

# The Cybercrime Act 2018 of Guyana

## *Offence Architecture, Intimate-Image Offences and the Rights Balance*

Naomi Eglantine Christie

September 2026

---

Naomi Eglantine Christie · LL.B. (Distinction) · L.E.C. (Honours) · LL.M., New York University, 2015 — International Legal Studies · Attorney-at-Law, admitted to the Bar of Guyana, October 2013, and to the Bar of Grenada, 2014. Correspondence: [naomi@christiejustuslaw.com](mailto:naomi@christiejustuslaw.com).

### Abstract

Guyana's Cybercrime Act 2018 was enacted after a two-year passage dominated by objection to a sedition clause that was excised on the night the Bill passed. This paper asks whether the Act that survived strikes a defensible balance between the suppression of the harms it was written to suppress and the constitutional guarantee of expression. It argues that the Act contains two architectures stitched together. The first, in sections 3 to 13, is a computer-misuse core drafted around the integrity of systems and data on the pattern of the Convention on Cybercrime; it is technically sound. The second, in sections 14 to 19, is a set of content and conduct offences drafted around harm to persons and to the polity, and there the rights balance is struck unevenly. Section 16, the intimate-image offence, is consent-based, fills a real gap in Guyanese law and survives the de Freitas proportionality test. Sections 18 and 19 are drawn broadly enough to attract the vagueness objection the Caribbean Court of Justice sustained in *McEwan* and to collide with the principle in *Hector* that those in public office must remain open to criticism. Each section is read from the Gazette text against the Constitution, the treaty it follows, and the statutes of Jamaica and the United Kingdom. A narrowing construction of sections 18 and 19 is available now and the courts should adopt it; targeted amendment is a better course than the promised repeal. Part III's investigative powers presuppose safeguards the Data Protection Act 2023 was written to supply, and that Act has not been commenced.

**Keywords:** cybercrime; Guyana; freedom of expression; intimate images; vagueness; proportionality; Convention on Cybercrime; data protection

## I. Introduction

At forty-eight minutes past ten on the night of Friday 20 July 2018, the National Assembly of Guyana read the Cybercrime Bill a third time and passed it as amended.<sup>1</sup> The sitting had opened at nine minutes past two. The debate had run for more than five hours before the House suspended its own standing order in order to sit until the Bill was disposed of, and the clause that had brought the Guyana Press Association, the Guyana Human Rights Association, the National Toshias Council, a telephone company and the Leader of the Opposition into a single chorus of objection had been cut out by the Government's own amendment an hour before the vote.<sup>2</sup> The Act received the President's assent and was published in the Official Gazette on 13 August 2018 as Act No 16 of 2018.<sup>3</sup>

What survived that night is the subject of this paper. The question is whether the Cybercrime Act 2018, read as it stands, strikes a defensible balance between the suppression of the harms it was written to suppress and the guarantee of expression in article 146 of the Constitution. The question is not academic. Since 2018 the Act has been used to charge a caterer, an information technology technician, a photographer, members of the National Assembly, a mayor, a visiting businessman and a man who posted a status on WhatsApp about a Permanent Secretary; the Attorney General has announced its repeal and, later, its revision; and in December 2025 a magistrate's court halted a prosecution to receive written submissions on whether a charge of using a computer system to humiliate could be sustained at all.<sup>4</sup> The politics of the Act are well known. The architecture is less so, and it is the architecture I examine here.

The argument advanced here is that the Act contains two architectures stitched together. The first, in sections 3 to 13, is a computer-misuse core drafted around the confidentiality, integrity and availability of computer systems and data. It follows, at times word for word, the pattern of

<sup>1</sup> Guyana, National Assembly Debates (Hansard), 93rd Sitting of the First Session of the Eleventh Parliament (20 July 2018) 103 ("Bill reported with amendments, read the third time and passed as amended. 10.48 p.m."). The Assembly convened at 2.09 pm: *ibid* 1.

<sup>2</sup> Hansard (20 July 2018) 94 (suspension of Standing Order No 10(1) on the motion of the Prime Minister), 102–103 (amendments to clause 18). For the objectors see 'PPP/C proposing deletion of sedition clause from cyber crime bill' *Stabroek News* (Georgetown, 20 July 2018); 'GPA says sections in Cybercrime Bill "criminalizing freedom of expression" must go' *iNews Guyana* (Georgetown, 2 May 2018).

<sup>3</sup> Cybercrime Act 2018 (Guyana), Act No 16 of 2018, Official Gazette (Legal Supplement A), 13 August 2018. The Gazette copy records assent on 13 August 2018 and carries the Clerk's endorsement "Passed by the National Assembly on the 20th July, 2018" over the reference "(BILL No. 17/2016)". The Act is cited hereafter as "Cybercrime Act 2018".

<sup>4</sup> 'Caterer charged with uploading woman's nude images' *Stabroek News* (Georgetown, 31 August 2023); 'Man on \$150k bail for publishing nude pictures of ex-girlfriend' *Kaieteur News* (Georgetown, 23 July 2024); 'One witness called in cybercrime trial of photographer' *Stabroek News* (Georgetown, 6 January 2023); 'Cybercrime Act to be repealed – AG' *Stabroek News* (Georgetown, 19 December 2022) (charges against a mayor and a member of the National Assembly; announcement of repeal); 'Court dismisses cybercrime charge against US businessman' *Stabroek News* (Georgetown, 28 February 2026); 'Case dismissed against man over cyber "humiliation" of Home Affairs PS' *Stabroek News* (Georgetown, 27 July 2023); Ministry of Legal Affairs (Guyana), 'Nandlall announces revision of cybercrime law' (Georgetown, 25 September 2024); 'Court halts cybercrime prosecution to address novel challenges to speech-based offences in Guyana' *Demerara Waves* (Georgetown, 21 December 2025).

the Council of Europe's Convention on Cybercrime, which the Attorney General told the House had been relied on "particularly" in the drafting, and it is technically sound.<sup>5</sup> The second, in sections 14 to 19, is a set of content and conduct offences drafted around harm to persons and to the polity: child pornography, child luring, the publication of intimate images, mass messaging, offences against the State, and the use of a computer system to coerce, harass, intimidate or humiliate. Only the first of these has a treaty model. It is in the second architecture that the rights balance is struck, and it is struck unevenly. Section 16, the intimate-image offence, is a well-targeted, consent-based provision that fills a real gap in Guyanese law and is defensible under article 146 read with the proportionality test the Privy Council formulated in *de Freitas*.<sup>6</sup> Sections 18 and 19 are drafted in terms broad enough to attract the vagueness and overbreadth objections that the Caribbean Court of Justice sustained in *McEwan*,<sup>7</sup> and to collide with the principle, stated for the Board by Lord Bridge in *Hector*, that those who hold public office must always remain open to criticism.<sup>8</sup>

Two further claims follow. A narrowing construction of sections 18 and 19 is not merely available but required: the mental element and the harm element of each offence should be read restrictively, speech on matters of public interest about the conduct of public administration should be treated as outside section 19, and section 18 should be read in the light of the sedition clause that was cut out of it. And targeted amendment is preferable to the repeal that has been promised, because the integrity core and section 16 are worth keeping and the defects of sections 18 and 19 can be cured by subtraction. Section VI then treats the investigative powers of Part III, several of which go beyond anything the Convention requires, against the constitutional protection of the person, property and correspondence, and against a Data Protection Act that was enacted in 2023 and, at the date of writing, has not been brought into operation.<sup>9</sup>

The method is textual and comparative. Every section discussed is read from the Gazette text. The comparators are confined to instruments whose text could be read directly: the Convention on Cybercrime as registered with the United Nations, the United Nations Convention against Cybercrime as published by the Office on Drugs and Crime, the Cybercrimes Act of Jamaica, and the relevant sections of the United Kingdom's Criminal Justice and Courts Act 2015 and Online Safety Act 2023. The paper takes no position on Guyana's treaty relationship with the Convention on Cybercrime, which could not be verified against the Council of Europe's treaty records at the time of writing; it notes only that accession by a state outside the Council presupposes legislation already in place, as the Parliament of Trinidad and Tobago's Joint Select Committee recorded in 2019 when it observed that its own country "is unable to sign on as a party to the Budapest

<sup>5</sup> Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) 2296 UNTS 167, ETS No 185 (hereafter "Convention on Cybercrime"). For the drafting models see Hansard (20 July 2018) 2–3 (Attorney General: "conventions, model laws and precedent from other jurisdiction were relied upon, particularly the Budapest Convention on Cybercrime", together with the HIPCAR model texts, the 2014 Cybercrime Bill of Trinidad and Tobago, the 2015 Cybercrimes Act of Jamaica, the Electronic Crimes Bills of Grenada and Saint Vincent and the Grenadines, and the United Kingdom's Computer Misuse Act 1990).

