IN THE SUPREME COURT OF JUDICATURE OF JAMAICA

IN THE FULL COURT

CLAIM NO. SU 2022CV03991

CORAM: **THE HONOURABLE MRS. JUSTICE L. SHELLY WILLIAMS**
THE HONOURABLE MRS. JUSTICE A. PETTIGREW-COLLINS
THE HONOURABLE MRS. JUSTICE S. WOLFE-REECE

IN THE MATTER of the Charter of Fundamental Rights and Freedoms of the Constitution of Jamaica.

AND

IN THE MATTER of an Application by Detective Constable Julian Frazer, an Authorised Officer, for a Production Order pursuant to Section 21 of the Cybercrimes Act 2015.

BETWEEN	**AMOI LEON – ISSA**	**CLAIMANT**
AND	**DETECTIVE CONSTABLE JULIAN FRAZER**	**1ST DEFENDANT**
AND	**THE COMISSIONER OF POLICE**	**2ND DEFENDANT**
AND	**HER HONOUR MRS. SASHA MARIE ASHLEY**	**3RD DEFENDANT**
AND	**THE ATTORNEY GENERAL OF JAMAICA**	**4TH DEFENDANT**

FULL COURT

Mr. Chukwuemeka Cameron for the Claimant

Ms. Kamau Ruddock and Matthew Gabbadon instructed by the Director of State Proceedings for the Defendants

Heard: 14th and 21st July and 29th September 2023.

CONSTITUTIONAL LAW – The Constitution of Jamaica – The Charter of Fundamental Rights and Freedoms (Constitutional Amendment) Act, 2011, sections 13(2) and (3)(j)(iii), 16(2) & 19 – Whether section 21 of the Cybercrimes Act breaches the Claimant's fundamental rights and freedoms guaranteed under section 13(3)(j)(iii) of the Charter – Whether any breach of the Claimant's right to privacy guaranteed under section 13(3)(j)(ii) of the Charter are demonstrably justified in a free and democratic society – Whether breach of Claimant's rights guaranteed under section 16(2) – Proportionality - Production Order-Disclosure-Cybercrimes Act, section 21 – Data Protection Act, sections 22 to 31

SHELLY WILLIAMS, SPJ (AG.), PETTIGREW-COLLINS, J & WOLFE-REECE, J

This is the joint judgment of the Court, to which each member has contributed a substantial portion.

INTRODUCTION & BACKGROUND

[1] The Claimant, Mrs Amoi Leon-Issa filed a constitutional claim seeking declarations among other reliefs under Section 19 of the Constitution of Jamaica. The subject of this claim surrounds a Production Order granted by the 3rd Defendant Her Honour Mrs. Sasha Marie Ashley which she alleges breaches her constitutional right to privacy.

[2] The 1st Defendant, Detective Constable Julian Frazer made an ex parte application for the grant of a Production Order in respect of the key to an iPhone cellular telephone, the property of the Claimant, for the purpose of an investigation

into the death of GK, son of the said Mrs. Leon-Issa. The murder of GK occurred on Thursday January 13, 2022, about 11:30 am between Oak Hill Avenue and Fairfield Avenue, Fairfield Estate in the parish of St. James.

[3] On Tuesday September 6, 2022, the Production Order was granted by Her Honour Mrs. Sasha Marie Ashley in the St. James Parish Court. The Production Order granted, upon the ex parte application of Detective Constable Julian Frazer, was as follows:

> 1) *Mrs. Amoi Leon Issa, owner of a gold and white IPhone 13 Pro Max bearing IMEI number 352060425852025 and cellular number 876-379-2847 (hereinafter referred to as "the cellular phone"), produces in intelligible form to Detective Constable Julian Frazer, an authorized officer pursuant to section 21 of the Cybercrimes Act 2015, within forty-eight (48) hours of service of this Order, any communication data, cell site data and other data contained on the said cellular phone for the purpose of a criminal investigation into the murder of Gabriel King which occurred on Thursday January 13, 2022 about 11:30a.m. between Oak Hill Avenue and Fairfield Avenue, Fairfield Estate in the parish of St. James.*
>
> 2) *Mrs Amoi Leon Issa, owner of a gold and white IPhone 13 Pro Max bearing IMEI number 352060425852025 and cellular phone number 876-379-2847, produces to Detective Constable Julian Frazer, within forty-eight (48) hours of service of this Order any key that is in her control or possession that is necessary to obtain access to any communication data, cell site data and other data contained on the said cellular phone, for the purpose of a criminal investigation into the murder of Gabriel King which occurred on Thursday January 13, 2022 about 11:30am between Oak Hill Avenue and Fairfield Avenue, Fairfield Estate in the parish of St. James.*

[4] On November 4, 2022, a Notice of Application for Court Orders was filed at the St. James Parish Court by Carolyn C. Reid & Co, Attorneys-at-Law on behalf of the Claimant, seeking a discharge or in the alternative a variation of the Production Order and an extension of time within which to comply with the Order. The application was heard between November 14 and 18, 2022.

[5] Her Honour Mrs Ashley refused the Claimant's application to discharge the Production Order but varied the original order by deleting any mention of cell sites

in the order. The Learned Parish Court Judge also added some ancillary orders to the Production Order. The amended Production Order stated:

> *i) Mrs Leon-Issa, owner of a gold and white IPhone 13Pro Max bearing IMEI number 352060425852025 and cellular telephone number 8763792847 (hereinafter referred to as the cellular phone) on or before the 24th day of November 2022 provides access to and/or produces in intelligible form to Detective Inspector Roderick Muir, an authorised officer pursuant to section 21 of the Cybercrimes Act 2015, any communication data or other data contained on the cellular phone by making written disclosure of the key that is in her possession or control that is necessary to obtain access to and/or put in intelligible form communication data or other data for the purpose of a criminal investigation into the death of Gabriel King which occurred on the 13th day of January 2022 in the parish of St. James.*
>
> *ii) Mrs. Amoi Leon-Issa shall not be entitled to be present during the accessing and/or producing in intelligible form the said communication data or other data however an Attorney-at-Law instructed by her may attend as an observer only.*
>
> *iii) In the event the Attorney-at-Law so instructed is unable to be present, the process of accessing and/or producing in intelligible form the said communication data and other data shall not, on that account only, be postponed or otherwise delayed but may proceed in the absence of such Attorney-at-Law.*
>
> *iv) A third party, being a qualified computer expert mutually agreed upon by counsel for the Jamaica Constabulary Force and counsel for Mrs Amoi Leon-Issa, may attend as an observer only the process of accessing and/or producing in intelligible form the said communication data or other data.*
>
> *v) In the event a qualified computer expert cannot be mutually agreed upon by counsel for the Jamaica Constabulary Force and counsel for Mrs Amoi Leon-Issa by the 22nd day of November 2022, the process of accessing and/or producing in intelligible form the said communication data or other data shall not, on that account only, be postponed or otherwise delayed but may proceed in the absence of that third party. Every key produced in pursuance of this Order shall be stored, for so long as it is retained, in a secure manner and any records of such key shall be destroyed as soon as no longer needed to access and/or put into intelligible form the said communication data or other data. The number of persons to whom the key is produced or otherwise made available, and any copies made thereof, shall be limited to the minimum that is necessary for the purpose of enabling the communication data or other data to be accessed or put into intelligible form.*

[6] The Claimant also filed an application for disclosure of all documents related to the request for the Production Order. That application was heard by the Parish Court Judge and refused.

[7] On the 16th of December 2022 the Claimant filed a Fixed Date Claim Form before this Court challenging the Production Order. The claim is for constitutional redress under Section 19 of the Constitution of Jamaica, that the provisions of Section 13 of Chapter III entitled "Charter of Fundamental Rights and Freedoms", have been and are being breached. The Claimant sought the following relief:

Declaration that:

a. The 1st and 2nd Defendants' action of compelling the Claimant, by obtaining a production order which in effect would compel the Claimant to provide access to all personal and private information for an unlimited period of time: -
    i. knowing that neither the mobile phone nor the data thereon was in the possession or control of the Claimant at the time the application was made, and
    ii. knowing that the "cell site data" being sought does not reside on any phone and in particular the phone of the Claimant.

    contravened or is likely to contravene the Claimant's right to privacy and her right to informational privacy guaranteed by section 13(3)(i) of the **Charter of Fundamental Rights and Freedoms** as there was no lawful or legitimate basis to seek to restrict the right to privacy by obtaining the said order.

b. The 1st and 2nd Defendants in making representations to the Parish Court Judge while knowing them to be false; to wit, cell site data can be found on the Claimant's phone or any phone at all, and causing a production order to be issued compelling the production of cell site

data does not exist on the Claimant's phone and exposing her to contempt proceedings and/or custodial sanctions: -

i. Abused their investigatory powers and was not in furtherance of the public interest to investigate crime and
ii. Abused the process of the court which violated the Claimant's right to fair hearing guaranteed by section of the Constitution.

c. The 1st and 2nd Defendants contravened or is likely to contravene the Claimant's right to privacy guaranteed by section 13 (3) (j) of the **Charter of Fundamental Rights and Freedom**s and was not in accordance with the law when they failed to put in place the necessary arrangements prescribed by section 21 (14 (a) the **Cybercrimes Act** to safeguard the handling of the key.

d. The 1st and 2nd Defendants abused the process of the court by making and application under section 21 of the **Cybercrimes Act** to obtain "communication data" instead of section 16 (2) of the **Interception of Communication Act** which was a less intrusive method and the lawful method to obtain "communication data", which act undermined and/or avoided the safeguards provided at section 16 (5) of the **Interception of Communication Act** which ae meant to protect the privacy of the Claimant herein meeting the public interest to investigate and detect crime.

