
- Access is controlled to only allow persons requiring stored information for a "prescribed purpose or a purpose contemplated in terms of the act"[27]
- Data retention is regulated by several conditions. Section 73 allows for the Minister to prescribe varying periods ranging from 1 year to 10 years

The application of this Act is much more detailed than the draft POPIA and there is no clarity on what the interplay between these two Acts would eventually be.

The Protection of Information Act, 1982

This Act comes from 1982. It deals with the classification and declassification of government information under the apartheid regime of the time and while this Act is rarely used these days, by being still not repealed it may be used to freeze the access of information under the PAIA

The National Archives of South Africa Act, 1996

This act establishes that all archival information older than 20 years should be made available to the public. This is in contrast with the rules of Sections 14 and 15 the PAIA which allows for the public and private bodies to self-determine which type of information is available. The Act also allows for the Archivist to make a determination that specific classes of information may be released earlier than the standard 20 years.

The Legal Deposit Act, Act 54 of 1997

[26] Section 70(2)(c) of Act 34 of 2005
[27] Section 70((2)(g)of Act 34 of 2005

This Act requires that all published materials to be deposited with specific state institutions such as archives and libraries. Section 7(3)[28] allows for the head of an institution of legal deposit to place limits on access to specific types of documents

The Protected Disclosures Act, Act 26 of 2000

This Act provides legal cover to employees that disclose information about illegal activities of their employers. The act has an exceptions clause that bans the disclosure by an employee of "*a breach of the duty of confidentiality of the employer towards any other person."* Information that is disclosed about "irregular conduct" depends on official interpretation.

The Promotion of Equality and Unfair Discrimination Act, Act 4 of 2000(PEUDA)

This Act was proclaimed to prevent and outlaw hate speech.

Chapter 2, Section 12 "Prohibition of dissemination and publication of information that unfairly discriminates

> 12. No person may—
> (a) Disseminate or broadcast any information;
> (b) Publish or display any advertisement or notice,
> that could reasonably be construed or reasonably be understood to demonstrate a clear intention to unfairly discriminate against any person: Provided that bona fide
> engagement in artistic creativity, academic and scientific inquiry, fair and accurate
> reporting in the public interest or publication of any information, advertisement or
> notice in accordance with section 16 of the Constitution, is not precluded by this section.
> "prohibits the publication of information that can be viewed as unfair discrimination.

The Exceptions clause Chapter 2 Article 5 of the PAIA

> Application of other legislation prohibiting or restricting disclosure
> 5. This Act applies to the exclusion of any provision of other legislation that—

[28] The Legal Deposit Act, Act 54 of 1997

(a) prohibits or restricts the disclosure of a record of a public body or private
body; and
(b) is materially inconsistent with an object, or a specific provision, of this Act" conflicts with the exceptions clause Chapter 1, Section 5(2) of PEUDA which holds "Application of Act
5. (2) If any conflict relating to a matter dealt with in this Act arises between this Act and the provisions of any other law, other than the Constitution or an Act of Parliament expressly amending this Act, the provisions of this Act must prevail.
.

This creates interplay between the right of access in PAIA and the right to equality in PEUDA

The Promotion of Administrative Justice Act, Act 3 of 2000(PAJA)

This Act implements article 33 of the South African Constitution. Taken with the PAIA it carries out promoting transparency values and accountability. PAJA manages decisions to grant or deny request for information under PAIA for governmental bodies.

The Minimum Information Security Standards of 1996

This is a government policy document that sets standards for classifying all government information. Information is classified into Restricted, Confidential, Secret and Top Secret. The nature of this document is fundamentally opposed to the right to freedom of information and the rules of the PAIA

The Draft Protection of Personal Information Act

The draft bill aims to regulate processing personal information by government and private groups.

Personal information is defined as "information about an identifiable natural person." This definition is similar to the matching definition in the Promotion of Access to Information Act.[29]

---

[29] 'personal information' means information about an identifiable individual, including, but not limited to-
(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-

Processing is defined as "any operation or any set of operations concerning personal information, including in any case the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as blocking, erasure or destruction of information."