<sup>6</sup> *de Freitas v Permanent Secretary of Ministry of Agriculture, Fisheries, Lands and Housing* [1999] 1 AC 69 (PC) 80.

<sup>7</sup> *McEwan v Attorney General of Guyana* [2018] CCJ 30 (AJ).

<sup>8</sup> *Hector v Attorney-General of Antigua and Barbuda* [1990] 2 AC 312 (PC) 318.

<sup>9</sup> Data Protection Act 2023 (Guyana), Act No 18 of 2023, s 1; 'Digital ID law now active, but data protection act still not operational' *Demerara Waves* (Georgetown, 31 March 2026). See section VI.C below.

Convention because the Convention requires members to have cybercrime legislation and the requisite legal framework already in place".<sup>10</sup> Nor does the paper take any position on the outcome of proceedings now pending in the magistrates' courts. It describes the record and stops.

## II. Enactment history

The Act had a long gestation for a statute of forty-three sections. The Attorney General told the House at the second reading that a draft Bill had been posted on the website of the Ministry of Legal Affairs in September 2015 for comment, that comments had been received between October 2015 and March 2016, and that a public consultation had been held at the Pegasus Hotel on 16 March 2016 with the Director of Public Prosecutions, the Revenue Authority, the Rights of the Child Commission, the women's organisation Red Thread and the Bar Association among those attending.<sup>11</sup> The draft was also published in the Official Gazette at the end of December 2015, and its content was reported at the time: a suite of computer-misuse offences carrying three million dollars and three years on summary conviction, a child pornography offence, and a "violation of privacy" offence directed at the capture, storage, publication or transmission of an image of a person's private area without consent "where the other person has a reasonable expectation that he could disrobe in privacy".<sup>12</sup> That last phrase will matter in section IV, because it did not survive.

The Bill was sent to the National Assembly on 3 August 2016, published on 4 August 2016 as Bill No 17 of 2016, read a first time the same day and referred to a Special Select Committee.<sup>13</sup> The Committee held its meetings between March 2017 and April 2018, and its report was tabled on 26 April 2018.<sup>14</sup> While the Bill was in committee it was reviewed by a cybercrime specialist made available to the Attorney General's Chambers through the International Senior Lawyers Project, and the Attorney General told the House that most of the specialist's comments had been incorporated.<sup>15</sup>

The controversy that followed the tabling of the report concerned clause 18. As reported, clause 18(1) provided that a person committed the offence of sedition if the person, whether in or out of Guyana, intentionally published, transmitted or circulated by use of a computer system a statement, text, video, image, sign or visible representation that "brings or attempts to bring into hatred or contempt, or excites or attempts to excite disaffection towards the Government established by law in Guyana"; clause 18(4) defined disaffection to include "disloyalty and all feelings of enmity" and then set out the traditional savings for comments expressing

<sup>10</sup> Parliament of Trinidad and Tobago, *Final Report of the Joint Select Committee on the Cybercrime Bill, 2017* (Fourth Session, Eleventh Parliament, 2019) 52 (Appendix I, clause-by-clause examination, clause 20). The Committee's current statute is the Computer Misuse Act, Chap 11:17, which it compared with the Bill: *ibid* 30.

<sup>11</sup> Hansard (20 July 2018) 3.

<sup>12</sup> 'Cybercrime bill targets child porn, hacking, identity theft' *Stabroek News* (Georgetown, 29 December 2015) (reporting the draft "published on the site of the Official Gazette" and quoting the privacy clause); 'Cyber Crime law to prohibit child porn, sharing of nude images' *Demerara Waves* (Georgetown, 28 December 2015). Both are cited for the fact and reported content of the publication, not as authority for the text.

<sup>13</sup> Hansard (20 July 2018) 3.

<sup>14</sup> Hansard (20 July 2018) 3 (Attorney General: before the Committee "from 4th August, 2016 to 9th April, 2018", report tabled 26 April 2018); *ibid* 63 (Opposition Chief Whip: the Committee "was set up in March, 2017" and held seven meetings between then and April 2018). See also 'Sedition and cybercrime' (editorial) *Stabroek News* (Georgetown, 30 April 2018) (final meeting 8 April 2018; report circulated 26 April 2018).

<sup>15</sup> Hansard (20 July 2018) 3.

disapprobation of the measures of the Government with a view to their alteration by lawful means.<sup>16</sup> The penalty was five years' imprisonment, rising to life where death resulted.<sup>17</sup> The Opposition Chief Whip, who had sat on the Committee, told the House that the 2015 draft had contained no sedition clause and that the offence had entered with the 2016 Bill.<sup>18</sup> Within a week of the report's tabling the Leader of the Opposition had described the clause as a retrograde step with "no place in a democratic, in a free Guyana";<sup>19</sup> the Guyana Press Association, marking World Press Freedom Day, called on both sides of the House to delete provisions that "will amount to institutionalisation of criminal defamation";<sup>20</sup> the telephone company GTT wrote that the offence "seeks to limit the press and freedom of speech against the Government and should be struck from the draft";<sup>21</sup> and the Guyana Human Rights Association, the Working People's Alliance, the National Toshias Council and Transparency Institute Guyana Inc took the same position in public.<sup>22</sup> Reporters Without Borders raised a distinct objection to clause 9, which made the unauthorised receiving of electronic data an offence and could, they said, be used against journalists who published material from a confidential source.<sup>23</sup>

The Government's response was to refer the Bill back to Cabinet. Cabinet decided to delete subsection (1)(a); consequential changes were made; and the clause was redrafted by the Drafting Division "in collaboration with a free speech and media attorney" from the same International Senior Lawyers Project.<sup>24</sup> Two rival amendments therefore reached the House on 20 July 2018. The Opposition's, under the hand of the Chief Whip, read "Offences of Sedition – Delete entire clause 18 (1) – (4)"; it was put and negatived. The Attorney General's substituted a new clause 18 headed "Offences against the State"; it was agreed to.<sup>25</sup> Clause 9 was replaced by the narrower provision that now stands as section 9; an Opposition amendment to add the Guyana Elections

<sup>16</sup> 'Sedition and cybercrime' (editorial) *Stabroek News* (Georgetown, 30 April 2018), quoting clauses 18(1) and 18(4) of the Bill as reported from the Committee; 'PPP/C proposing deletion of sedition clause from cyber crime bill' *Stabroek News* (Georgetown, 20 July 2018), quoting clause 18(1) in the same terms. Bill No 17 of 2016 as printed could not be retrieved from parliament.gov.gy at the date of writing; the clause is described from these reports.

<sup>17</sup> 'Sedition and cybercrime' (editorial) *Stabroek News* (Georgetown, 30 April 2018) ("comes with a five-year prison sentence"); 'Controversial sedition clause removed as amended Cybercrime Bill passed' *Kaieteur News* (Georgetown, 21 July 2018) (a life sentence "where death occurs").

<sup>18</sup> Hansard (20 July 2018) 63 ("The original 2015 Bill never had any insertion of a sedition clause ... The 2015 Bill, which went through some form of consultation, did not include clause 18 which deals with sedition.").

<sup>19</sup> 'Gov't converted Cybercrime Bill to protect their interest – Opposition Leader on Clause 18' *iNews Guyana* (Georgetown, 30 April 2018).

<sup>20</sup> 'GPA says sections in Cybercrime Bill "criminalizing freedom of expression" must go' *iNews Guyana* (Georgetown, 2 May 2018).