e. On a proper interception of section 21 (1) of the **Cybercrimes Act** the 1st and 2nd Defendants are required to specify the information being requested in a production order.

f. On a proper interpretation of section 2 1(2) the learned Parish Court Judge in issuing a Production Order would have to identify the specified data that is to be produced by the Claimant.

g. The Order and the subsequent Variation Order issued by the learned Parish Court Judge was unconditional in that it breached the Claimant's right to privacy guaranteed by section 13(3) (j) of **the Charter of Fundamental Rights and Freedoms (Constitutional Amendment) Act 2011** and was disproportionate to the interest of the public in investigating and detecting crime and not in accordance with the section 21 of the **Cybercrimes Act**.

h. The Order granted by Her Honour Mrs. Sasha-Marie Ashley on 6 September 2022 pursuant to section 21 of the **Cybercrimes Act 2015** in an application made by Detective Constable Julian Frazer for a Production Order ("the Order") is in breach of section 13 (3) (j) of the Charter of Fundamental Rights and Freedom (Constitutional Amendment) Act 2011, in that the said Order was wholly disproportionate to the interest of the public in having crime detected and investigated.

i. The Order granted by Her Honour Mrs. Sasha-Marie Ashley on18 November 2022 pursuant to section 21 of the **Cybercrimes Act 2015** in an application made by Detective Constable Julian Frazer for a Production Order ("the Variation Order") is in breach of the Claimant's right to due process and a fair hearing guaranteed by section 16 (1) of the **Charter of Fundamental Rights and Freedom (Constitutional Amendment) Act 2011**, in that the said Order was granted without the Claimant having the benefit of full disclosure of the need for the infringement of her rights and was wholly disproportionate to the interest of the public in having crime detected and investigated.

j. The Order and Variation Order sought by the 1st and 2nd Defendants and issued by the 3rd Defendant breached section 13 3 (j) of the **Charter of Fundamental Rights and Freedoms** contained in the Constitution of Jamaica, in that the Claimant was deprived of her right to protection from search of her property; respect for and protection of her private and family life; and protection of privacy of property and communication.

k. The Order breached section 16 (1) of the **Charter of Fundamental Rights and Freedoms** contained in the Constitution of Jamaica, in that the Claimant was deprived of her right to a fair hearing as the order was granted in her absence and without the Court having the benefit of full and frank disclosure, in particular that some of the data requested in the application did not reside on the cell phone and that the data could be obtained from a telecommunication provider in a less intrusive manner.

l. The Variation Order breached Section 16 (1) of the **Charter of Fundamental Rights and Freedoms** contained in the Constitution of Jamaica, in that the Claimant was deprived of the right to a fair hearing as the learned Parish Judge wrongly refused the application for disclosure of original source documents which led to the grant of the Order thereby preventing the Claimant from raising challenges as to:

    i. The basis of the reasonable and probable cause for suspecting data relevant to the crime was on the instrument;

    ii. The adequacy of the safeguards in place to protect the Claimant's privacy and that of third parties.

iii. Whether the reasonable and probable cause was due to hearsay, stereotypes, generalizations or simply proximity of the device to the crime scene;

iv. Whether there was disclosure as when and how the phone came to be in the possession of the 1st and/ or 2nd Defendant;

v. Whether there was disclosure of the letters from the Claimants Attorney-at-Law advising of the Claimant's agreement to assist with assessing the instrument; and

m. The Order and the Variation Order has violated and will continue to violate the constitutional rights of the Claimant as the Claimant has been ordered to hand over access to the key to her gold and white iPhone 13 Pro Max being IMEI number 352060425852025 and cellular phone (876) 379-2847 ("the iPhone") to Detective Constable Julian Frazer and undisclosed members of the Jamaica Constabulary Force to conduct a search of all communication data, and other data contained on the iPhone for the purpose of the criminal investigation of the Gabriel King which occurred on 13th January 2022 and should she fall to do so she may be deprived of her liberty by virtue of obstruction or contempt proceedings.

n. That neither the manner nor the extent, of the abrogation abridgement or infringement of the Claimant's rights, are proportionate or necessary to the ends to be achieved by the 1st and 2nd Defendants which is the detection of crime.

o. The Order is unconstitutional as it failed to take into account any likely contents of the iPhone which should be excluded on the basis that they are personal data protected by the **Data Protection Act,** privileged documents or confidential documents which have nothing to do with the criminal investigation into the death of Gabriel King and

which disclosure could have a deleterious effect on the Claimant and third parties.

That this Honourable Court do grant a stay of execution of all proceedings pursuant to the said Variation Order granted on 18th November 2022 pursuant to the application of the 1st Defendant until the conclusion of the hearing of this matter.

[8] The Relief being sought by the Claimant is as follows: -

1) Quashing the orders granted by the learned Parish Court Judge, Sasha-Marie Ashley on 6 September 2022 and 18 November 2022 as unconstitutional, void and of no legal effect;
2) Vindicatory Damages on the footing that the actions of the 1st, 2nd and 3rd Defendants amounts to a breach of the Constitutional rights granted to the Claimant by the Charter of Fundamental Rights and Freedoms and Cybercrimes Act.
3) Further and such other relief as this Honourable Court deems fit; and
4) Cost to be costs in the claim.

Claimant's Submissions

Right to Privacy

[9] Mr. Cameron submitted that there is a constitutional right to privacy enjoyed by all individuals and the State should take no action to restrict that right, unless demonstrably justifiable. Mr. Cameron argued that the Production Orders made by Parish Court Judge Ms. Ashley were not proportionate or necessary, as they do not meet the test of being demonstrably justifiable in a free and democratic society and therefore breached the Claimant's right to privacy.

[10] It is the Claimant's submission that the Production Order would give an untold number of persons, for an indefinite period, access to all the personal data and

information contained on the mobile phone of the Claimant, without any restrictions. This would breach the Claimant's right to privacy.

[11] Counsel argued that the constitutional right to privacy is essential to every individual and so too is the protection it affords. He submitted that it is only in extreme situations where there are justifications for the abrogation, abridgement, and infringement that the right may be trespassed upon. In such circumstances safe guards must be established to ensure a minimal amount of infringement.

[12] Mr. Cameron relied on the case of ***Julian Robinson v The Attorney General*** [1], which, he argued, clarified that the right to privacy encompasses the right to informational privacy. He submitted that the **Julian *Robinson*** case identified three key areas as being covered by the right to privacy which are: -

a. non-intrusion into an individual's physical body,
b. informational privacy and
c. privacy of choice.

He submitted that the right to privacy provides individuals with the autonomy not only to control their personal lives but also to secure their personal information.

[13] In determining whether there was a breach of the Claimant's right to privacy Counsel commended the approach of the court in the Canadian case of ***R v Canfield*** [2]. In that case the court opined that:

> *"To claim s.8 protection, a claimant must first establish a reasonable expectation of privacy in the subject matter of the search, i.e. that the person subjectively expected it would be private and that this expectation was objectively reasonable."*

---

[1] [2019] JMC Full 04
[2] 2020 ABCA 383

[14] The line of enquiry proposed by Counsel for the Claimant, to guide the determination of whether the Claimant had a reasonable expectation of privacy in the totality of the circumstances were:

1. What was the subject matter of the alleged search?
2. Did the Claimant have a direct interest in the subject matter?
3. Did the Claimant have a subjective expectation of privacy in the subject matter?
4. If so, was the Claimant's subjective expectation of privacy objectively reasonable?

[15] Counsel acknowledged that in ***Julian Robinson (supra)*** the court saw no need to go into the arguments on reasonable expectation of privacy as the violation was quite plain. Though, urging this court to take a similar position that the violation here is plain, he nonetheless made the case that the Claimant had a reasonable expectation of privacy.

[16] Counsel submitted that the subject matter of the search, was all the Claimant's personal data and informational content on her personal electronic device (iPhone). He indicated that at all material times the Claimant believed that the data and information on her phone would remain private. This was explicitly declared by letter expressing that access to the phone will only be granted subject to protecting the Claimant's right to privacy. It was also argued that it was objectively reasonable for the claimant to believe that her phone, which contains intimate details of her life would be safe from arbitrary search. He opined that in today's age there were a few things that could be considered more private than one's cell phone as they held a wealth of personal information such as conversations, photos, locations and much more. He submitted that it is only in exceptional circumstances that such information should be viewed, much less extracted.

[17] Counsel then went on to consider the issue of justification. He explained that in accordance with the wording of the Charter the standard of justification to override

this constitutionally protected right must be one that is demonstrably justified in a free and democratic society. He submitted that it is the state, as the party seeking to limit this right, that has this burden to prove the breach is justifiable in a free and democratic society.

[18] Counsel submitted that the Court should be guided by the Canadian Supreme Court case of ***R v Oakes***[3] to determine whether the measures limiting the right to privacy was 'demonstrably justified in a free and democratic society.

[19] Counsel sought to examine each discrete action of the State in the procurement of the Production Order and summed up that the state had failed to satisfy the test. He argued that the original Production Order granted requested information pertaining to cell site data, which could not be produced from the data on the Claimant's phone. He submitted that the state knew or ought to have known that it was impossible to furnished such information from a phone as such data did not reside on the phone. Counsel's position was that if the information is not located on the phone then the order cannot be said to be reasonable and demonstrably justified.