Section 3 of this Act applies to-

(a) the fully or partly automated processing of personal information, and the non-automated processing of personal information entered in a record or intended to be entered therein;

(b) The processing of personal information carried out in the context of the activities of a responsible party established in the Republic of South Africa;

(c) The processing of personal information by or for responsible parties who are not established in South Africa, whereby use is made of automated or

---

being, disability, religion, conscience, belief, culture, language and birth of the individual;

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

(c) any identifying number, symbol or other particular assigned to the individual;

(d) the address, fingerprints or blood type of the individual;

(e) the personal opinions, views or preferences of the individual, except where they are

About another individual or about a proposal for a grant, an award or a prize to be Made to another individual;

(f) correspondence sent by the individual that is implicitly or explicitly of a private or Confidential nature or further correspondence that would reveal the contents of the Original correspondence;

(g) the views or opinions of another individual about the individual;

(h) the views or opinions of another individual about a proposal for a grant, an award or a

Prize to be made to the individual, but excluding the name of the other individual where

It appears with the views or opinions of the other individual; and

(i) the name of the individual where it appears with other personal information relating to

The individual or where the disclosure of the name itself would reveal information about

The individual,

But excludes information about an individual who has been dead for more than 20 years;

non-automated means situated in South Africa, unless these means are used only for forwarding personal information.

This condition shows the Act is not only applicable to computer databases but also to manual written documents.

The Act goes further by defining public and private bodies similar to their definition in the Promotion of Access to Information Act.

- A "public body" is an organ of state or any entity exercising public power or performing a public function.
- A "private body" is any other entity or individual except for individuals acting in their private capacity.

The Act therefore tries to regulate the personal information processing in our society, similar to the constitutional protection of privacy.

Section 4 of the Act excludes several categories from the operation of this Act This Act will not apply to information processing 'in the course of a purely personal or household activity' or to formerly personal information that has been permanently anonymized.

The Act protects information privacy by controlling processing personal information in ways that are different from those envisaged in the Act. The person responsible for processing personal information is responsible to comply with the eight general information protection principles, which arose from the OECD's framework on the limits of the transfer of personal information. Sensitive personal information is subject to specific protection.

Principles of information protection

The eight general information protection principles are as follows:

Limitation of processing.

- Processing of personal information must be lawful.

- The minimum data required should be collected.
- The data should be collected directly from the subject of the information rather than from third parties.

Purpose specification.

- Personal information must be collected only for a specific, clearly defined purpose.
- The subject of the information should be aware why the information is wanted.
- Information should only be held as only as long as its is needed

Further processing.

Information collected for one purpose must not be used for another.

Information quality.

The information that has been collected must be complete, not misleading, up-to-date and accurate.

Openness.

- Processing the information should be transparent
- Information should be collected openly so that the subject is aware of it.

Security of information.

Personal information must be protected against risks such as loss, unauthorized access, destruction, use, change or disclosure.

Individual participation.

The subject should be able to find out

- if their data is being processed

- to know the content of the information
- to correct wrong information

Accountability.

This principle places the responsibility for the data with the controlling party.

Special conditions for processing sensitive information

Part B of Chapter 3 of the Draft Bill lays down conditions for the lawful processing of special information that is stricter that the eight principles outlined above.

These conditions apply to information that concerns "a person's religion or philosophy of life, race, political persuasion, health or sexual life, or personal information concerning trade union membership, criminal behaviour, or unlawful or objectionable conduct connected with a ban imposed with regard to such conduct."

This information cannot be processed without the 'explicit consent' of the person concerned.

Common law approaches to data privacy

In South Africa we have a common law right to privacy, which is included under the right to privacy, which falls under the right to "dignitas."[30] This approach in fact is similar to article 12[31] of the Universal Declaration of Human Rights, article 17[32] of the International Covenant on Civil and Political Rights and of course article 8[33] of the European Convention on Human Rights.

The original action of "injuria" as developed by Roman Jurisprudence is still in use today in South African jurisprudence. It takes a broad view of the action and extends it to cover any situation in which an individual's dignity was unlawfully injured.

In the *S v Bailey*[34] the court held interfering with the plaintiffs right to privacy was lawful because it was justified by "some superior legal right", in this case the Statistics Act.[35] It therefore appears that in common law matters around data privacy the courts follow the approach of the body of case law at a constitutional level.

The Delict of invasion of Privacy

The South African Common law delict of invasion of privacy is based on the Roman and Roman Dutch law principles of Lex Aquilia and Actio Injuriarum.