<sup>21</sup> *ibid*, reporting GTT's correspondence of 25 April 2018. The same passage of the letter was read to the House: Hansard (20 July 2018) 23.

<sup>22</sup> 'PPP/C proposing deletion of sedition clause from cyber crime bill' *Stabroek News* (Georgetown, 20 July 2018) (Guyana Human Rights Association, Working People's Alliance, National Toshias Council); 'Controversial sedition clause removed as amended Cybercrime Bill passed' *Kaieteur News* (Georgetown, 21 July 2018) (Transparency Institute Guyana Inc).

<sup>23</sup> Hansard (20 July 2018) 4; 'Controversial sedition clause removed as amended Cybercrime Bill passed' *Kaieteur News* (Georgetown, 21 July 2018).

<sup>24</sup> Hansard (20 July 2018) 7 ("In response to those criticisms the Attorney General referred the Bill back to Cabinet for its consideration. The Cabinet ... decided on deleting subsection (1)(a) which was the main cause of concern.").

<sup>25</sup> Hansard (20 July 2018) 102–103.

Commission to the critical infrastructure protected by clause 12 was negated; clauses 13 to 17 and 19 to 43 were agreed to without amendment.<sup>26</sup> The Attorney General's closing words were that "the State has a right to protect itself", that the Government had been "prepared to accommodate the concerns raised in relation to clause 18 (1)(a) and that is why we excised it", and that "the rest of the provisions in clause 18 are sound provisions".<sup>27</sup> The Bill was reported with amendments, read a third time and passed. One fact in that record bears on section V below. Section 19 was never amended at any stage: it went through the Special Select Committee and the Committee of the whole House in the form in which it had been drafted, while the argument of two years was spent entirely on its neighbour.

The Act did not settle the argument. In December 2022 the Attorney General of the succeeding administration told the press that the Act would be repealed and replaced by "a modern Act formed out of recommendations" of the United Nations convention then under negotiation, and that the replacement would be "a model cybercrime Bill for the CARICOM region".<sup>28</sup> That convention was adopted by the General Assembly on 24 December 2024 by resolution 79/243 and opened for signature at Hanoi on 25 October 2025.<sup>29</sup> In September 2024, however, the same Attorney General announced not repeal but revision: the Act was being amended to address the use of social media to attack private citizens, with penalties that "must be condign", and the Law Reform Commission had been asked to review the procedural provisions on jurisdiction and the service of documents on persons overseas.<sup>30</sup> The Vice-President said in the same week that the amendments were "not aimed at targeting social media commentators or ordinary citizens".<sup>31</sup> No amending Act had been located at the date of writing [VERIFY: whether any Cybercrime (Amendment) Bill was tabled or passed after September 2024; check parliament.gov.gy and the Official Gazette before print]. The statute examined below is therefore the statute of 2018.

### III. The offence architecture

#### A. Two architectures

Part II of the Act creates its offences in sections 3 to 24. Read in sequence they fall into two groups that were drafted on different principles, and a third group of general provisions.

The first group, sections 3 to 13, protects computer systems and electronic data as such. Its definitions are taken from the Convention on Cybercrime. The Convention defines a computer system as "any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data"; the Act's definition is "a device

<sup>26</sup> Hansard (20 July 2018) 100–103.

<sup>27</sup> Hansard (20 July 2018) 94–95. See also Department of Public Information (Guyana), 'Cyber Crime Bill will offer shield of protection for nation's youths – AG Williams' (Georgetown, 21 July 2018); 'Cybercrime Bill passed' *Guyana Chronicle* (Georgetown, 21 July 2018).

<sup>28</sup> 'Cybercrime Act to be repealed – AG' *Stabroek News* (Georgetown, 19 December 2022).

<sup>29</sup> United Nations Office on Drugs and Crime, 'UN Convention against Cybercrime' (status page), unodc.org (read 4 September 2026): adopted by consensus by General Assembly resolution 79/243 of 24 December 2024; opened for signature at Hanoi on 25 October 2025; open at United Nations Headquarters until 31 December 2026. See United Nations Convention against Cybercrime, art 64(1) (hereafter "UN Convention against Cybercrime").

<sup>30</sup> Ministry of Legal Affairs (Guyana), 'Nandlall announces revision of cybercrime law' (Georgetown, 25 September 2024).

<sup>31</sup> 'Amendments to Cybercrime Act will not target social media commentators – Jagdeo' *Kaieteur News* (Georgetown, 7 September 2024).

or group of interconnected or related devices, which follows a computer programme or external instruction to perform automatic processing of electronic data", followed by an inclusive list that runs from desktop computers to smart phones, smart televisions and video cameras, and the definitions of "service provider" and "traffic data" are near-verbatim.<sup>32</sup> The offences follow the Convention's first two titles in order: illegal access (section 3, article 2), illegal interception (section 4, article 3), data interference (section 5, article 4), system interference (section 7, article 5), misuse of devices (section 8, article 6), computer-related forgery (section 10, article 7) and computer-related fraud (section 11, article 8); the Convention's requirement that the conduct be "without right" is rendered throughout as "without lawful excuse or justification", and its requirement of intention as "intentionally".<sup>33</sup> Guyana added four offences of its own: illegal acquisition of data (section 6), unauthorised granting of access to or giving of data (section 9), an aggravated offence where the target is critical infrastructure (section 12), and identity-related offences (section 13).

The second group, sections 14 to 19, is drafted around harm to persons and to the polity rather than around systems. Section 14 (child pornography) is the one offence in this group with a treaty model, and it follows article 9 of the Convention closely, adding a duty on any person or service provider with knowledge of the offence to report it to the police.<sup>34</sup> Section 15 (child luring), section 16 (publication or transmission of an image of a person's private area), section 17 (multiple electronic mail messages and fraudulent websites), section 18 (offences against the State) and section 19 (using a computer system to coerce, harass, intimidate or humiliate) have no counterpart in the Convention at all. They are not offences against the integrity of systems; they are offences committed by means of a system, and the system does no more work in them than the postal service did in the older offences of sending threatening letters. That is not a criticism. It is a description of a different design, and the different design calls for a different constitutional analysis, because the conduct these sections reach is, in most cases, communication.

The third group is general. Section 20 makes it an offence to use a computer system to infringe copyright, patent, design or trade mark rights; section 21 provides for corporate liability and for the liability of officers who consented, connived or "failed to exercise due diligence"; section 22 treats attempt, incitement, conspiracy and facilitation as the principal offence; section 24 penalises disclosures and destruction of evidence that prejudice an investigation.<sup>35</sup> Section 23 deserves separate notice. It provides that where an offence under any other law is capable of being committed through the use of a computer system, that law "shall be deemed to provide that the offence may be committed" in that way, and the offender "shall be liable to a fine of four times the monetary penalty provided by that law and to the same custodial sentence".<sup>36</sup> A single sentence thereby amends every penal statute in the Laws of Guyana, quadrupling the fine for any offence committed by computer. The provision has attracted no public attention, and none of the

<sup>32</sup> Convention on Cybercrime, art 1(a), (c), (d); Cybercrime Act 2018, s 2 ("computer system", "service provider", "traffic data"). The Act's "electronic data" corresponds to the Convention's "computer data" (art 1(b)).

<sup>33</sup> Cybercrime Act 2018, ss 3, 4, 5, 7, 8, 10, 11; Convention on Cybercrime, arts 2–8. The formula "intentionally and without lawful excuse or justification" appears in ss 4(1), 5(1), 6, 7(1) and 8(1); s 3(1) uses "intentionally, without authorisation or in excess of authorisation, or by infringing any security measure".

<sup>34</sup> Cybercrime Act 2018, s 14(1)–(3); Convention on Cybercrime, art 9(1).

<sup>35</sup> Cybercrime Act 2018, ss 20, 21(2), 22, 24.

<sup>36</sup> Cybercrime Act 2018, s 23.

reported prosecutions appears to have relied on it, but it is the broadest sentence in the Act. I am not sure anyone in the House noticed it.