[20] Mr. Cameron further submitted that where the State seeks to restrict any right, it must use the least restricted method possible. He argued that it is incumbent on the Court to put safeguards in place which seek to restrict certain information being accessed.

[21] He also argued that applying to obtain the communication data under section 21 of the **Cybercrimes Act** instead of section 16(2) of the **Interception of Communication Act**, was a more intrusive method of obtaining the communication data and had the effect of undermining and/or violating the safeguards provided at sections 16(5) of the **Interception of Communication**

---

[3] *26 DLR (4th) 200*

Act. This he argued, meant there was no protection of the privacy of the Claimant while meeting the public interest to investigate and detect crime. He submitted that under the **Interception of Communications Act** the police have the power to request specific communication data from a telecommunication provider to further the criminal investigation, which is less intrusive than requiring the claimant to hand over all personal and private information on the phone for an indefinite period of time. He argued that this would have preserved the Claimant's right to privacy while also achieving the state's legitimate objective of investigating the crime.

[22] Mr. Cameron submitted that section 21 of the **Cybercrimes Act** under which the State applied for a Production Order did not give them the power to search computer material i.e. the Claimant's phone. He indicated that the requisite investigative tool to search the phone of the Claimant is the search and seizure warrant under section 18 of the said Act. This he states lends more flexibility to a search for incriminating evidence in general, while section 21 was primarily for telecommunication providers or third parties holding data. In light if that, the Defendant's would have had to be able to specify the data they are in search of.

[23] It was also contended that the Parish Court Judge failed to comply with the prescribed procedures of the Cybercrimes Act, which is to identify specific data being sought in the issuing of the Production Order. He argued that the Production Order was, in essence, a demand for all data on the mobile phone. He argued that the Order could have been specific to emails, Facebook posts or messages, sms text messages, WhatsApp messages, calendar and photos. His position is that there no limitation to the data requested, which amounted to a constitutional overreach and a significant invasion of privacy of the applicant. He further submitted that there was not even a limitation on the time within which the search could be undertaken.

[24] Mr. Cameron submitted that without this reference to any specific data or specific computer output the learned Parish Court Judge would not have been able to

determine whether the information was reasonably required for the purpose of a criminal investigation as per section 21(1) of the **Cybercrimes Act**.

[25] It was also his submission that on an examination of the orders the Parish Court Judge failed to ensure that any of the safeguards or measures that are statutorily required by section 21 of the **Cybercrimes Act** and the **Data Protection Act** to limit the invasion of the Claimant's privacy were followed through. There was also no mechanism in place to ensure that the statutory requirements are complied with or even any affidavit evidence or otherwise from the Jamaica Constabulary Force to indicate what measures or safeguards will be put in place.

[26] Additionally, Counsel took issue with the order directing the non-attendance of the Claimant during the production process. It was argued that the Claimant's attendance during the process is vital to ensure effective and practical compliance with the order to produce the data as her absence may give rise to challenges in properly understanding the specific nature and context of the data.

[27] Finally, it was submitted that the State's failure to disclose the evidence relied on when granting the Production Order and subsequently failing to provide the ex parte application and the supporting evidence to the constitutional court fundamentally undermined the ability of the Court to perform its constitutionally mandated function of reviewing the lower Court's decision. Counsel argued that this failure creates an insurmountable hurdle to the Claimant's right to challenge the constitutionality of the Production Order as the Court is not privy to the complete record of the lower court, thereby, impeding the Claimant's right to a fair hearing and the Court's ability to ensure the proper administration of justice.

[28] He argued that there is a duty of candour imposed on the State which mandates that all necessary information be provided, especially in matters relating to constitutional rights. He submitted that in the present case this duty was neglected and as such the Court should rule in favour of the Claimant. It was further submitted

that the State has not provided any basis to support its non-disclosure being demonstrably justified.

Defendant's Submissions

[29] Ms. Ruddock argued that the manner in which the ex-parte application for the Production Order was made and issued did not infringe the Claimant's right to privacy. Counsel indicated that the manner in which the application was made was done, not with a view to infringe Claimant's right to privacy but was a tactical approach on the part of the police. Counsel relied on the authority of **George Neil v. The Attorney General of Jamaica**[4].

[30] The Defendant submitted that there was no breach of the Claimant's constitutional right to privacy. Counsel argued that the right to privacy is not absolute and in the circumstances of the instant case the information sought pursuant to the Cybercrimes Act was required for an ongoing criminal investigation. Counsel for the Defendant argued that the objective of the Cybercrimes Act is to enable access to information to aid in solving crimes. It was submitted that the Production Order as well as the ancillary orders made, were carefully crafted to achieve this objective, and as such did not breach the Claimant's rights.

[31] Ms. Ruddock argued that based on section 21 of the Cybercrimes Act, there is no indication as to whether the application ought to be made *inter partes* as opposed to *ex parte*. In the circumstances, Ms. Ruddock submitted that by proceeding by an *ex parte* application was not unlawful or in contravention of the statute.

[32] It was submitted that the Parish Court Judge, having made the Production Order, pursuant to the Cybercrimes Act, ensured that safeguards were built in. Since the Order was made subject to the said Act, the police would be subjected to the safeguards stipulated in the Act. Miss Ruddock pointed to section 21 as examples

---

[4] [2022] JMFC Full 06 (para. 36)

from the Act that contained safeguards i.e.(a) subsection (14) (b) indicates the manner or period for which the key is to be retained and (c) limits the number of persons to whom the key is to be produced or made available. Section 21 (15) imposes a penalty for a constable who contravenes subsection (14). Therefore, the Claimant was protected by the safeguards in the Act as well as the order itself.

[33] It was argued in the alternative that in the event the court found that that there was a breach of the Claimant's right to privacy, the breach was demonstrably justifiable in a free and democratic society. It was argued that the Cybercrimes Act is directed at a proper purpose which is sufficiently important to override the right to privacy. The measure adopted to achieve the objective was also carefully designed with numerous safeguards both within the order and the Cybercrimes Act itself. The means (key) has also caused as little violation as possible and will be disposed of once the objective has been fulfilled. Finally, it was argued that there was clearly proportionality in the objective and the measures adopted to achieve the objective.

ISSUES

[34] The issues raised in this case are-

(a) whether the Production Order issued pursuant to section 21 of the Cybercrimes Act breached the Claimant' right to privacy?

(b) If there was a breach, was it proportionate?

(c) Were there other orders that could have been made by the Learned Parish Court Judge that would have been less intrusive?

(d) Were the orders made in the Production Order too wide and so breached the Claimant's right to privacy?

LAW & ANALYSIS

The Right to Privacy

[35] Section 13(j)(i), (ii) and (iii) of the **Charter of Fundamental Rights and Freedoms (Constitutional Amendment) Act**, 2011 provides as follows:

> *"(j) the right of everyone to: -*
>
> *(i) protection from search of the person and property*
>
> *(ii) respect for and protection of private and family life, and privacy of the home; and*
>
> *(iii) protection of privacy of other property and of communication;"*

[36] The Claimant has asserted that the Production Order and the Varied Production Order breached her rights as guaranteed under section 13(3)(j) of the Charter, in that the Claimant was deprived of her right to privacy.

The scope of the right to privacy

[37] The scope and the right to privacy has been examined in a number of cases. The cases point to the manner in which the Court should approach the issue of the right to privacy in a free and democratic society.

[38] The elements and scope of the right to privacy were examined by Sykes CJ at para 172 – 175 in **Julian J Robinson**. In citing from the majority judgment of **Justice K S Puttaswamy (Rtd)** (September 28, 2018), at para 174, Sykes CJ stated the following characteristics of the right to privacy: -

At page 98,

> *"521. In the Indian context, a fundamental right to privacy would cover at least the following three aspects;*
>
> - *Privacy that involves the person, i.e. when there is some invasion by the State of a person's rights relatable to his physical body, such as the right to move freely;*
>
> - *Informational privacy which does not deal with a person's body but deals with a person's mind, and therefore recognises that an individual may have control over the dissemination of material that is personal to him. Unauthorised use of such information may, therefore lead to infringement of his right; and*

- *The privacy of choice, which protects an individual's autonomy over fundamental personal choices..."*

Also at page 114,

> *"(iv) Privacy has both positive and negative content: The negative content restrains the State from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the State to take all necessary measures to protect the privacy of the individual…"*

And also at page 117,

> *"328. Informational privacy is a facet of the right to privacy. The dangers of privacy in an age of information can originate not only from the State but from the non-State actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the State. The legitimate aims of the State would include for instance protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits. These are matters of policy to be considered by the Union Government while designing a carefully structured regime for the protection of the data…"*

[39] The Canadian case of **Sheldon Wells Canfield v R**[5] relied on by Mr Cameron involved the constitutionality of a search of the claimants' personal electronic devices by Canadian Border Services Agency at an international airport while the appellants were entering into Canada foreign jurisdictions. The main issue was whether the search was in breach of their rights under section 8 of the Canadian Charter which guarantees the right to be secure against unreasonable search and seizure.

[40] The Court of Appeal of Alberta quoted from the case of **R v Fearon**[6], a case involving the search of a cell phone. In that case the Court found that the search incident of a cell phone had implications which differed from the search of other places. In examining the constitutionality of section 99(1) (a) of the Customs Act

---

[5] [2020] ABCA 383
[6] [2014] SCC 77

which purportedly provided the rationale for the search, the Court set out the test earlier referred by Mr Cameron. The Court pronounced that to claim protection under section 8, a Claimant must establish a reasonable expectation of privacy in the subject matter of the search, that is, that the person subjectively expected that it would be private and that this expectation was objectively reasonable".