Restating Invasion of Privacy as a Delict

Mc Quoid-Mason defines invasion of privacy as "*Any intentional and wrongful interference with another right to seclusion in his private life"*[36]

---

[30] See law of Delict 2nd ed, Neetling, Potgieter and Visser
[31] Article 12 of the Universal Declaration on Human Rights – Adopted and Proclaimed by the General Assembly Resolution 217 A(III) of 10 December 1948
[32] The International Covenant on Civil and Political rights – G. A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (NO. 16) at 52, U.N. Doc A/6316 (1996) , 999 U.N.T.S. 171 entered into force March 23, 1976
[33] The European Union Congress No. 108
[34] S v Bailey 1981 4 SA 187 (N)
[35] This Act was later replaced with the Statistics Act 6 of 1999
[36] Mc Quoid-Mason. The law of privacy in SA 1978

CORBETT CJ in *Financial Mail v Sage Holdings* held the unlawfulness of invasion of privacy should be judged in the light of a contemporary boni mores and general sense of justice of the community as perceived by the court[37]

This test is applied against "*current values and thinking of the communities"*[38]

Aminus Injuriandi[39] is the basis for an action for injuria. It has to be present for such an action to survive.

> When an act is done by a person with the definite object of hurting another in regard to his person, dignity or reputation or when an unlawful act is done as a means of effecting another object the consequences of which act such a person is aware will be to hurt another in regard to his person, dignity or reputation [36]

Clearly amicus injuriandi needs an intention to injure and a consciousness of wrongfulness. The concept intention to injure is further expanded by Jansen J in Ngubane[40] by his finding that Intention (dolus) does not exclude a finding of negligence (Culpa). He held that "*Dolus postulates foreseeing, but culpa does not necessarily postulate not foreseeing. A man may foresee the possibility of harm and yet be negligent in respect of that harm ensuing"*

Burchell[41] explains the categories suggested by Prosser can be used as guideline for implementing privacy law in South Africa.

Delict of invasion of privacy

Like the American definition, this action has four specific actions that may be used to prosecute an action of invasion of privacy namely Intrusion, Publication of Private Facts, Presentation of a person in a false light and Appropriation

---

[37] Financial Mail (Pty) Ltd and another V Sage Holdings Ltd and Another 1993 (2) SA 451 (A)
[38] Delonga V Costa 1989 (2) SA 857(A)
[39] The intention to injure
[40] Government of the Republic of South Africa v Ngubane 1971 (4) SA 367 (T)
[41] Burchell, Personality Rights and freedom of expression (1998)

Intrusion

This occurs where there is an intrusion "upon the plaintiff's physical solitude or seclusion."[42] McQuiod-Mason explains that an action for invasion of privacy lies where a person's peace and tranquillity in his home is disturbed by another telephoning or persistently calling to sell him something. I include sending large volumes of spam in this action.

If we hold that *Bernstein* defined the constitutional right to privacy also extends to man's interactions and surroundings it might be that an action to invasion of privacy would also lay when a person's mail server is spammed.

Neethling[43] suggest that an action may also lay when a person's mental repose has been disturbed by a flood of advertisements in mail or by telephone. Again I would argue that this could be extended to include also disturbing a person's mental repose by flooding his in box with spam e-mails.

Publication of Private Facts

An action of invasion of privacy may exist when private facts are published.

Presentation of a person in a false light

An action for invasion of privacy may exist when a person is exposed to publicity which places them in a false light in public. The publicity does not necessary even be defaming in nature.

Appropriation

An action of invasion of privacy may exist where a person's name, image or likeness is used without their consent.[44] This Delict is similar to the delict of

---

[42] William L. Prosser. Handbook of the Law on Torts. West Publishing Co., St. Paul, MN, 1971.
[43] Neethling et al – Law of Delict (2007)
[44] O Keeffe V Argus Printing and Publishing Company 1954 (3) SA 244 (C)

"false light". Injuring a person's "dignitas" is the basis for an action of invasion of privacy.

Remedies

In South African Law there are three accepted remedies to common law invasions of privacy.