Table 1 sets out the architecture of Part II with the treaty parallels and the penalties.

| Section | Offence                                                  | Convention on Cybercrime parallel | Summary conviction                           | Conviction on indictment                     |
|---------|----------------------------------------------------------|-----------------------------------|----------------------------------------------|----------------------------------------------|
| 3       | Illegal access to a computer system                      | art 2                             | G\$3m and 3 years                            | G\$5m and 5 years                            |
| 4       | Illegal interception                                     | art 3                             | G\$5m and 3 years                            | G\$8m and 5 years                            |
| 5       | Illegal data interference                                | art 4                             | G\$3m and 3 years                            | G\$8m and 5 years                            |
| 6       | Illegal acquisition of data                              | none                              | G\$3m and 3 years                            | G\$8m and 5 years                            |
| 7       | Illegal system interference                              | art 5                             | G\$3m and 3 years                            | G\$8m and 5 years                            |
| 8       | Illegal devices                                          | art 6                             | G\$3m and 3 years                            | G\$8m and 5 years                            |
| 9       | Unauthorised granting of access to or giving of data     | none                              | G\$3m and 3 years                            | G\$8m and 5 years                            |
| 10      | Computer-related forgery                                 | art 7                             | G\$3m and 3 years                            | G\$5m and 5 years                            |
| 11      | Computer-related fraud                                   | art 8                             | G\$5m and 5 years                            | G\$10m and 10 years                          |
| 12      | Offences affecting critical infrastructure               | none                              | not triable summarily                        | G\$20m and 10 years                          |
| 13      | Identity-related offences                                | none                              | G\$5m and 3 years                            | G\$8m and 5 years                            |
| 14      | Child pornography                                        | art 9                             | G\$10m and 5 years                           | G\$15m and 10 years                          |
| 15      | Child luring                                             | none                              | G\$3m and 5 years                            | G\$8m and 5 years                            |
| 16      | Image of the private area of a person                    | none                              | G\$3m and 3 years                            | G\$8m and 5 years                            |
| 17      | Multiple electronic mail messages; fraudulent website    | none                              | G\$3m and 3 years                            | G\$5m and 5 years                            |
| 18      | Offences against the State                               | none                              | not triable summarily                        | 5 years; life where death results            |
| 19      | Coercion, harassment, intimidation, humiliation          | none                              | G\$5m and 3 years                            | G\$10m and 5 years                           |
| 20      | Infringement of copyright, patents, designs, trade marks | art 10                            | G\$3m and 3 years                            | not provided                                 |
| 23      | Offence under any other law committed by computer        | none                              | four times the fine; the same custodial term | four times the fine; the same custodial term |

| Section | Offence                            | Convention on Cybercrime parallel | Summary conviction | Conviction on indictment |
|---------|------------------------------------|-----------------------------------|--------------------|--------------------------|
| 24      | Offences prejudicing investigation | none                              | G\$5m and 3 years  | G\$8m and 5 years        |

Source: Cybercrime Act 2018, sections 3 to 24.<sup>37</sup>

### ***B. The soundness of the core***

The integrity offences are competently drafted. They carry the two elements the Convention insists on, intention and the absence of right, and they are graded: the offence that requires a further intent (fraud, section 11) and the offence that touches critical infrastructure (section 12) carry heavier penalties, and section 12 is indictable only. Section 4 contains a carefully worked list of exceptions for interception that is public, consensual, performed by a service provider in the course of service, or authorised under the Interception of Communications Act, and section 8 confines the devices offence to devices and passwords held "for the purpose of committing an offence under this Act or any other law".<sup>38</sup> Section 28 permits a search to be extended to another system from which the data sought is lawfully accessible, which is article 19(2) of the Convention in domestic dress.<sup>39</sup>

Two of the Guyanese additions are less carefully bounded. Section 6 makes it an offence, without more, intentionally and without lawful excuse or justification to acquire "electronic data of another person"; there is no requirement of dishonesty, of damage or of a security measure defeated, and the phrase "of another person" is not defined by reference to ownership, possession or confidentiality.<sup>40</sup> Section 9, the clause that Reporters Without Borders objected to, was narrowed in the Committee of the whole House so that it now reaches a person who obtains data that is commercially sensitive, relates to national security, or is protected against unauthorised access, and who then "grants access to or gives" it to another "whether or not he knows that the other person is authorised to receive or have access to the electronic data".<sup>41</sup> The amendment removed the receiving limb that had alarmed the press. It left a provision under which a journalist who obtains a leaked document relating to national security and passes it to an editor has, on the words, committed an offence; the phrase "whether or not he knows" does not protect the person who reasonably believes the recipient is authorised, but removes the recipient's authorisation from the elements altogether. I read that as a drafting slip, curable by a public-interest defence, and not as a reason to doubt the core.

Two points about the penalties before leaving the core. The fines and terms are expressed as fixed sums and fixed periods, joined by "and": a person convicted summarily under section 16 "is liable

<sup>37</sup> Cybercrime Act 2018, ss 3–24. Sections 21 and 22 are omitted from the table: s 21(3) provides for officers of a body corporate (G\$5m and three years summarily; G\$8m and five years on indictment) and s 22 punishes inchoate participation "as if he had committed the offence as a principal offender".

<sup>38</sup> Cybercrime Act 2018, s 4(2)(a)–(f), s 8(1). The Interception of Communications Act is Cap 47:03 according to the marginal reference to s 4.

<sup>39</sup> Cybercrime Act 2018, s 28(2); Convention on Cybercrime, art 19(2).

<sup>40</sup> Cybercrime Act 2018, s 6.

<sup>41</sup> Cybercrime Act 2018, s 9(1); Hansard (20 July 2018) 100–101 (substitution of clause 9 in the Committee of the whole House).

... to a fine of three million dollars and to imprisonment for three years".<sup>42</sup> Whether those words create maxima or mandatory penalties is a question of the general law of sentencing on which the Act is silent; if the latter reading were adopted, the objection the Caribbean Court of Justice upheld in *Nervais* to sentences that deprive a court of the function of fitting the punishment to the crime would arise.<sup>43</sup> The other point is section 19, which carries a single penalty for four offences of very different gravity, from extortion by threat of exposure to the publication of a single "vulgar" message with intent to embarrass. Section V returns to that.

## IV. The intimate-image offence: section 16

### A. Text and elements

Section 16 reads in full:

16. (1) A person commits an offence if the person intentionally captures, stores in, publishes or transmits through a computer system, the image of the private area of another person without that other person's consent. (2) A person who commits an offence under subsection (1), is liable – (a) on summary conviction to a fine of three million dollars and to imprisonment for three years; and (b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years. (3) For the purposes of this section, "private area" means naked genitals, buttocks or female breasts.<sup>44</sup>

The section has four elements. The conduct is any one of four acts, capture, storage, publication or transmission, done "through a computer system", which by section 2 includes "a smart phone" and "a video camera".<sup>45</sup> The object is "the image of the private area of another person", with "private area" exhaustively defined as naked genitals, buttocks or female breasts. The mental element is intention as to the act. The circumstance that makes the act criminal is the absence of the depicted person's consent. There is no requirement that the image be sexual, that the accused have acted for sexual gratification or with intent to cause distress, that the image have been private when taken, or that the person depicted have had a reasonable expectation of privacy. There is no defence.

### B. The gap it fills

Before 2018 Guyanese law reached this conduct only at its edges. The Sexual Offences Act 2010 created the offence of voyeurism, committed by a person who "for the purpose of obtaining sexual gratification" observes another doing a private act without consent, who installs equipment or adapts a structure to enable such observation, or who "records another person ... doing a private act with the intention that the accused or a third person will, for the purpose of obtaining sexual gratification, look at an image of the complainant doing the act".<sup>46</sup> A private act is one done in a place which "would reasonably be expected to provide privacy" while the person's

<sup>42</sup> Cybercrime Act 2018, s 16(2)(a). Sections 3 to 15 join the alternatives with "or"; ss 16, 17, 19, 21 and 24 with "and".