[41] Further, that whether the Claimant had a reasonable expectation of privacy must be assessed in "the totality of the circumstances" The Court laid out four lines of inquiry to guide the determination of whether a Claimant has a reasonable expectation of privacy "in the totality of the circumstances". They are:

1. What was the subject matter of the alleged search?

2. Did the Claimant have a direct interest in the subject matter?

3. Did the Claimant have a subjective expectation of privacy in the subject matter?

4. If so, was the Claimant's subjective expectation of privacy objectively reasonable?

[42] The court in **Canfield** found that the Appellants had a direct interest in the subject matter of the search which was the data or informational content of their personal electronic devices and concluded that the matter concerned informational privacy: that is "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others. The Court went on to observe that although none of the Appellants had testified about their subjective expectation of privacy in the informational content of their electronic devices, the presumption that an individual's "direct interest and subjective expectation of privacy in the informational content of his computer can be readily inferred from the use of his laptop to browse the internet and to store personal information on the hard drive" would be applied. It was also decided that the same inference would be drawn in relation to the cell phone. The inference

was also drawn from one of the appellant's reluctance to provide his password. The Court also went on to opine that the following factors should be considered in assessing whether privacy expectations were objectively reasonable:

1. Possession, ownership or control of the property searched
2. The private nature of the subject matter searched
3. The place where the search occurred.

[43] The Court also considered the extent to which an expectation of privacy at a border was reasonable and concluded that that the law recognized some objectively reasonable expectation and that since the search of computer or cell phone represented a significant intrusion of personal privacy, to be reasonable, such a search must have a threshold requirement. The Court ultimately found that since the relevant section of the Customs Act permitted the unlimited search of personal electronic devices, it violated the protection against unreasonable search. The Court went on to consider whether section 99(1) of the Customs Act was a reasonable limit in accordance with section 1 of the Charter which guarantees the rights subject to reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society. The Court thereafter applied the **Oakes** test but still concluded that that the relevant section enabled substantial "deleterious effects to personal and digital privacy and that the provision could not be said to be a reasonable and demonstrably justified on Charter rights.

[44] In **R v Fearon**[7], the court considered privacy rights in the context of the search and seizure incident to an arrest of the appellant's phone without a search warrant. The Canadian Supreme Court determined that although any search of any cell phone had the potential to be a very significant invasion of a person's informational privacy interests, the invasion of the Claimant's privacy was not particularly grave,

---

[7] [2014] SCC 77

and the evidence garnered from the phone would be admitted. In the course of the judgment, the court stated that an assessment of the importance of the legitimate law enforcement objectives served by the search and of the nature and extent of the appellant's reasonable expectation of privacy was required. Also that more was required than simply to show that the arrest was lawful and the search was incidental to the arrest and was reasonably conducted.

[45] In the case of **Brake and another v Guy and Others**[8] the Claimants alleged that the Defendants had gained access to their e-mail accounts and other data held within those accounts, and thereafter shared the information with their lawyers and others, to include the Claimants' trustees in bankruptcy. The Claimants brought a claim against the Defendants, contending that by accessing and sharing the information, the Defendants had committed the equitable wrong of breach of confidence, and in accessing and retaining the information, they had committed the tort of misuse of private information, which had developed following the incorporation into domestic law of the European Convention on Human Rights.

[46] The Defendants sought to rely on the defence that there was a public interest in accessing, retaining and sharing the e-mails and the data contained in them (referred to as the iniquity defence), on the ground that the Claimants had allegedly been engaged in wrongdoing against creditors and insolvency officials. The Claimants contended inter alia that the iniquity defence was not available to defend a misuse of personal information claim, and that the only defences being those in article 8(2) and the other rights and freedoms in the Convention, such as article 10. The preliminary issue as to whether on the facts, the iniquity defence arose, was before the court for determination. In making submissions on behalf of the Claimant's contention that there was no "iniquity" defence available to a claim in the tort of misuse of private information, counsel directed the Court's attention to

---

[8] [2021] EWHC 670

the case of **Imerman v Tchenguiz**[9] where it was observed at paragraph 66 of that case that:

> *"66. As Lord Phillips's observation suggests, there are dangers in conflating the developing law of privacy under article 8 and the traditional law of confidence. However, the touchstone suggested by Lord Nicholls of Birkenhead and Lord Hope of Craighead in Campbell, paras 21 and 85, namely whether the claimant had a 'reasonable expectation of privacy' in respect of the information in issue, is, as it seems to us, a good test to apply when considering whether a claim for confidence is well founded. (It chimes well with the test suggested in classic commercial confidence cases by Megarry J in Coco v A N Clark (Engineers) Ltd [1969] RPC 41, 47, namely whether the information had the 'necessary quality of confidence' and had been 'imparted in circumstances importing an obligation of confidence'.)"*

[47] In making further submissions, the Claimants also pointed the court to another excerpt from the case of **JQL v NTP**[10] where the judge observed, at paras 134–135 that the general principles which relate to claims for misuse of private information involve applying a two-stage test: (1) does the claimant have a reasonable expectation of privacy in the relevant information; and (2) if yes, is that outweighed by countervailing interests, typically freedom of expression under article 10. Further that in assessing the question of expectation of privacy at the first stage, the considerations should be:

1. *what a reasonable person of ordinary sensibilities would feel if s/he were placed in the same position as the claimant and faced with the same publicity;*

2. *the court should consider all the circumstances to include(a) the attributes of the claimant; (b) the nature of the activity in which the claimant was engaged; (c) the place at which it was happening; (d) the nature and purpose of the intrusion; (e) the absence of consent and whether it was known or could be inferred; (f) the effect on the claimant; and (g) the*

---

[9] [2010] EWCA Civ 908; [2011] Fam 116,
[10] [2020] EWHC 1349 (QB),

circumstances in which and the purposes for which the information came into the hands of the publisher

3. *whether the availability in the public domain of the same or similar information leads to the conclusion that the claimant cannot have a reasonable expectation of privacy is a matter of fact and degree, to be assessed in the individual case: the question is not whether the information was generally accessible, but rather whether the remedy of injunction would serve a useful purpose.*

[48] The Judge went on to say that the second stage involved a balancing exercise and among other things, he said that there should be a balancing between article 8 and Article 10 rights and the justifications for interfering with or restricting each right must be taken into account. Further, the proportionality test must be applied, and that Courts need to be on guard against bringing into account at stage one considerations which should more properly be considered at stage two.

[49] The requirement for a proportionality test is built into our own constitutional provisions. Section 13(1) of the Charter of Fundamental Rights and Freedom provides that the "*provisions of this Chapter shall have effect for the purpose of affording protection to the rights and freedoms of persons as set out in those provisions, to the extent that those rights and freedoms do not prejudice the rights and freedoms of others*". Section 13(2) provides that the rights guaranteed under the Charter are subject to sections 18 and 49, as well as to sub-sections 9 and 12 of section 13. Certain rights are qualified, and those rights may therefore be derogated from where it is demonstrably justified in a free and democratic society. The rights guaranteed under section 13 (3) j are among those that are qualified as explained in section 13(2).

[50] The Privy Council has opined on the issue of right to privacy in the case of ***Attorney General v Jamaican Bar Association; General Legal Council v Jamaican Bar Association*** [2023] UKPC 6. The facts in that case were that The

Claimant/Respondent, the Jamaican Bar Association ('the JBA'), challenged aspects of the statutory regime for combatting money laundering (including ss 91A and 94 of the Proceeds of Crime Act ('POCA') and the Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order 2013). The appellant had claimed that its application to attorneys-at-law, violated, without demonstrable justification rights, sections 13 and 14 of the Constitution—namely privacy, liberty and the freedom from search of property. They had argued that those statutory provisions should be declared void.

[51] Lord Briggs and Lord Hamblen found at paragraphs 93 to 96 of the judgement that a fair balance had been struck. They reasoned that: -

> *[93] If, as the Court of Appeal found, the Regime infringed LPP then one could well understand the conclusion that aspects of the Regime are not proportionate given the importance and (almost) absolute nature of LPP. However, the Board has found that LPP is protected, and the infringement is of attorney-client confidentiality rather than LPP. That is a much less serious matter. Confidentiality is, for example, routinely invaded in civil litigation through the obligation to give inspection of relevant documents. This is justified by the need to get at the truth. The justification in the present context is as important, if not more so. Moreover, in civil litigation disclosure may well lead to the material being in the public domain, whereas disclosure under the Regime is controlled and, in many cases, will not extend beyond the GLC.*
>
> *[94] It is also of relevance that a number of protections have been built into the Regime. These include entrusting responsibility for monitoring compliance to the GLC rather than the FID and requiring there to be a nominated officer to receive internal reports and to make the decision as to whether a STR should be made.*
>
> *[95] The Regime has serious implications for the practice of attorneys and imposes obligations previously unknown to the legal profession. That said, lawyers are just one of the DNFBPs to which the Regime is applied and, in all cases, it is limited to the six activities, as recommended by FATF.*
>
> *[96] Having regard to all the considerations urged upon us by the parties, the Board's conclusion, bearing in mind in particular the very great importance of the objectives of the Regime for Jamaican society and the Jamaican economy, is that a fair balance has been*

> *struck and that the Regime is a proportionate measure, as the Full Court held.*

[52] What emanates from the foregoing is that a central question in assessing the Claimant's right to privacy is whether the claimant had a 'reasonable expectation of privacy in respect of the information in issue and that a proportionality test must be applied.

