THE SUPREME COURT OF APPEAL OF SOUTH AFRICA

JUDGMENT

Reportable

Case no: 1009/2020

In the matter between:

GIFTWRAP TRADING (PTY) LTD	**APPELLANT**
and	
VODACOM (PTY) LTD	**FIRST RESPONDENT**
MOBILE TELEPHONE NETWORKS (PTY) LTD	**SECOND RESPONDENT**
TELKOM SA LTD	**THIRD RESPONDENT**
CELL C (PTY) LTD	**FOURTH RESPONDENT**

Neutral citation: *Giftwrap Trading (Pty) Ltd v Vodacom (Pty) Ltd and Others* (1009/2020) [2023] ZASCA 47 (4 April 2023)

Coram: VAN DER MERWE, GORVEN and MABINDLA-BOQWANA JJA and OLSEN and SIWENDU AJJA

Heard: 16 February 2023

Delivered: 4 April 2023

Summary: Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) – disclosure of customer information obtained and stored by Internet and cellular phone service providers under ss 39 and 40 of RICA – s 42(1)*(c)* of RICA permits disclosure if required as evidence in a court of law – not for purposes of identifying wrongdoers.

ORDER

On appeal from: Gauteng Division of the High Court, Pretoria (Mokose J, sitting as court of first instance):

1 The appeal is dismissed.

2 The registrar of this court is directed to bring this judgment to the attention of the Cabinet members responsible for the administration of justice and state security.

JUDGMENT

Van der Merwe JA (Gorven and Mabindla-Boqwana JJA and Olsen and Siwendu AJJA concurring):

[1] The first respondent in this appeal, Vodacom (Pty) Ltd (Vodacom), does business as a cellular phone and Internet service provider (service provider). So, too, do the other three respondents. As I shall show, service providers are required by law to obtain and keep specified information in respect of their customers (customer information). The appeal concerns rights of access to the customer information of the respondents and arose in the manner set out below.

Background

[2] The business of the appellant, Giftwrap Trading (Pty) Ltd (Giftwrap), is online sales of products such as corporate gifts and clothing. This means that it markets and sells its products on the international computer network known as the Internet. Giftwrap advertises its products on online platforms provided by the international technological company Google LLC. Giftwrap, of course, has to pay for the advertisements posted. These advertising fees are calculated with reference to the number of visits to a particular advertisement.

[3] For some years, however, Giftwrap has been the victim of what is referred to as ‘click fraud’. Click fraud takes place when an advertisement on the Internet is

repeatedly visited (clicked upon) with the intention of increasing the costs of the advertisement and/or draining the sales revenue of the advertiser. Revenue is lost because the repeated click fraud visits limit genuine access to the advertisement.

[4] Giftwrap employed various experts and strategies in attempts to put an end to the click fraud that it experienced. These efforts were unsuccessful until a breakthrough was made during March 2019. With the assistance of an expert, Giftwrap managed to obtain a large number of local Internet protocol (IP) addresses of devices from which, so Giftwrap believed, the click fraud on it had emanated. The information at its disposal also identified the service provider that each of these IP addresses used to gain access to the Internet. Giftwrap was therefore able to compile a list of IP addresses suspected of having perpetrated click fraud, for each service provider. The lists of IP addresses that pertained to the respondents (the listed IP addresses) formed the basis of the litigation that followed.

[5] During June 2019, Giftwrap launched an application in the Gauteng Division of the High Court, Pretoria against the respondents. In essence, Giftwrap sought the disclosure of the customer information in respect of each of the listed IP addresses. The purpose of the relief was to identify wrongdoers in order to take legal action against them. Giftwrap initially founded the application on the decision in *Nampak Glass (Pty) Ltd v Vodacom (Pty) Ltd & Others* [2018] ZAGPJHC 481; 2019 (1) SA 257 (GJ) (*Nampak*). In a supplementary founding affidavit, however, it placed reliance on s 42(1)*(c)* of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA). I shall reproduce this subsection shortly. For purposes of the narrative it suffices to say that it would permit access to customer information which is required as evidence in a court of law.

[6] The second to fourth respondents abided the outcome of the application, but Vodacom delivered an answering affidavit. It clarified its stance from the outset. This was that Vodacom did not dispute Giftwrap's factual averments nor that the information in question could be useful for the purpose for which it was required. It said that were the decision solely up to it, Vodacom would have provided the information to Giftwrap. In its view, however, the provisions of RICA precluded the disclosure that Giftwrap sought, hence the opposition to the application.

[7] The court a quo (Mokose J) agreed with Vodacom. It essentially reasoned that s 42(1)*(c)* of RICA does not permit disclosure of customer information for the purpose of identifying wrongdoers. It accordingly dismissed the application with costs. Giftwrap's appeal against that order is with the leave of this court. In this court Vodacom continued to adopt the aforesaid stance.