<sup>43</sup> *Nervais v The Queen* [2018] CCJ 19 (A.J) [45], as described in *McEwan* (n 7) [121] (Rajnauth-Lee JCCJ): the mandatory death penalty "deprived a court of the opportunity to exercise the quintessential judicial function of tailoring the punishment to fit the crime".

<sup>44</sup> Cybercrime Act 2018, s 16.

<sup>45</sup> Cybercrime Act 2018, s 2 ("computer system", para (b)).

<sup>46</sup> Sexual Offences Act, Cap 8:03 (Guyana) (Act No 7 of 2010), s 29(1)(a), (b), (d).

"genitals, buttocks or breasts are exposed or covered only with underwear", while using a lavatory, or during "a sexual act that is not of a kind ordinarily done in public"; the offence of exposure of the genitals in section 28 is committed by the person exposed, not by the person who photographs.<sup>47</sup> Voyeurism therefore catches the covert recording, but only where the recording is for sexual gratification and only where the subject was in a private place. It does not catch the former partner who publishes an image that was made with consent, nor the stranger who circulates an image he did not make, nor the person who acts from spite rather than desire. The ordinary criminal law had nothing to say about distribution. That is the gap, and it is the gap that has been filled, in the last decade, by the statutes conventionally described as "revenge porn" laws and, in the better literature, as laws against image-based sexual abuse.<sup>48</sup>

The scale of the conduct in Guyana was made visible in January 2023, when the police confirmed an investigation into a Telegram group described as "Guyanese ONLY", with 466 members and 414 photographs and 115 videos shared, in which, the reporting outlet was told, images were being circulated without the knowledge or consent of the persons depicted, some by former partners.<sup>49</sup> Charges in this class of case are reported with regularity: a caterer charged in August 2023 with using a computer system to publish personal information of a woman to cause her public ridicule and emotional distress; an information technology technician charged in July 2024 with acquiring images and videos from a former partner's messages and publishing them.<sup>50</sup> In neither report was the charge framed under section 16. Both were framed under sections 6 and 19, the acquisition offence and the harassment offence. That habit, reaching for section 19 in a case section 16 was written for, says something about how section 19 works in practice. I come back to it in section V.

### C. Comparators

Three comparators, each read from its own text, mark the range of legislative choice.

The first is England and Wales. Section 33 of the Criminal Justice and Courts Act 2015 made it an offence to disclose "a private sexual photograph or film" without the consent of the individual depicted and "with the intention of causing that individual distress"; it supplied defences for the prevention of crime, for journalistic publication reasonably believed to be in the public interest, and for a reasonable belief that the image had previously been disclosed for reward; it defined "private" as showing "something that is not of a kind ordinarily seen in public" and "sexual" by reference to exposed genitals or pubic area or what a reasonable person would consider sexual; and it provided that a defendant "is not to be taken to have disclosed a photograph or film with the intention of causing distress merely because that was a natural and probable consequence of the disclosure".<sup>51</sup> The maximum was two years. That model was repealed with effect from 31

<sup>47</sup> *ibid* ss 30(1), 28(1).

<sup>48</sup> Clare McGlynn and Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37 OJLS 534, 534 (defining the concept as "the non-consensual creation and/or distribution of private sexual images").

<sup>49</sup> 'Cops probing "Guyanese ONLY" Telegram group being used to share nudes' *News Room* (Georgetown, 6 January 2023).

<sup>50</sup> 'Caterer charged with uploading woman's nude images' *Stabroek News* (Georgetown, 31 August 2023) (charge framed as using a computer system "to publish electronic data containing personal information of a woman, to cause her public ridicule and emotional distress"); 'Man on \$150k bail for publishing nude pictures of ex-girlfriend' *Kaieteur News* (Georgetown, 23 July 2024) (charges of "illegal acquisition of data" and "using a computer system to intimidate a person"). Press reports do not always state the section charged; the descriptions are those of the reports.

<sup>51</sup> Criminal Justice and Courts Act 2015 (UK), s 33(1), (3)–(5), (8), (9) and s 35(2)–(3), as enacted.

January 2024 and replaced by sections 66B to 66D of the Sexual Offences Act 2003, inserted by section 188 of the Online Safety Act 2023.<sup>52</sup> The new base offence is committed by a person who intentionally shares a photograph or film which "shows, or appears to show" another person in an intimate state, where that person does not consent and the sharer "does not reasonably believe" that she consents; the motive requirement has been moved out of the base offence into aggravated forms (an intention to cause alarm, distress or humiliation; sexual gratification), and a separate offence of threatening to share has been added.<sup>53</sup> Consent is defined to include "general consent covering the particular act of sharing as well as specific consent to the particular act of sharing", and a set of exemptions covers images taken in a place to which the public had access where there was no reasonable expectation of privacy, images previously shared with consent, and medical and family contexts.<sup>54</sup>

The second is Jamaica. The Cybercrimes Act 2015 has no dedicated intimate-image offence. Section 9 makes it an offence to use a computer to send to another person data "that is obscene, constitutes a threat or is menacing in nature" with "the intention to harass any person or cause harm, or the apprehension of harm, to any person or property".<sup>55</sup> The Director of Public Prosecutions' guidelines on that section, issued in May 2017, describe its three ingredients, require proof of "the highest level of subjective mens rea", and warn that a communication "has to be more than simply offensive to be contrary to the criminal law".<sup>56</sup> Non-consensual distribution of an intimate image is prosecutable in Jamaica only if the image is obscene in the common-law sense and the sender intended to harass. That is a narrower net than Guyana's, and it leaves the consensually made image circulated without malice, or with a motive other than harassment, outside the criminal law.

The third is the United Nations Convention against Cybercrime, the instrument the Attorney General nominated in 2022 as the model for a replacement Act. Article 16 requires each State Party to criminalise, "when committed intentionally and without right, the selling, distributing, transmitting, publishing or otherwise making available of an intimate image of a person by means of an information and communications technology system, without the consent of the person depicted in the image"; an intimate image is a visual recording of a person over eighteen "that is sexual in nature, in which the person's sexual parts are exposed or the person is engaged in sexual activity, which was private at the time of the recording, and in respect of which the person or persons depicted maintained a reasonable expectation of privacy at the time of the offence"; and a State Party "may require the intent to cause harm before criminal liability attaches".<sup>57</sup>

Set against these, section 16 of the Guyanese Act is closer to the consent-based model of the 2023 United Kingdom reform and of article 16 of the United Nations Convention than to the motive-based model of 2015. In 2018 that was an unusual choice. The scholarly case for it had been made. McGlynn and Rackley's account of image-based sexual abuse argued that the

<sup>52</sup> Online Safety Act 2023 (UK), ss 188, 190; commencement on 31 January 2024 by the Online Safety Act 2023 (Commencement No 3) Regulations 2024, SI 2024/31, reg 2, as recorded on [legislation.gov.uk](https://legislation.gov.uk).

<sup>53</sup> Sexual Offences Act 2003 (UK), s 66B(1)–(4), as inserted.

<sup>54</sup> *ibid* s 66B(6)(a); s 66C(1), (3)–(5).

<sup>55</sup> Cybercrimes Act 2015 (Jamaica), Act 31 of 2015, s 9(1).

<sup>56</sup> Office of the Director of Public Prosecutions (Jamaica), *Guidelines for Prosecuting Cases Involving Malicious Communications: Section 9 of the Cybercrimes Act of Jamaica, 2015* (15 May 2017) 3, 6–7.

<sup>57</sup> UN Convention against Cybercrime, art 16(1), (2), (5).

language of "revenge" and "pornography" had skewed legislative debate towards motive and sexual content, when the wrong lay in the non-consensual creation or distribution of a private sexual image and the harm lay in physical and mental illness "together with the loss of dignity, privacy and sexual autonomy";<sup>58</sup> Citron and Franks had made the case in the United States for the direct criminalisation of non-consensual pornography, on the ground that the civil remedies, copyright included, were "an ineffective deterrent".<sup>59</sup> Guyana's drafter, whether or not with this literature in view, put consent at the centre and left motive out. The better view is that this was right.