[53] In **R v Oakes**[11], the Canadian Supreme Court set out the criteria that must be satisfied in order to establish that a limit to a constitutional right is demonstrably justified in a free and democratic society. They are:

1. The objective which the measures responsible for a limit on a Charter right of freedom are designed to serve must be of sufficient importance to warrant overriding a constitutionally protected right or freedom.

2. Once a sufficiently significant objective is recognised, the party seeking to limit the Charter right must show that the means chosen are reasonable and demonstrably justified. This criterion involves a form of proportionality test. The courts will be required to balance the interests of the persons or groups whose rights are or are likely to be infringed, with those of society.

[54] Regarding the three important components of a proportionality test, the Court said at page 139 paragraph C:

> *"First, the measures adopted must be carefully designed to achieve the objective in question. They must not be arbitrary, unfair or based on irrational considerations. In short, they must be rationally connected to the objective. Second, the means, even if rationally connected to the objective in this first sense, should impair "as little as possible" the right to freedom in question…Third, there must be a proportionality between the effects of the measures which are responsible for limiting the Charter right or freedom, and the objective which has been identified as of "sufficient importance"."*

---

[11] [1986] 1 SCR 103

[55] Guidance was given with regards to the principle of proportionality in the case of **Julian Robinson v AG**[12] Mr. Julian Robinson, a Jamaican citizen, challenged the constitutionality of some provisions of National Identification and Registration Act (NIRA) on the grounds that some of the provisions of the Act will likely violate the right to equality, liberty, security and privacy guaranteed under the Jamaican Charter of Fundamental Rights and Freedoms Act, 2011 ("the Jamaican Charter") which are enshrined in the Constitution of Jamaica.

[56] Sykes CJ considered the underlying theme of the claim to be narrowed down to freedom and privacy. He cited the Canadian case of ***Big M Drug Mart Ltd***[13] on the nature of freedom and went on to opine at paragraph 173 that :-

> *the rights dealing with freedoms of thought, religion, peaceful assembly, movement and from discrimination are about being free from compulsion or restraint from doing or not doing something that one does not want to do when there is no compelling reason other than somebody else's views, including the executive's and legislature's, that one should do it.*

[57] To assess whether a legislation is "demonstrably justified in a free and democratic society", Justice Sykes relied on the proportionality test applied in the **Oakes** case but modified it in paragraph 108 to a four step criteria:

> *a) the law must be directed at a proper purpose that is sufficiently important to warrant overriding fundamental rights or freedoms;*
>
> *b) the measures adopted must be carefully designed to achieve the objective in question, that is to say rationally connected to the objective which means that the measures are capable of realising the objective. If they are not so capable then they are arbitrary, unfair or based on irrational considerations;*
>
> *c) the means used to achieve the objective must violate the right as little as possible;*
>
> *d) there must be proportionality between the effects of the measures limiting the right and the objective that has been identified as sufficiently*

---

[12] [2019] JMFC Full 04
[13] 18 DLR (4th) 321

> *important, that is to say, the benefit arising from the violation must be greater than the harm to the right.*

[58] Sykes CJ went on to address the fact that the court must assess the requisite breach and to balance the resulting consequences. He stated at paragraphs 109-110:

> *[109] In respect of (d), if the consequences of the measure on individuals or groups are very severe then the objective must be shown to be of great importance in order to justify the severity of the consequences and if this is not shown then the law will be unconstitutional.*
>
> *[110] It is at (d) that one finds the courts engaging in a balancing exercise. What is it that is balanced? The balancing that is being done arises because on the one hand there is a limiting law and on the other is the constitutional right or freedom. The court takes account of the benefit to be gained on the one hand and the harm on the other. What this requires is an assessment of whether the benefit to be gained by the violation is outweighed by the severity of the harm to persons. If the harm caused is greater than the benefit, then the law is unconstitutional. This component of the proportionality test is asking that there be a proper relationship between benefit to be gained and harm caused.*

[59] In **The Jamaica Bar Association v The Attorney General and The General Legal Council**[14], McDonald-Bishop JA observed that the proportionality test as outlined in **R v Oakes** (supra) has been modified. She said at paragraphs 517 and 518 of the judgment that:

> *[517] It has been noted by Andrew S Butler (Limiting Rights, page 569), that the Oakes' stipulation at item (ii) above, that in order to be proportionate, a limiting measure must impair the right or freedom "as least as possible" …"came to be regarded as too stringent and too demanding a standard", and so, has been modified. Shortly after R v Oakes, Dickson CJ in R v Edwards Books and Art Ltd, modified that requirement by applying the test of whether the law or the act in question infringes the protected right "as little as is reasonably possible". This is a less stringent test than that in R v Oakes. Indeed, as Andrew S Butler highlighted, there have been Canadian cases, which have replaced the minimal impairment test, which was the focus in R v Oakes, to the concept of "excessive impairment" as the measure (see R v Sharpe [2001] 1 SCR 43 at paragraph 78). This*

[14] [2020] JMCA Civ 37

> *gradual modification in the Oakes test is aimed at causing less restraint on the exercise of Parliament's law making power.*
>
> *[518] Given the default position in section 13(2) of the Charter, however, that the rights are guaranteed and ought to be preserved, as a general rule, it does seem reasonable to apply the Oakes test in its classic form. It was the classic minimal impairment test that the Full Court applied, albeit that at the time, it had been modified by Dickson CJ, himself, who had established the test in Oakes v R. I would not hold the Full Court to be wrong, in principle. However, since, the essence of the proportionality test involves a balancing exercise between the rights of Parliament to make laws for the peace, good order and government of the country and the rights of the individual to protection from state intrusion, it seems justified that some latitude is accorded to the exercise of Parliamentary discretion. The modified Oakes test that the law must infringe the right "as least as is reasonably possible" is endorsed as a better approach*

Issue: Whether the Production Order issued pursuant to Section 21 of the Cybercrimes Act breached the Claimants right to privacy guaranteed under Section 13(3)(j)(iii) of the Charter of Fundamental Rights and Freedoms

[60] Pursuant to Section 21 of the Cybercrimes Act, the Court has the power to issue a Production Order compelling the subject of the order, or who is in possession or control of data to surrender access to that data to an investigatory authority for the purpose of a criminal investigation or criminal proceedings. Section 21 states:

> *"21. –(1) A Resident Magistrate,[15] if satisfied on the basis of an application made by a constable, that any data or other computer output specified in the application is reasonably required for the purpose of a criminal investigation or criminal proceedings, may make an order under subsection (2).*
>
> *(2) An order under this subsection may require a person in possession or control of the data or other computer output to produce it in intelligible form to the constable…"*

[61] The right to protection of privacy in section 13(3)(j)(iii) provides that: -

> *"13. – (3) The rights and freedoms referred to in subsection (2) are as follows-*

---

[15] Now referred to as Parish Court Judge or Judge of the Parish Court

(j) the right to everyone to-

(iii) protection of privacy of other property and of communication;"

The **Constitution**, through section 13(2) of the **Charter of Fundamental Rights and Freedoms** provides that: -

> *"13. – (2) Subject to sections 18 and 49, and to subsections (9) and (12) of this section, and save only as may be demonstrably justified in a free and democratic society–*
>
> *(a) This Chapter guarantees the rights and freedoms set out in subsection (3) and (6) of this section and in sections 14, 15, 16 and 17; and*
>
> *(b) Parliament shall pass no law and no organ of the State shall take any action which abrogates, abridges or infringes those rights."*

[62] By virtue of section 19(1)[16] of the **Constitution**, the claimant alleges that she has been aggrieved by the issue of a production order pursuant to the Cybercrimes Act, and therefore seeks constitutional redress. The Court's understanding of the claim is that it is two-fold. The first part of the claim seeks to establish that section 21 of the Cybercrimes Act is unconstitutional because it does not contain adequate safeguards to protect the right to privacy of the subject of the order. The second aspect of the claim is that the production order breaches the claimant's right to privacy on the basis that is "exceedingly disproportionate and excessive".

[63] The starting point is that the fundamental rights and freedoms in section 13 of the Charter are universally and deeply protected human rights, and Parliament may pass no law which contravenes those rights and freedoms, unless that law is reasonably justified in the pursuit of a legitimate goal, aim or objective of the State.

[64] The test of constitutionality to be applied is seen in the authority of **Julian J Robinson** (supra) Batts J at para. 268 of the judgment expressed the test in the following terms: -

---

[16] See – section 19(1) and (2) of the Charter of Fundamental Rights and Freedoms

> *"The test of constitutionality of legislation now involves two stages, namely;*
>
> *A determination as to whether the law abrogates, abridges or infringes a guaranteed right; and*
>
> *Secondly, if it does, is the abrogation, abridgement or infringement demonstrably justified in a free and democratic society."*

[65] The burden and standard of proof is therefore on the Claimant to establish on a balance of probabilities the action of the State which infringes her fundamental right to privacy. Upon establishing that burden, the onus shifts to the Defendants to establish that the act which amounts to an infringement is reasonably or demonstrably justified in a free and democratic society. This test was reiterated by the Privy Council (per Lord Briggs and Lord Hamblen) at para. 26 of the judgment in the **JamBar** case.