Relevant RICA provisions

[8] Sections 39 and 40 of RICA are concerned with customer information. Before I turn to their provisions, however, it is necessary to deal with an oddity in RICA. When it was enacted, RICA contained definitions of 'telecommunication system', 'telecommunication service' and 'telecommunication service provider'. These expressions were widely employed in RICA, especially in Chapter 5 (ss 30-31), Chapter 6 (ss 32-38) and Chapter 7 (ss 39-41).

[9] Section 97 of the Electronic Communications Act 36 of 2005 amended RICA by replacing the 'telecommunication' definitions with definitions of 'electronic communication system', 'electronic communications service' and 'electronic communication service provider'. Curiously, however, corresponding amendments were not effected in the body of RICA, not even in ss 30 and 32, which were amended in other respects. When s 40 of RICA was subsequently substituted by Act 48 of 2008,[1] however, the 'electronic communication' expressions were employed.

[10] The result is that many provisions of RICA still employ the 'telecommunication' expressions, even though they were replaced by the 'electronic communication' definitions. In particular, s 39 refers to information to be kept and obtained by certain telecommunication service providers. Section 40, as I have said, concerns information to be obtained and kept by an electronic communication service provider (which provides a mobile cellular electronic communications service).

[11] The Telecommunications Act 103 of 1996 was repealed and replaced by the Electronic Communications Act and s 97 thereof introduced amendments to reflect that fact. There are no intrinsic differences between the 'telecommunication' and 'electronic communication' definitions. The definition of 'telecommunication service

[1] The Regulation of Interception of Communications and Provision of Communication-Related Information Amendment Act 48 of 2008.

provider' included an Internet service provider and so does the definition of 'electronic communication service provider'.

[12] In the result it must be concluded that the legislature intended to replace all the 'telecommunication' expressions with the 'electronic communication' expressions, but as a result of an unfortunate oversight failed to effect that. In these peculiar circumstances, I think that the proper thing to do is to read the 'telecommunication' expressions in RICA as 'electronic communication' expressions as defined. That would, as a matter of statutory interpretation akin to filling in a *casus omissus*, give effect to the intention to the legislature. The legislature should, however, correct this with expedition and for that purpose I shall direct that this judgment be brought to the attention of the Cabinet members responsible for the administration of justice and for state security.[2]

[13] Various provisions of RICA enable an 'applicant' to obtain disclosure of information, including customer information (under ss 39(3) and 40(7)). An 'applicant' is defined in RICA. It is not necessary to reproduce this rather extensive definition. It suffices to say that only specified government officials (such as officers in the South African Police Service) are included in the definition and that Giftwrap is not an 'applicant' under RICA.

[14] As I have demonstrated, ss 39 and 40 of RICA apply to service providers. Section 39(1)[3] specifies the customer information that a service provider other than a

---

[2] 'Minister' is defined in RICA as the Cabinet member responsible for the administration of justice, except in Chapter 6 where it means the Cabinet member responsible for state security.

[3] Section 39(1) reads:

'(1) Before a telecommunication service provider, other than a telecommunication service provider who provides a mobile cellular telecommunication service, enters into a contract with any person for the provision of a telecommunication service to that person, he or she-

(a) must, if that person is a natural person-

(i) obtain from him or her-

(aa) his or her full names, identity number, residential and business or postal address, whichever is applicable; and

(bb) a certified photocopy of his or her identification document on which his or her photo, full names and identity number, whichever is applicable, appear;

(ii) retain the photocopy obtained in terms of subparagraph (i) (bb); and

(iii) verify the photo, full names and identity number, whichever is applicable, of that person with reference to his or her identification document; or

(b) must, if that person is a juristic person-

(i) obtain from the person representing that juristic person-

(aa) his or her full names, identity number, residential and postal address, whichever is applicable;

cellular phone service provider, must obtain and verify before it enters into a contract with any person for the provision of an electronic communications service to that person. Section 39(1)*(a)* lists the customer information to be obtained and verified in respect of a natural person and s 39(1)*(b)* with those of a juristic person. The keeping of records of this information is prescribed in s 39(2).[4]

[15] In terms of s 40(1)*(a)* a service provider who provides a cellular phone service shall not activate a Subscriber Identity Module (SIM-card) on its electronic communications system unless s 40(2)[5] has been complied with. That section

---

(bb) the business name and address and, if registered as such in terms of any law, the registration number of that juristic person;
(cc) a certified photocopy of his or her identification document on which his or her photo, full names and identity number, whichever is applicable, appear; and
(dd) a certified photocopy of the business letterhead of, or other similar document relating to, that juristic person;
(ii) retain the photocopies obtained in terms of subparagraph (i) (cc) and (dd); and
(iii) verify the-
(aa) photo, full names and identity number, whichever is applicable, of that person with reference to his or her identification document; and
(bb) name and registration number of that juristic person with reference to its business letterhead or other similar document; and

(c) may obtain from such person any other information which the telecommunication service provider deems necessary for purposes of this Act.'