#### **D. The constitutional test**

Publication is expression, and section 16 restricts it. The restriction must therefore be one "reasonably required" under article 146(2), and the natural ground is paragraph (b): provision "reasonably required for the purpose of protecting the reputations, rights, and freedoms of other persons"; article 40(2) makes explicit that the limitations in Title 1 exist "to ensure that the enjoyment of the said rights and freedoms by any individual does not prejudice the rights and freedoms of others or the public interest".<sup>60</sup> The content of "reasonably required" has been settled in this region since *de Freitas*, where Lord Clyde asked "whether (i) the legislative objective is sufficiently important to justify limiting a fundamental right; (ii) the measures designed to meet the legislative objective are rationally connected to it; and (iii) the means used to impair the right or freedom are no more than is necessary to accomplish the objective".<sup>61</sup> The Board has since accepted that the test "has been somewhat refined" and now conforms to the four-stage structure that adds a final question whether "a fair balance has been struck between the rights of the individual and the interests of the community",<sup>62</sup> and the Caribbean Court of Justice applied the same structure to Guyana's Constitution in *McEwan*, requiring that the infringing law "pursue some pressing objective and be rationally connected to that objective", that it "impair only such of the right as is necessary to be impaired", and that there be "proportionality of effects between the deleterious and salutary effects of the infringing law".<sup>63</sup>

Section 16 passes the first two limbs without difficulty. The objective, the protection of the privacy, dignity and sexual autonomy of persons whose bodies are exposed to strangers without their consent, is of the first importance, and a prohibition on the non-consensual capture and distribution of such images is rationally connected to it. The third and fourth limbs are where the drafting must answer, and it answers well on the essentials. The offence is confined to a narrowly defined class of images. It requires intention. It turns on consent, which is the element that distinguishes the wrong from the harmless. It does not reach the discussion of ideas at all. And the penalty, three years summarily and five years on indictment, sits within the range of the comparators.

<sup>58</sup> McGlynn and Rackley (n 48) 534–535.

<sup>59</sup> Danielle Keats Citron and Mary Anne Franks, 'Criminalizing Revenge Porn' (2014) 49 Wake Forest L Rev 345.

<sup>60</sup> Constitution of the Co-operative Republic of Guyana, Cap 1:01, arts 146(2)(b), 40(2).

<sup>61</sup> *de Freitas* (n 6) 80 (Lord Clyde), as quoted in *Rambally & Sons Ltd v Attorney General of Saint Lucia* (High Court of Justice, Saint Lucia, Civil Suit No 355 of 1999, 19 September 2000) [25] (Hariprashad-Charles J); reported also at (1998) 53 WIR 131, the citation used by the Caribbean Court of Justice in *McEwan* (n 7) [62].

<sup>62</sup> *Suraj v Attorney General of Trinidad and Tobago* [2022] UKPC 26 [51], citing Tracy Robinson, Arif Bulkan and Adrian Saunders, *Fundamentals of Caribbean Constitutional Law* (2nd edn, Sweet & Maxwell 2021) 473–475.

<sup>63</sup> *McEwan* (n 7) [62].

Four features nonetheless impair the right more than is necessary, and each is curable by amendment. The first is the absence of any privacy qualification. The draft published in December 2015 had, as reported, confined the offence to cases where the person depicted had a reasonable expectation of privacy; the Act as passed does not.<sup>64</sup> On the words, a press photograph of a naked protester, a documentary image of a traditional ceremony, a medical photograph stored on a hospital system without a signed consent, and the image of an intoxicated stranger on a public beach are all within section 16. The United Kingdom's 2023 exemptions and article 16 of the United Nations Convention both use a reasonable-expectation-of-privacy limb to exclude such cases, and its restoration would cost the offence nothing that matters.<sup>65</sup> Then there is the absence of any defence: no journalism or public-interest defence, no defence for the prevention or investigation of crime, no defence of prior consensual publication. The 2015 English model carried all three; the 2023 model carries the last and a reasonable-excuse defence for the base offence.<sup>66</sup> Consent is the third. The section does not say consent to what. A person who consents to being photographed has not consented to the photograph's publication, and a person who sent an image to a partner has not consented to its retention after the relationship ends; the English provision meets the first point by distinguishing general consent from consent to "the particular act of sharing". The fourth is the definition of the object: "the image of the private area of another person" does not on its face include an image that "appears to show" that person, which is the formula the United Kingdom adopted to reach altered and synthetic images, nor an image of sexual activity in which the private area is not exposed.<sup>67</sup>

None of these is a reason to hold section 16 unconstitutional. Each is a reason to read it so that it does not reach the cases that would make it so. The argument advanced here is that the courts should read the phrase "without that other person's consent" as directed to the specific act charged, so that consent to capture is not consent to publish; that "intentionally" should be read as requiring knowledge of, or at least recklessness as to, the absence of consent, since an offence of this seriousness ought not to be one of strict liability as to its defining circumstance; and that the principle of legality, which the Caribbean Court of Justice restated in *McEwan* as the rule that an intention to interfere with fundamental rights must be expressed "by clear and unambiguous language", should lead a court to decline to apply the section to images taken in public of persons who had no reasonable expectation of privacy, because nothing in the Act expresses an intention to criminalise the photography of public events.<sup>68</sup> So read, section 16 is a defensible restriction on expression. It is also, in comparative terms, an early and creditable choice of the consent model that the international instruments have since endorsed.

<sup>64</sup> 'Cybercrime bill targets child porn, hacking, identity theft' *Stabroek News* (Georgetown, 29 December 2015); 'Cyber Crime law to prohibit child porn, sharing of nude images' *Demerara Waves* (Georgetown, 28 December 2015). [VERIFY: compare clause 16 of Bill No 17 of 2016 as printed, and the Special Select Committee's report of 26 April 2018, to establish at which stage the reasonable-expectation limb was removed.]

<sup>65</sup> Sexual Offences Act 2003 (UK), s 66C(1); UN Convention against Cybercrime, art 16(2).

<sup>66</sup> Criminal Justice and Courts Act 2015 (UK), s 33(3)–(5), as enacted; Sexual Offences Act 2003 (UK), ss 66B(8), 66C(3).

<sup>67</sup> Sexual Offences Act 2003 (UK), s 66B(1)(a), (6)(a); Cybercrime Act 2018, s 16(1), (3).

<sup>68</sup> *McEwan* (n 7) [125] (Rajnauth-Lee JCCJ).

## V. Sections 18 and 19 and the constitutional test

### A. The text of section 18

Section 18 is what remained of the sedition clause. It provides:

18. (1) A person commits an offence if the person, whether in or out of Guyana, intentionally publishes, transmits or circulates by use of a computer system, a statement or words, either spoken or written, a text, video, image, sign, visible representation, or other thing, that – (a) advocates the use, without authority of law, of force as a means of accomplishing a governmental change within Guyana; (b) incites, counsels, urges, induces, aids or abets any person to commit, participate in the commission of, or to conspire with another person to commit treason under section 314 or 317 of the Criminal Law (Offences) Act; (c) encourages, incites, induces, aids, abets, counsels any person to commit or to conspire with another person to commit any criminal offence against the President or any member of the Government; (d) (i) encourages, entices, induces or motivates any person in or out of Guyana to join a terrorist group or to commit or participate in the commission of an offence of or in relation to terrorist financing under Part V of the Anti-Money Laundering and Countering the Financing of Terrorism Act; or (ii) incites, urges, teaches or trains any person in or out of Guyana to commit or participate in the commission of a terrorist act or an offence under the Anti-terrorism and Terrorist Related Activities Act; or (e) excites or attempts to excite ethnic divisions among the people of Guyana or hostility or ill-will against any person or class of persons on the ground of race.<sup>69</sup>

The offence is indictable only and carries five years; where the death of the President, a member of the Government "or any other person" results, life. Subsection (4) then provides that a statement does not constitute an offence if it "expresses disapprobation of the measures of the Government with a view to obtain their alteration by lawful means", expresses disapprobation of the administrative or other action of the Government, expresses that the President or the Government "has been misled or mistaken in their measures", "points out errors or defects of the Government, Constitution or Parliament", or "procures, by lawful means, the alteration of any matter of government".<sup>70</sup>

Three of the five limbs are unobjectionable in principle. Paragraph (a), advocacy of unlawful force to change the government, is the core of what a democratic state may legitimately forbid, and it is expressly directed at force. Paragraphs (b) and (d) are incitement provisions parasitic on the offences of treason and terrorism; they add little to section 22 and to the general law of incitement, but they add nothing dangerous. The difficulties lie in paragraphs (c) and (e), and in the relationship between the whole section and the words "intentionally" and "that".