[66] If an assessment utilizing the criteria established in the **Canfield** case as well as **Brake and another v Guy and Others**[17] is undertaken, then it may quite readily be said that the present claimant has established that she has a direct interest in the subject matter of the search. It is not in dispute that she is the owner of the instrument in relation to which the police wish to carry out the search. The cellular phone question is pass word protected. That fact is sufficient to show that the Claimant held a subjective expectation of privacy in the contents of the instrument. It is the Claimant's evidence that she is the managing director of a travel company and that she has information and software on the phone in relation to the company's clients. She had earlier alluded to the fact of having photographs of her son in the phone when she asserted that a photograph had appeared in the media that could only have come from her phone. Counsel in his submissions made reference to the probable existence of other material in the phone but in relation to which there is no evidence. The contents deponed to is however sufficient in light of the fact that we are here dealing with a piece of electronic device that belonged

---

[17] Citation

to the Claimant. The fact of the circumstances of how the phone was retrieved is part of the totality of circumstances that must be considered and in this particular instance, the discussion of those circumstances may be more appropriate when considering whether the reasonable expectation of privacy in the subject matter of the search may be outweighed by countervailing interests; in other words, whether limiting the claimant's right to privacy is demonstrably justified. This will be done by applying the modified **Oakes** Test.

The test of proportionality – Whether the law is demonstrably justified

[67] The constitutionality of the Cyber Crimes Act has not been challenged. But to the extent that safeguards to protect privacy rights are built into the act, thereby obviating the need for those safeguards to have been incorporated into the Production Order that was granted, it is necessary to scrutinize the Act. It is widely accepted that section 21 of the Cybercrimes Act is an invasive investigative tool which seriously interferes with the constitutional right to protection of privacy guaranteed in section 13(3)(j)(iii) of the **Constitution of Jamaica** through the **Charter of Fundamental Rights and Freedoms (Constitutional Amendment) Act**.

[68] Parliament has made clear its intention to curtail or in other words restrict the right to protection of privacy in circumstances where, as the legislation suggests, based on investigations the data or computer device is connected to the commission of a criminal offence and is reasonably required to assist authorities with their criminal investigation or involvement in criminal proceedings connected with the matter.

[69] The requirement of ***"… save only as may be demonstrably justified in a free and democratic society…"*** means that any interference with the right to privacy must be necessary in order to satisfy a legitimate aim of the State. These are the relevant components of the test of proportionality Dickson CJ referred to in **Oakes**.

[70] It is a well-known fact that Jamaica, though a relatively small geographical area is plagued with very high crime rates. Jamaica has been experiencing a high and intermittently growing number of violent crimes against women and children across parishes over the past fifteen to twenty years. It is therefore a legitimate aim of the State to implement effective legislative measures to reduce crimes by strengthening the investigatory powers of the Jamaica Constabulary Force in the investigation of the specific crimes that fall under the ambit of the legislation.

[71] It is clear that the purpose of the Cybercrimes Act, which is to assist the police with investigations into these specific criminal activities and criminal organizations is a measure that is sufficiently and reasonably justified, given the seriousness of the risk and threat to public and national safety, in the event that the State fails to meet its obligation of enacting legislation with the primary objective of reducing these criminal threats. If this State obligation is not met by strict application of legislation, the safety and well-being of all citizens, as well as the peace, order and good governance of the Jamaican society will remain at risk.

[72] The proportionate and justified nature of the Act is further affirmed by the relevant safeguards that are included in the section authorizing the issue of production orders. Based on Strasbourg jurisprudence, which contains authorities from countries whose applicants seek the Court's guidance on the interpretation of Article 8 of the European Convention on Human Rights[18], the Article which embodies the universal **"Right to respect for private and family life"**, a component of the test of whether a law is proportionate and/or necessary is whether the law interfering with the right contains safeguards or guarantees necessary to preserve and protect the right as much as possible.

[73] The issue of whether safeguards in legislation was sufficient to deem the legislation reasonably justified and therefore constitutional was addressed in **The**

---

[18] Long title, "Convention for the Protection of Human Rights and Fundamental Freedoms"

Queen (On the Application of National Council for Civil Liberties (Liberty) v Secretary of State for the Home Department[19] A case which considered the compatibility of certain sections of the UK Investigatory Powers Act with Articles 8 and 10 of the European Convention on Human Rights. At para. 79 of the judgment delivered by Singh LJ and Holgate J, they stated the following: -

> *"Turning to the question of whether an interference is "necessary in a democratic society", in Weber v Saravia, at para. 106, the Court said:*
>
> *"The Court reiterates that when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, it has consistently recognised that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security … **Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse** … This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law …"*

[74] Once a Production Order is reasonably required for the purpose of a criminal investigation or criminal proceedings, the safeguards stated in section 21 that must be implemented in the order compelling access to private and personal data, in order to minimize any risk of breach of the individual's right to privacy these include: -

a) Describing the data or other computer output to which the production order relates;

b) Imposition of time limits on life of the production order;

---

[19] 2020 1 WLR 243; 2019 EWHC 2057.

c) Specifying what is to be produced and the form and manner of the production;

d) Requirement for the addressee of the order to keep secret the contents and existence of the order;

e) Limiting the production to what is proportionate to what is sought to be achieved;

f) Requirement of securely storing the key for the period it is required, after which the key should be destroyed; and

g) Limiting the persons with access to the key and copies of the key made to the minimum necessary.

[75] It is a question of fact and degree within the circumstances whether safeguards are adequate. However, certain factors that must be present include: (i) certainty by way of time limits and quotas in storing, accessing, retrieving, copying and destroying the data content; (ii) methods to ensure maintenance of the integrity, security, confidentiality and private nature of the data content for as long as it is stored; and (iii) limiting the necessity and use of the production order and the data content to which it refers to the specific objective being sought.

[76] The key consideration for adequacy of safeguards is whether the section of the legislation expressly and clearly indicates the scope and powers of the public authority and the manner in which the powers are to be exercised. This is to ensure that there is certainty and clarity in the intended interference and to guard against legislation arbitrarily interfering with the fundamental right being sought to be protected from that very interference.

[77] Section 21 (14) of the Cybercrime Act has embedded in its provisions what can best be described as inherent safeguards. It states that: - A constable who obtains an ancillary order shall ensure that such arrangements are made as are necessary for securing that-

> a) a key produced in pursuance of the order is used to obtain access to, or put into intelligible form, only data or other computer output in relation to which the order was made;
>
> b) every key produced in pursuance of the order is stored, for so long as it is retained, in a secure manner, and any records of such key are destroyed as soon as no longer needed to access the data or other computer output concerned or put it into intelligible form; and
>
> c) the number of- (i) persons to whom the key is produced or otherwise made available; and (ii) copies made of the key, is limited to the minimum that is necessary for the purpose of enabling the data or other computer output concerned to be accessed or put into intelligible form.

[78] The Varied Production Order granted by the Learned Parish Court Judge stated that, the key produced in pursuance of this Order shall be stored, for so long as it is retained, in a secure manner and any records of such key shall be destroyed as soon no longer needed to access and/or put into intelligible form the said communication data or other data. The number of persons to whom the key is produced or otherwise made available, and any copies made thereof, shall be limited to the minimum that is necessary for the purpose of enabling the communication data or other data to be accessed or put into intelligible form.

[79] It is a fair conclusion that the very wording of the Order coupled with the provisions of the Cybercrime Act provides the necessary safeguards.

[80] The European Court **in National Council for Civil Liberties** found that the legislative scheme established by the UK Investigatory Powers Act were compatible with convention rights in Articles 8 and 10 on the basis that it creates an important set of interlocking safeguards which are sufficient to meet the legal requirements of the Convention. The Court finds that in these circumstances, a similar scheme is present in the Cybercrimes Act. Subsections (7), (8), (11) and (14) of section 21 create a set of sufficient safeguards that can minimize the risk of infringement of the right to privacy enjoyed by individuals in section 13(3)(j)(iii) of the **Charter**.

[81] We therefore find that section 21 of the Cybercrimes Act contains the necessary safeguards sufficient to limit as much as possible, the harm or risk to enjoyment of the right to privacy and is therefore proportionate to the State's aim of improving investigative measures for the detection and investigation of serious crimes in a digitally and technologically advanced society, and therefore demonstrably justified in the circumstances.

The Data Protection Act

[82] The introduction of the EU General Data Protection Regulation, 2018 is an indication that there is a general consensus among international and domestic Tribunals of the need to strengthen measures for the protection of the democratic right to privacy, not only within physical spaces but also within virtual and digital spaces. If the State wishes to maintain the right to impose legislative interference on the fundamental right to privacy by creating an environment of surveillance, it must implement measures to ensure corresponding safeguards and guarantees are effectively in place.

[83] The introduction of the Data Protection Act is also a progressive step towards ensuring that the right to privacy does not lose its fundamental significance domestically but strengthens with judicial force. It is therefore accepted that with the general protection provided by the Act, there are general additional safeguards for data providers who choose to keep their personal data and private communication unencumbered and free from public and private sector interference.

[84] A comprehensive data protection framework ensures that data providers are aware of their rights in respect of their personal data when using online interfaces. A data provider's right to privacy is comprehensively protected, safeguarded or guaranteed by primary legislation when that data provider is aware of and can choose to determine, which of their data may be legally collected, stored and processed, to whom the data is being made available, where their data is being

stored and how it is being used. These safeguards extend to the right to requesting copies of a data provider's data in the possession and control of a data controller and the right to request that their personal data be deleted.

[85] The matter of whether this expansive fundamental right has been breached is a question of degree based on the facts and circumstances. The Court already accepts the evidence that section 21 of the Cybercrimes Act, is reasonable and necessary to achieve the legitimate aim of the State to strengthen investigatory powers of police authorities towards securing public safety and reducing and/or eliminating national security threats of increasing crime rates and violent criminal behaviour within a digitized society. The question is whether the Varied Production Order breached the Claimant's right to privacy.