- The Actio Injuriarum which provides for sentimental damages for injured feelings
- The Actio Legis Aquiliae which provides for damages for actual monetary losses
- The interdict

The Delict of Defamation

This is based on an Actio Injuriarum. An action of defamation lies where a person's personality rights have been harmed intentionally by an unlawful act of another. Such an act should be unlawful or contra bone mores. The law of defamation protects the right to reputation or fama[45]

This right is also constitutionally protected "Everyone has inherent dignity and the right to have their dignity respected and protected."[46]

Generally this right is also limited by article 36 of the South African constitution

Freedom of Speech

On a constitutional level Article 16 of the South African Constitution[47] creates a right to free speech

> 16. (1) everyone has the right to freedom of expression, which includes -
> 1. Freedom of the press and other media;
> 2. Freedom to receive and impart information and ideas;
> 3. Freedom of artistic creativity; and

[45] Fama is the good name or the respect that a person enjoys in society
[46] Chapter 2, Section 10 of the South African Constitution
[47] Article 16,South African Constitution ,Act 108 of 1996

4. Academic freedom and freedom of scientific research.

This right is limited by section 16(2):

> (2) The right in subsection (1) does not extend to -
> 1. Propaganda for war;
> 2. Incitement of imminent violence; or
> 3. Advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm.

This is of course is an important limitation in our society and our jurisprudence with its emphasis on social and restorative justice.

Generally this right is also limited by article 36 of the South African constitution

This limitations clause had been tested in our courts in *S v Makwanyane and Another*[48] where Chaskalson J held

> The limitation of constitutional rights for a purpose that is reasonable and necessary in a democratic society involves the weighing up of competing values, and ultimately an assessment based on proportionality. This is implicit in the provisions of s 33(1). The fact that different rights have different implications for democracy and, in the case of our Constitution, for 'an open and democratic society based on freedom and equality', means that there is no absolute standard which can be laid down for determining reasonableness and necessity. Principles can be established, but the application of those principles to particular circumstances can only be done on a case-by-case basis. This is inherent in the requirement of proportionality, which calls for the balancing of different interests. In the balancing process the relevant considerations will include the nature of the right that is limited and its importance to an open and democratic society based on freedom and equality; the purpose for which the right is limited and the importance of that purpose to such a society; the extent of the limitation, its efficacy and, particularly where the limitation has to be necessary, whether the desired ends could reasonably be achieved through other means less damaging to the right in question. In the process regard must be had to the provisions of s 33(1) and the underlying values of the Constitution, bearing in mind that, as a Canadian Judge has said, 'the role of the Court is not to second-guess the wisdom of policy choices made by legislators'.

The net effect of this is that we have a balancing act between the constitutional right to freedom of expression and other rights and interest.

---

[48] S v Makwanyane and Another, 1995 (3) SA 391 (CC)

This approach is pervasive throughout South African Jurisprudence from our common law to our labour laws. As an example of an application in our labour laws I refer to the cases *Cronje V CCMA and Others*[49] and *Dauth V Brown and Weir Cash and Carry*[50] in which both the applicants found their dismissals confirmed because of racially and religious comments made by them that was found to be contrarily to our societies norms and values.

On a constitutional level, *Laugh it off V South African Breweries International (Finance) B.V. t/a Sabmark International*[51] the constitutional court found the right to freedom of expression of the defendant outweighs the economic benefits of a trademark of one of the world largest breweries.

Commercial Speech

Commercial Speech demands particular examination as often the argument is made that

In *City of Cape Town v Ad Outpost (Pty) Ltd and Others*[52], Davis J held that it is clear that advertising falls within the nature of expression and thus have constitutional protection under section 16(1) of the constitution[53] . However the right to protection of commercial speech is not always absolute and thus requires a balancing test as in *S v Makwanyane*[48] above. The consensus in our courts currently is that although commercial speech is protected that protection exists at the edge of the protections offered speech in our constitution.

Application of the protections afforded by the constitution

In most jurisdictions the constitutions only applies vertically, to protect the individual against abuses from the state. In *Mandela V Falati*[54], Van Schalkwyk J held the constitutional right to freedom of expression has horizontal

---

[49] Cronje v CCMA & Others ,2002 (9) BLLR 855 (LC)
[50] Dauth v Brown & Weir's Cash and Carry ,2002 (8) BALR 837 (CCMA)
[51] Laugh It Off Promotions v SAB International (Finance) BV t/a Sabmark International, 2005 (8) BCLR 743 (CC)
[52] City of Cape Town v Ad Outpost (Pty) Ltd, 2000 (2) SA 733 (C)
[53] Section 16 (1), South African Constitution, Act 108 of 1996
[54] *Mandela V Falati 1995 1 SA 251(W)*

application also.