Paragraph (c) creates a special protection for the President and members of the Government against incitement to "any criminal offence" against them. The words are not confined to violence. A statement that encourages a crowd to obstruct a Minister's motorcade, to trespass on a Minister's lawn or to shout down a Minister at a public meeting, each of which may be a summary offence, is, on the words, a statement that encourages the commission of a criminal

<sup>69</sup> Cybercrime Act 2018, s 18(1). The marginal references identify the Criminal Law (Offences) Act as Cap 8:01, the Anti-Money Laundering and Countering the Financing of Terrorism Act as Cap 10:11 (Act No 13 of 2009) and the Anti-Terrorism and Terrorist Related Activities Act as Act No 15 of 2015.

<sup>70</sup> Cybercrime Act 2018, s 18(2)–(4).

offence against a member of the Government, and the speaker is exposed to five years' imprisonment on indictment. No other class of person in Guyana enjoys that protection. This is the inversion that Lord Bridge described in *Hector*: "In a free democratic society it is almost too obvious to need stating that those who hold office in government and who are responsible for public administration must always be open to criticism. Any attempt to stifle or fetter such criticism amounts to political censorship of the most insidious and objectionable kind."<sup>71</sup> Paragraph (c) does not stifle criticism in terms; it fetters it in effect, by attaching a five-year indictable offence to speech about Ministers that would, if it concerned anyone else, be at most an incitement to a summary offence.

Paragraph (e) has a constitutional anchor that paragraph (c) lacks. Article 146(3) provides that freedom of expression "does not relate to hate speeches or other expressions, in whatever form, capable of exciting hostility or ill-will against any person or class of persons", and article 146(2)(d) saves laws that restrain any person or party "from taking any action or advancing, disseminating or supporting any idea, which may result in racial or ethnic divisions among the people of Guyana".<sup>72</sup> The second half of paragraph (e), hostility or ill-will "on the ground of race", tracks the constitutional language and is defensible. The first half, "excites or attempts to excite ethnic divisions among the people of Guyana", is not language the Constitution uses to define an offence, and it has no settled legal content. A political scientist who publishes an analysis of ethnic voting patterns, a columnist who argues that a policy benefits one community over another, and a candidate who appeals to a constituency defined by ethnicity all publish material that may, in the ordinary sense, excite ethnic division. The Opposition itself, in the debate, described the paragraph as "equally dangerous as worded".<sup>73</sup>

The words "intentionally" and "that" then decide how much of this matters. Section 18(1) punishes a person who "intentionally publishes ... a statement ... that advocates", "that ... incites", "that ... excites or attempts to excite". On the ordinary reading the adverb governs the publication and the relative clause describes the statement's tendency. Intention to incite is not, on that reading, an element. A statement is criminal if it has the described character, and the accused need intend only to publish it. That is the structure of the old law of sedition, in which the seditious tendency of the words was enough; and it is the structure that the excision of paragraph (1)(a) was supposed to have removed from the Act. Subsection (4) confirms the ancestry. Its five savings are the savings of the excised sedition clause, reported in April 2018 as the qualifications on the offence of exciting disaffection;<sup>74</sup> they were carried into the substituted clause even though the offence they qualified had gone, so that the Act now solemnly provides that a statement pointing out "errors or defects of the Government" does not constitute the offence of inciting treason or terrorism, which nobody had supposed it could. I doubt that was intended. It reads like a proviso that nobody remembered to delete. The shadow of the excised clause lies across the section, and it is the shadow, not the text, that a court should read out.

<sup>71</sup> *Hector* (n 8) 318 (Lord Bridge of Harwich), as quoted by the Board in *Ramadhar v Ramadhar* [2020] UKPC 7 [24], through Lord Keith of Kinkel's citation of the passage in *Derbyshire County Council v Times Newspapers Ltd* [1993] AC 534 (HL) 548.

<sup>72</sup> Constitution of Guyana, art 146(3), (2)(d).

<sup>73</sup> Hansard (20 July 2018) 27. The member referred to the paragraph as "clause 18 (1) (f)", its lettering in the text then before the House; it is paragraph (e) of s 18(1) as enacted.

<sup>74</sup> 'Sedition and cybercrime' (editorial) *Stabroek News* (Georgetown, 30 April 2018).

## **B. The text of section 19**

Section 19 creates four offences. Subsection (1) is an offence of coercion: using a computer system, "with intent to compel another person to do any act which the other person is not legally bound to do or to abstain from doing any act which the other person has a legal right to do", to publish or transmit data that "intimidates the other person" or threatens violence to him or his family or injury to their property, "intimidate" being defined to include causing "a person substantial emotional distress".<sup>75</sup> Subsection (4) is an offence of extortion: using a computer system "with the intent to extort a benefit from another person by threatening to publish electronic data containing personal or private information which can cause the other person public ridicule, contempt, hatred or embarrassment".<sup>76</sup> Both have a specific intent, both are directed at conduct the criminal law has always reached by other names, and neither is in difficulty under article 146. The difficulties lie in subsections (2) and (3):

(2) A person commits an offence if he uses a computer system – (a) to publish or transmit electronic data that is obscene, vulgar, profane, lewd, lascivious or indecent with intent to humiliate, harass or cause substantial emotional distress to another person; or (b) to repeatedly send to another person electronic data that is obscene, vulgar, profane, lewd, lascivious or indecent with intent to humiliate or harass the other person to the detriment of that person's health, emotional well-being, self-esteem or reputation. (3) A person commits an offence if the person uses a computer system to disseminate any information, statement or image, knowing the same to be false, that – (a) causes damage to the reputation of another person; or (b) subjects another person to public ridicule, contempt, hatred or embarrassment.<sup>77</sup>

All four offences carry the same penalty: five million dollars and three years on summary conviction, ten million dollars and five years on indictment.<sup>78</sup>

Subsection (2)(a) has two elements, a content element and a purpose element, and each is troubling. The content element is satisfied by data that is "obscene, vulgar, profane, lewd, lascivious or indecent". "Obscene" and "indecent" have a settled meaning in the criminal law, and a demanding one: the Jamaican Director of Public Prosecutions' guidelines, applying the same word in section 9 of the Jamaican Act, adopt the test in *R v Hicklin* of a tendency "to deprave and corrupt", and place "indecent" at the lower and "obscene" at the upper end of a single scale.<sup>79</sup> "Vulgar" and "profane" have no criminal-law meaning at all. They are words of taste. A great deal of political speech in Guyana, as anywhere, is vulgar; a great deal of religious criticism is, by definition, profane. To make either a component of a criminal offence is to do precisely what the Caribbean Court of Justice said in *McEwan* a penal statute must not do: to state the offence "in ways that allow law enforcement officials to use subjective moral or value judgments as the basis for its enforcement".<sup>80</sup> The purpose element does not cure the content element. An intent "to humiliate" accompanies most sharp criticism of public conduct, and "substantial emotional distress" is a state that a truthful and public-spirited exposure of wrongdoing is likely, and may

<sup>75</sup> Cybercrime Act 2018, s 19(1), (6).

<sup>76</sup> Cybercrime Act 2018, s 19(4).

<sup>77</sup> Cybercrime Act 2018, s 19(2)–(3).

<sup>78</sup> Cybercrime Act 2018, s 19(5).

<sup>79</sup> Office of the Director of Public Prosecutions (Jamaica), *Guidelines* (n 56) 4, adopting the test of Cockburn CJ in *R v Hicklin* (1868) LR 3 QB 360.

<sup>80</sup> *McEwan* (n 7) [80].

be intended, to produce in the wrongdoer.