[86] The case law on breach of the fundamental right to privacy is also wide in scope. The principles applicable to determining whether there is an infringement of the right are similar to those applicable in determining proportionality of legislation interfering with the right.

[87] The primary test is whether the judicial authority issuing the Production Order, failed to contemplate, consider and incorporate expressly in the Order, the necessary safeguards within the legislation, or failed to follow any other legal requirement under the Act, which resulted in an abrogation, abridgement or infringement of the right. The three main elements laid down in the case **R v. Oakes** are: -

1. What is the objective to be served by limiting the Charter right?

[88] The circumstances that led to the Production Order being requested is of great importance. The affidavit evidence of the Claimant is that GK had been traveling in a motor vehicle with her. The Claimant made a report to the police that the motor vehicle had been stolen. Shortly thereafter the motor vehicle was recovered with

the deceased body of GK and the iPhone, (for which the key is being requested by the police).

[89] The Original Production Order contained a request for information from cell sites. It is accepted that such cell site data does not exist on the phone and therefore could not be accessed from the Claimant's phone. It is also noted that the first Order did not include ancillary Orders for the protection of unwarranted searches of the Claimant's Phone. The Order was subsequently varied. It is the Varied Production Order that subsists.

[90] There is no doubt that it was necessary to carry out an investigation in the murder of GK. The Court finds that the objective therefore of the Varied Production Order is in furtherance of the investigation of the circumstances that led to the death of GK. The clear objective of the production order is to further the investigation into the murder of GK.

2. Are the means reasonable and demonstrably justified?

[91] The police must be able to utilise all tools at their disposal in an attempt to explore the circumstances leading to the death of GK. The Court finds that although the Production Order prima facie breached the privacy rights of the Claimant, the granting of the Production Order was reasonable in the circumstances where a murder was being investigated. The circumstances leading up to the murder is of importance, as the Claimant, in her affidavit, had indicated that she had given the deceased her iPhone to occupy his time whilst they were in the motor vehicle. It is unclear as to what may could have been captured on the phone that could possibly be of assistance to the police in their investigations. The Court finds that the breach of the constitutional right of the Claimant would be justified under the circumstances.

3. Is whether the breach was proportionate?

[92] **R v Oakes** states that with regard to proportionality:

(a) the measures must be fair and not arbitrary,

(b) carefully designed to achieve the objective in question and

(c) rationally connected to that objective.

(d) the means should impair the right in question as little as possible.

The accepted test which now replaces (d) above is that the means should impair the right in question as least is reasonably possible.

[93] The first issue under this aspect of proportionality is whether the Production Order is fair and not arbitrary. Counsel for the Claimant had submitted that the wording of the order would allow for the wholesale harvesting of all the information contained in the iPhone of the Claimant. His submission was that the words *any communication data or other data contained on the cellular phone* was too wide and would lead to a breach of the rights of the Claimant. He submitted that this was similar to the case of **R v Canefield** where the Court of Appeal in Canada had ruled: -

> *The law recognizes that individuals have some objectively reasonable expectations of privacy at the border. Both Simmons and the Customs Act, s 98 recognize that reasonable grounds are necessary before a strip search can be conducted. Moreover, body cavity searches "may raise entirely different constitutional issues for it is obvious that the greater the intrusion, the greater must be the justification and the greater the degree of constitutional protection": Simmons at para 28.*

[94] In assessing whether the Varied Production Order satisfied the test of proportionality a careful assessment of the actual wording of the order is necessary. It is noted that the wording of the Varied Production Order is much more restrictive than that which was proposed by Counsel for the claimant as it stated the purpose for which the data was being extracted. Incidental to the process of extraction was the necessity to interface with information in the Claimant's phone which was irrelevant to the investigation. The data to be extracted would have to be limited to the purpose stated in the order. The

circumstances under which the iPhone came to be in the possession of the police is also of great importance. The iPhone was retrieved from the vehicle that GK's body was recovered from. The Claimant stated in her affidavit that she had given the iPhone to GK to keep him occupied whilst he was in the vehicle. Based on these facts, it is understandable and reasonable that the investigators would wish to view and possibly utilise the contents of the iPhone to assist them in their investigation.

[95] The Court finds on assessment of the evidence before it that:

1. The objective of the investigating officer is the investigation concerning the death of GK.

2. The iPhone may be useful in the investigation and as such the request to retrieve potentially relevant data cannot be considered arbitrary and

3. That the relevant data would be rationally connected to the investigation.

Issue: Were there other orders that could have been made by the Learned Parish Court Judge that would have been less intrusive

[96] The final issue on this aspect of proportionality is whether the means impair the right in question as least as is reasonably possible? Counsel for the Claimant had argued that there were less intrusive methods that could be deployed by investigators that would not trample on the Claimant's right to privacy. In furtherance of this submission, the Claimant had highlighted two alternate approach that could have been adopted.

[97] Mr. Cameron, raised the issue as to whether the police could have utilised the Interception of Communication Act. Counsel argued that the same information would have been garnered under the Interception of Communication Act without breaching the claimant's right to privacy.

[98] The Interception of Communication Act defines electronic signature as: -

anything in electronic form which-

> *(a) is incorporated into, or otherwise logically associated with, any electronic communication or other electronic data;*
>
> *(b) is generated by the signatory or other source of the communication or data; and is used for the purpose of facilitating, by means of a link between the signatory or other source and the communication or data, the establishment of the authenticity of the communication or data, the establishment of its integrity, or both;*

It defines Intercept as: -

> *a communication means the-*
>
> > *(a) monitoring of transmissions made by wireless telegraphy to or from apparatus comprising in the network;*
> >
> > *(b) monitoring or modification of, or interference with, the network by means of which the communication is transmitted, so as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication, and "interception" shall be construed accordingly;*

[99] From a perusal of the Interception of Communication Act it would appear that the information that can be gathered and made the subject of an order is limited to information that had been transmitted. The Production Order that had been granted in this case was under the Cybercrimes Act. The Cybercrimes Act appears to focus on information and data that are located on computers. A telephone can be defined as a computer under the Cybercrimes Act. A computer is defined as: -

> *computer" means any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data and- (a) includes any data storage facility or electronic communications system directly connected to or operating in conjunction with such device or group of such interconnected or related devices; 2 (b) does not include such devices as the Minister may prescribe by order published in the Gazette;*

Whilst computer service is defined as: -

> *computer service" includes provision of access to any computer or to any function of a computer, computer output, data processing and the storage or retrieval of any program or data.*

[100] On a perusal, of the Cybercrime Act, the information that the investigating officers would have access to is wider than that available under the Interception of Communication Act. There is a possibility that events leading to the death of GK could have been captured on the iPhone as it was in his possession at the time of his death. We take this view having regard to the circumstances of the discovery of the iPhone. It would be foolhardy for an investigating officer to limit himself during an investigation to mere telecommunication transmissions based on these circumstances.

[101] The second issue raised by Counsel for the Claimant was that the data to be collected pursuant to the Production Order was unlimited. Mr. Cameron submitted that it is only in extreme situations where there is justification and adequate safeguards, that the right to privacy and the protection that it affords, may be trespassed upon.

[102] It is without doubt that the original Production Order had been lacking with regards to safeguards. The ancillary orders that could have been ordered under the Cybercrime Act had not been included in that order. The Claimant had challenged the original order and as such the Parish Court Judge had amended the order, to now include several safeguards. Counsel for the Claimant had submitted that despite the amendment, there were not enough safeguards in place in the order as it relates to the data that is to be collected. He referred the Court to Sections 26 and 28 of the Data Protection Act and urged the Court to acknowledge that there are no similar safeguards in the amended Production order.

[103] The Data Protection Act sought to establish standards by which data is collected and preserved. Section 26 and 28 state that –

> *26. The third standard is that personal data shall be adequate, relevant, and limited to what is necessary for the purposes for which they are processed.*

28.- (1) The fifth standard is that—

(a) personal data processed for any purpose shall not be kept for longer than is necessary for that purpose; and

(b) the disposal of personal data by a data controller shall be in accordance with regulations made under section 74.

The question is whether the ancillary orders in the amended Production order establish safeguards with regards to the Claimant's data?

[104] The ancillary orders in the amended Production Order states that: -

i) Mrs. Amoi Leon-Issa shall not be entitled to be present during the accessing and/or producing in intelligible form the said communication data or other data however an Attorney-at-Law instructed by her may attend as an observer only.

ii) In the event the Attorney-at-Law so instructed is unable to be present, the process of accessing and/or producing in intelligible form the said communication data and other data shall not, on that account only, be postponed or otherwise delayed but may proceed in the absence of such Attorney-at-Law.

iii) A third party, being a qualified computer expert mutually agreed upon by counsel for the Jamaica Constabulary Force and counsel for Mrs Amoi Leon-Issa, may attend as an observer only the process of accessing and/or producing in intelligible form the said communication data or other data.

iv) In the event a qualified computer expert cannot be mutually agreed upon by counsel for the Jamaica Constabulary Force and counsel for Mrs Amoi Leon-Issa by the 22nd day of November 2022, the process of accessing and/or producing in intelligible form the said communication data or other data shall not, on that account only, be postponed or otherwise delayed but may proceed in the absence of that third party. Every key produced in pursuance of this Order shall be stored, for so long as it is retained, in a secure manner and any records of such key shall be destroyed as soon as no longer needed to access and/or put into intelligible form the said communication data or other data. The number of persons to whom the key is produced or otherwise made available, and any copies made thereof, shall be limited to the minimum that is necessary for the purpose of enabling the communication data or other data to be accessed or put into intelligible form.