[4] Section 39(2) provides:
'(2) A telecommunication service provider referred to in subsection (1) must ensure that proper records are kept of-
(a) the information, including the photocopies, referred to in subsection (1) and, where applicable, any change in such information which is brought to his or her attention;
(b) the telephone number or any other number allocated to the person concerned; and
(c) any other information in respect of the person concerned which the telecommunication service provider concerned may require in order to enable him or her to identify that person.'

[5] Section 40(2) reads:
'(2) From the date of commencement of this section an electronic communication service provider must, subject to subsection (4), at own cost implement a process to record and store, and must record and store-
(a) the Mobile Subscriber Integrated Service Digital Network number (MSISDN-number) of the SIM-card that is to be activated by an electronic communication service provider at the request of a person contemplated in paragraphs (b) and (c);
(b) in the case of a person who-
(i) is a South African citizen or is lawfully and permanently resident in the Republic, the full names and surname, identity number and at least one address of such person who requests that a SIM-card referred to in subsection (1) be activated on the electronic communication system of an electronic communication service provider; or
(ii) is not a South African citizen or who is not permanently resident in the Republic, and who requests that a SIM-card referred to in subsection (1) be activated on the electronic communication system of an electronic communication service provider, the full names and surname, identity number and at least one address of such person and the country where the passport was issued; or
(c) in the case of a juristic person-
(i) the full names, surname, identity number and an address of the authorised representative of the juristic person; and
(ii) the name and address of the juristic person and, where applicable, the registration number of the juristic person.'

specifies the information that such a service provider must record, verify and store in respect of South African citizens, non-South African citizens and juristic persons. When a customer sells or otherwise provides a SIM-card to a person other than a family member, the customer and the person who is to receive the SIM-card are obliged, in terms of s 40(5), to provide similar information to the service provider. In terms of s 40(6) that information must also be recorded, verified and stored as contemplated in s 40(2).

[16] Section 40(3)[6] prescribes the process of verification of information for purposes of s 40(2). In terms of s 40(4) a service provider must ensure that the process contemplated in s 40(2), the information recorded and stored in terms of that subsection and the facility in or on which the information is recorded and stored 'are secure and only accessible to persons specifically designated . . .'. Section 40(10) essentially provides that customer information must be stored for a period of five years after the termination of the contract between the customer and the service provider.

Analysis

[17] In determining whether Giftwrap is entitled to disclosure of the customer information in respect of the listed IP addresses, it is firstly necessary to have regard to *Nampak*.[7] There the applicant had been the victim of a robbery. In an urgent application, it sought information from Vodacom and a number of other cellular phone service providers on the basis that the information would assist in an investigation to

---

[6] Section 40(3) provides:

'(3) *(a)* For the purposes of subsection (2), an electronic communication service provider must, in the manner provided for in paragraph (b), verify-

(i) the full names, surname, identity number and identity of the person contemplated in subsection (2) *(b)* and *(c)* and, where applicable, the country where the passport was issued;
(ii) the name and, where applicable, the registration number of the juristic person;
(iii) in the case of a person contemplated in subsection (2)*(b)* (i) and *(c)*, the address; and
(iv) the authority of the representative of a juristic person.
(b) An electronic communication service provider must verify-
(i) the information contemplated in paragraph *(a)*(i) by means of an identification document;
(ii) the information contemplated in paragraph *(a)*(ii) by means of documentation, including a registration document, founding statement, document issued by the South African Revenue Service or any other similar document;
(iii) the address contemplated in paragraph *(a)* (iii) by means of documentation, including a bank statement, a municipal rates and taxes invoice, telephone or cellular phone account of not older than three months, or any other utility bill or an account of a retailer of not older than three months, or an existing lease, rental or credit sale agreement, insurance policy, a current television licence or a new motor vehicle licence document; and
(iv) the authority of the representative of the juristic person by means of a letter of authority or an affidavit.'

[7] Para 5 above.

identify the wrongdoers. The information sought firstly related to the identification of all the cellular phones that had been used in the vicinity of the applicant's premises during a specified period (approximately an hour). Secondly, the applicant essentially sought customer information and detailed call logs in respect of all the cellular phones so identified. Vodacom and the service providers did not oppose the urgent application.

[18] The court nevertheless determined to develop the common law as expounded in *House of Jewels & Gems & Others v Gilbert & Others* 1983 (4) SA 824 (W). It did so on the basis of: the applicant's constitutional right to access to courts; the 'regrettable omission' of the Uniform Rules of Court to provide a remedy in advance of litigation having been instituted; and the inherent power of the High Court to regulate its own process. After adopting English law in this regard, the court granted the far-reaching relief sought.

[19] The court was not, however, referred to the provisions of RICA. A development of the common law in this regard could not legitimately have been undertaken without consideration of the provisions of RICA. For the reasons furnished below, RICA precluded the disclosure of customer information. To this extent *Nampak* was wrongly decided. It also appears to me that at least the bulk of the call logs in *Nampak* constituted archived communication-related information, the disclosure of which is strictly regulated by RICA.[8] However, it is not necessary for purposes of this case to make a final determination in respect of the call logs.

[20] Returning to RICA, the starting point is s 42(2). It *inter alia* provides that no service provider may disclose any information obtained in the exercise of its powers or the performance of its duties in terms of RICA, except for the purposes mentioned in s 42(1). This clearly applies to customer information obtained under s 39 and s 40.

[21] Section 42(1) reads:

'(1) No person may disclose any information which he or she obtained in the exercising of his or her powers or the performance of his or her duties in terms of this Act, except-

(a) to any other person who of necessity requires it for the performance of his or her functions in terms of this Act;

[8] Part 2 of Chapter 2 of RICA.

(b) if he or she is a person who of necessity supplies it in the performance of his or her functions in terms of this Act;
(c) information which is required in terms of any law or as evidence in any court of law; or
(d) to any competent authority which requires it for the institution, or an investigation with a view to the institution, of any criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act.'

[22] It is necessary to point out that in terms of s 13 of the Prevention of Organised Crime Act 121 of 1998 (POCA), proceedings under Chapter 5 (Proceeds of Unlawful Activities) are civil proceedings and not criminal proceedings. In terms of s 37 of POCA the same applies to proceedings under Chapter 6 (Civil Recovery of Property). It follows that s 42(1)*(d)* of RICA applies to the institution of criminal proceedings, as well as to proceedings under Chapters 5 and 6 of POCA.

[23] As I have said, Giftwrap requires the customer information to identify the perpetrators of click fraud in order to take legal action against them. It goes without saying that disclosure of the customer information in respect of the listed IP addresses would not necessarily lead to legal action against a person so identified. It follows that in reality Giftwrap requires the customer information as part of an investigation with a view to taking appropriate legal action. The question is whether s 42(1)*(c)* permits this. The answer must, of course, be found in an interpretation of s 42(1)*(c)* of RICA by a holistic consideration of its text, context and apparent purpose.

[24] According to its text ('information which is required . . . as evidence in any court of law'), s 42(1)*(c)* conveys that the information must at the time of its disclosure be required as evidence in a court of law. It therefore envisages disclosure of information which is required as evidence in proceedings that are pending in a court of law. On this basis, information that is required to investigate whether legal proceedings could be instituted, falls outside the ambit of s 42(1)*(c)*. This is supported by the context provided by s 42(1)*(d)*. It expressly provides that information may be disclosed for purposes of 'an investigation with a view to the institution' of (criminal or POCA-related) proceedings. The absence of a similar provision in s 42(1)*(c)* indicates that disclosure for the purpose of an investigation or identification of wrongdoers is excluded from s 42(1)*(c)*.

[25] In the main, RICA prohibits the interception of the contents of communications and the disclosure of related and other specified information, subject to prescribed exceptions. The purpose of s 42(1) is to prohibit the disclosure of private information, save in limited cases where it is justified in the public interest. Thus, the limited ambit of s 42(1)*(c)* that its text and context indicate, accords with the purpose of s 42(1).

[26] This interpretation would not render a person in the position of Giftwrap remediless. As counsel for Vodacom rightly pointed out, RICA does not preclude the preservation of customer information pending the institution of legal proceedings in which it would be required as evidence. A criminal complaint could also be laid, after which s 205 of the Criminal Procedure Act 51 of 1977 or s 42(1)*(d)* of RICA could be employed to obtain customer information.

[27] For these reasons I conclude that s 42(1)*(c)* of RICA does not permit the disclosure of customer information of a service provider for purposes of investigation or identifying wrongdoers. It follows that the appeal must fail. Vodacom did not ask to be awarded costs of the appeal.

[28] The following order is issued:

1 The appeal is dismissed.

2 The registrar of this court is directed to bring this judgment to the attention of the Cabinet members responsible for the administration of justice and state security.

_____

C H G VAN DER MERWE

JUDGE OF APPEAL

Appearances

For appellant:	F W Botes SC with A S L van Wyk
Instructed by:	Hefferman Attorneys, Pretoria Webbers Attorneys, Bloemfontein
For 1st respondent:	S Budlender SC with H P Pretorius and K A R Thobakgale
Instructed by:	Adams & Adams Attorneys, Pretoria Phatshoane Henney Attorneys, Bloemfontein