[105] As stated earlier, the amended Production Order was limited to retrieving data that related to the death of GK. This would be similar to the third standard under the

Data Protection Act. Secondly, section (iv) of the amended Production Order speaks the fact that the information should be destroyed when no longer needed. The Court is aware that the Data Protection Act had not been operational at the time that the amended Production Order had been granted. We note that there were other ancillary orders made established which granted more than adequate safeguards for the Claimant. The Ancillary order: -

a. Allowed the Claimant to have an attorney at law present at the time of the extraction of the data on her iPhone.

b. Allowed the Claimant to have computer expert present when the data was being extracted.

c. Limited the number of persons who would have access to the key and the copies made of the data.

[106] Although this had not been argued, it is noted that the Cybercrimes Act established penalties that can be imposed if there is any breach of the Cybercrimes Act. We therefore find no favour with the submissions of Counsel for the Claimant as it relates to insufficient safeguards.

[107] The final aspect of proportionality that is to be decided is what is the effect of the limiting measure as per the objective? The objective in this case is the investigation of the death of a child. The Claimant may view the extraction of the data from the iPhone as less than desirous, however, under the circumstances where it may assist with the murder investigation, we find that the Order made was not overarching and based on the evidence, we conclude that it would be proportional to make an order that the key to access the iPhone be produced.

Issue: Whether there should have been disclosure of the Application and the affidavit in support that was filed and placed before the learned Judge of the Parish Court

[108] The issue is whether there should have been disclosure of the application and the affidavit that was submitted to the Parish Court Judge at the time the ex-parte application had been made. Counsel for the Claimant had submitted that the lack of disclosure to either himself or to the Court at this stage breached the Claimant's right to privacy. Counsel's position was that the present panel should have been privy to the information, to make an informed decision on this matter.

[109] In considering this issue we considered the dicta in the case of **Bobette Smalling v Dawn Satterswaite** [2022] UKPC 44 where Lord Stephens at paragraph 56 of the judgement stated that: -

> *Before any of these investigatory orders can be made a judge has to be satisfied that there are reasonable grounds for believing that:*
>
> > *(a) the information or material is likely to be of substantial value, whether or not by itself, to the investigation for the purposes of which the order is sought ("the substantial value condition"); and*
> >
> > *(b) it is in the public interest for the information or material to be produced or for access to the information or material to be given, having regard to the benefit likely to accrue to the investigation if the information or material is obtained ("the public benefit condition").*

This rational can be applied to any application for a Production Order as the Cybercrime Act has a similar provision where Section 21 (1) states that:

> *A Resident Magistrate, if satisfied on the basis of an application made by a constable, that any data or other computer output specified in the application is reasonably required for the purpose of a criminal investigation or criminal proceedings, may make an order under subsection (2).*

[110] Although the actual application and affidavit were not disclosed to the Court, it is clear from the circumstances of this case that a production order could have been granted. In the affidavit of Her Honour Mrs. Sasha Marie Ashley she stated in particular at paragraphs 11,15,17 & 19 extracted as follows;

> **11. The hearing was conducted in chambers as it concerned a *sensitive matter which had national security concerns as well.***

> ***15. Having heard both parties I was satisfied that the data was reasonably required for the purpose of the criminal investigation in the murder of GK who was the nine- year old son of the Claimant***
>
> ***17. I also took into consideration that the Court must at all times protect the public interest by ensuring the course of justice is not perverted nor any attempt made to pervert the course of justice. To that end I addressed my mind to the provisions that may be included in a Production Order to safeguard the rights of Mrs. Issa guaranteed her under the Constitution. I only considered what was relevant to the hearing of the application.***
>
> ***19. I made the orders in a manner which safeguarded the Claimant's rights as far as possible having regard to the important objective of the criminal investigation into the death of GK, son of the Claimant.***

[111] We conclude based on the fact that the phone was in the motor vehicle in which of the deceased was found that there could possibly be information on the iPhone that could be of substantial value. Further we conclude it is would be in the interest of the investigation for this information to be produced.

[112] Secondly, it is noted that the investigation is in its initial stage and as such there is no duty to disclose such documents. This was found to be the position in the Canadian case of ***R v Gills***[20]. The issue in that case was whether the certificate for a Breathalyzer could be admitted into evidence in light of the fact that the police officer had not allowed the appellant to read the breathalyser readings as his breath samples were being analysed. Fraser CJA stated at paragraph 7 of his decision that: -

> *"Further, a person suspected of having committed a criminal offence has no right to disclosure unless and until he has been charged with a criminal offence. The reason is that disclosure is designed to ensure that an accused knows the case he has to meet. Unless and until he has been charged, there can be no conviction and there is no case for him to meet.*

---

[20] 1994 ABCA 21

> *Here no charges had been laid at the time that the appellant took the breathalyser test."*

[113] In this case there is no evidence that the Claimant is a suspect in this case. The police officers are at the stage that they are seeking to gather information during the course of their investigation. We cannot agree with counsel for the claimant that the non-disclosure of the contents of the application and the supporting affidavit breached the Claimant's right to privacy. It is understandable, based on the circumstances of this case, as to why a Production order had been requested by the investigating officers to further their investigation.

[114] Mr. Cameron also submitted that the Production Order breached the Claimant's right to a fair hearing as is guaranteed by the Charter of Fundamental Rights and Freedoms. The Fixed Date Claim Form paragraphs K and I reference was made to Section 16 (1), however we conclude that was a typographical error and the relevant section is 16(2) which refers to civil liberties.

[115] He argued that the initial Order made in her absence and the failure to make full and frank disclosure to the Court resulted in the Court making an Order with regard to cell site data which was never on the phone and could not be produced by the Claimant. Counsel argued that the refusal of the Claimants application for disclosure and the failure to provide to this Court the documents that were placed before the Learned Parish Judge further breached the Claimants right to a fair hearing.

[116] Section 16(2) of the Charter of Fundamental Rights and Freedoms provides:

> *"In the determination of a person's civil rights and obligations or of any legal proceedings which may result in a decision adverse to his interests, he shall be entitled to a fair hearing within a reasonable time by an independent and impartial court or authority established by law."*

[117] A Right to a fair hearing encompasses established principles that parties have a right to be heard and to know and respond to allegations made against them.

Edwards JA in **Al-Tec Inc. Ltd. v James Hogan and Renee Latibudaire**[21] assessed the right to a fair trial in some detail. She noted that the right is not absolute and may be abrogated pursuant to the provisions of section 13(2) of the Charter. In analysing the "Right" she made reference and drew a comparison with Article 6 (1) of the European Convention of Human rights which provides:

> *"In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice."*

[118] In analysing the right to fair trial Edwards JA extracted from **Beles and Others v The Czech Republic**[22] where it was said as follows:

> ***"The Court has already stated on a number of occasions that the right to a fair trial, as guaranteed by Article 6(1) of the Convention, must be construed in the light of the Rule of Law, one of the fundamental aspects of which is the principle of legal certainty, which requires that all litigants should have an effective judicial remedy enabling them to assert their civil rights…. …the 'right to a court', of which the right of access is one aspect, is not absolute. It is subject to limitations permitted by implication, in particular where the conditions of admissibility of an appeal are concerned, since by its very nature it calls for regulation by the State, which enjoys a certain margin of appreciation in this regard… nonetheless, the limitations applied must not restrict or reduce the individual's access in such a way or to such an extent as to impair the very essence of the right. Furthermore, limitations will only be compatible with Article 6(1) if they pursue a legitimate aim and there is a reasonable relationship of proportionality between the means employed and the aim pursued. See Guerin v France judgment of 29 July 1998, Reports 1998-V, p 1867 & 37." (Emphasis added)]***

---

[21] [2019] JMCA Civ 9,
[22] Application No. 47273/99 ECHR 2002 (unreported) judgment delivered November 12, 2002

[119] It is our considered view that in the case at bar the circumstances provide and permit the tribunal to impose limitations on the "right" of the Claimant, in furtherance of a legitimate aim. We find that there was no breach of the Claimant's right to a fair hearing pursuant to Section 16(2) of the Charter of Fundamental Rights and Freedoms.

CONCLUSION

[120] We find that although there would be a breach of the Claimant's right to privacy, it was proportional in a free a democratic society. The Court finds that the request for the key to access the data on the iPhone would be limited to investigation into the death of GK on the 13th of January 2022. It is our considered conclusion and finding that the benefit gained from granting the varied Production Order that would aid in the investigation into the death of GK far outweigh the breach of the privacy of the Claimant.

ORDERS

1. The Claimant is not entitled to any of the declarations sought in the Fixed Date Claim Form.

2. An order quashing the orders granted by the learned Parish Court Judge, Sasha-Marie Ashley on 6 September 2022 and 18 November 2022 is refused.

3. The Court does not find that the amended Production order granted on the 18th of November 2022 to be unconstitutional, void and of no legal effect.

4. An Order for vindicatory damages on the footing that the actions of the 1st, 2nd and 3rd Defendants amounts to a breach of the Constitutional rights granted to the Claimant by the Charter of Fundamental Rights and Freedoms and Cybercrimes Act, is refused.

5. The Claimant is to produce the key to the iPhone as per the Varied Production Order made by Her Honour Mrs Sasha Marie Ashley on the 18th November 2022, no later than 29th of September 2023 by 4p.m.

6. No order as to cost.