Subsection (3) is criminal defamation by another name, with one element added and several removed. The element added is knowledge of falsity, which narrows the offence to the deliberate lie; that is a real limitation, and it is the reason the subsection is not simply void. The elements removed are any requirement of intent to harm, any defence of public interest, and any threshold of seriousness: the dissemination of any false statement that "subjects another person to public ridicule ... or embarrassment" is sufficient. The Guyana Press Association's objection in 2018 was directed at the sedition clause, but the phrase it used, the "institutionalisation of criminal defamation", describes subsection (3) exactly, and subsection (3) passed the House without a word.<sup>81</sup> One reported prosecution under it concerned an animated video about a reporter.<sup>82</sup>

The record of enforcement is consistent with the breadth of the words. The Attorney General who promised repeal in 2022 was reported as acknowledging the argument of free speech advocates "that the state and private individuals are using the provisions of the act to target political and other figures", and the same report recorded that the charges brought had included one "over a statement that a Hindu pandit had consumed fish at a religious ceremony" and charges against a mayor and a member of the National Assembly "over utterances they had made".<sup>83</sup> A charge under section 19(2)(a) against a man who had posted a WhatsApp status about a Permanent Secretary was dismissed in July 2023; someone had taken a screenshot of the status and sent it to the Permanent Secretary, who complained to the police.<sup>84</sup> A charge arising from a video in which a visiting businessman complained on social media about the length of the firearm-licence process was dismissed in February 2026 on the advice of the Director of Public Prosecutions that "no cybercrime elements were present in the video", after the accused had spent almost two months in the country on bail with his passport lodged.<sup>85</sup> In December 2025 a magistrate at Diamond halted a prosecution for using a computer system to publish data with intent to humiliate in order to receive written submissions that the charge was "defective, vague, and insufficiently particularized" and that the pleading of jurisdiction in speech-based offences must meet a strict standard; the prosecution sought and obtained an adjournment to respond.<sup>86</sup> Nothing is said here about the merits of that application, which is for the court. What the record shows is a section used against speech about public officials and public administration, and charges dismissed once they reach a hearing. The process is the punishment.

<sup>81</sup> 'GPA says sections in Cybercrime Bill "criminalizing freedom of expression" must go' *iNews Guyana* (Georgetown, 2 May 2018); Hansard (20 July 2018) 103 ("Clauses 19 to 43 agreed to and ordered to stand part of the Bill").

<sup>82</sup> 'One witness called in cybercrime trial of photographer' *Stabroek News* (Georgetown, 6 January 2023) (charge that the accused "used a computer system to disseminate information about [the complainant], knowing same to be false and which subjected [him] to public ridicule, contempt, hatred or embarrassment").

<sup>83</sup> 'Cybercrime Act to be repealed – AG' *Stabroek News* (Georgetown, 19 December 2022).

<sup>84</sup> 'Case dismissed against man over cyber "humiliation" of Home Affairs PS' *Stabroek News* (Georgetown, 27 July 2023) (charge under s 19(2)(a)).

<sup>85</sup> 'Court dismisses cybercrime charge against US businessman' *Stabroek News* (Georgetown, 28 February 2026).

<sup>86</sup> 'Court halts cybercrime prosecution to address novel challenges to speech-based offences in Guyana' *Demerara Waves* (Georgetown, 21 December 2025). The matter was adjourned to 6 January 2026; no ruling had been located at the date of writing.

### C. The constitutional framework

Guyana's guarantee of expression is broad in its statement and specific in its exceptions. Article 146(1) protects "freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to communicate ideas and information without interference and freedom from interference with his or her correspondence"; article 146(2) saves laws "reasonably required in the interests of defence, public safety, public order, public morality or public health" and laws reasonably required for the protection of "the reputations, rights, and freedoms of other persons".<sup>87</sup> Article 8 makes the Constitution supreme and any inconsistent law void "to the extent of the inconsistency", and article 153 gives the High Court original jurisdiction to grant redress.<sup>88</sup> The protection of the law in article 144, and the general guarantee of the fundamental rights in article 40, supply the second ground on which a penal statute may fail, which is vagueness.<sup>89</sup>

The vagueness ground was settled for Guyana in *McEwan*, and it is a decision of unusual authority for present purposes because it struck down a Guyanese penal provision, section 153(1)(xlvii) of the Summary Jurisdiction (Offences) Act, on the very grounds that sections 18 and 19 invite. The President of the Court, delivering the judgment of the majority, set the standard:

A penal statute must meet certain minimum objectives if it is to pass muster as a valid law. It must provide fair notice to citizens of the prohibited conduct. It must not be vaguely worded. It must define the criminal offence with sufficient clarity that ordinary people can understand what conduct is prohibited. It should not be stated in ways that allow law enforcement officials to use subjective moral or value judgments as the basis for its enforcement. A law should not encourage arbitrary and discriminatory enforcement.<sup>90</sup>

The Court rejected the Solicitor General's argument that vagueness could be cured by particulars given at the time of charge, because "individuals require advance notice of any proscribed conduct so as to regulate their behaviour"; it held that "the rule of law requires that legislation which is hopelessly vague must be struck down as unconstitutional"; and it declared the section void and struck it from the Act.<sup>91</sup> Anderson JCCJ added that a vague offence "confers unacceptably broad discretion on state officials to arrest and charge at will".<sup>92</sup> Rajnauth-Lee JCCJ located the doctrine in the right to the protection of the law under articles 40 and 144, drew on Fuller's account of the reciprocity between government and citizen that publicly announced rules create, adopted the "legal debate" test of *R v Nova Scotia Pharmaceutical Society* and the

<sup>87</sup> Constitution of Guyana, art 146(1), (2)(a)–(b).

<sup>88</sup> Constitution of Guyana, arts 8, 153(1)–(2).

<sup>89</sup> Constitution of Guyana, arts 40, 144; *McEwan* (n 7) [110], [116]–[117] (Rajnauth-Lee JCCJ).

<sup>90</sup> *McEwan* (n 7) [80] (Saunders PCCJ, for himself and Wit and Barrow JJCCJ).

<sup>91</sup> *ibid* [82], [85], [147](vi)–(vii).

<sup>92</sup> *ibid* [96] (Anderson JCCJ).

fair-notice and control-of-discretion analysis of *Papachristou v City of Jacksonville*, and concluded that "the requirements of certainty and fair notice in a criminal statute are a logical corollary to the protection of the law as it operates in modern democracies" and that "criminal statutes which are vaguely drawn are inconsistent with the right to protection of the law".<sup>93</sup> She also restated the principle of legality as a rule of construction: where Parliament intends to interfere with fundamental rights, "it must express that intention by clear and unambiguous language".<sup>94</sup>

Two things about the doctrine matter here. One is that the test is "hopelessly vague". Some vagueness is a property of every legal rule; Endicott's demonstration that vagueness is an ineliminable feature of law is now orthodox, and the principle of maximum certainty in the criminal law is, in Horder's restatement of Ashworth's principles, a principle to be pursued rather than a condition that any statute perfectly satisfies.<sup>95</sup> The constitutional question is not whether a word has a penumbra but whether the offence, taken as a whole, delegates its own definition to the enforcer. The other is that the doctrine sits beside, and not in place of, the proportionality analysis. A provision may be clear and still disproportionate, and a provision may be proportionate in its core and vague at its edges. Article 8 speaks of voidness "to the extent of the inconsistency", and the Court in *McEwan* struck a single sub-paragraph out of a long section.<sup>96</sup> The remedy can be as narrow as the defect.

#### **D. Applying the tests**

The better view, respectfully, is that neither section 18 nor section 19 is void in its entirety, and that both contain words that are.

Section 18(1)(a), (b) and (d) are clear enough and serve objectives, the prevention of violence, treason and terrorism, that fall squarely within "defence, public safety, public order". Section 18(1)(e), in its second half, tracks article 146(3) and is saved by it. Section 18(1)(c) fails the third limb of *de Freitas*: a provision that protected the persons of the President and Ministers against incitement to violence would be reasonably required for public order, but a provision that reaches incitement to "any criminal offence" against them impairs expression far more than that objective requires, and it does so for a class of persons whom the Constitution, on the authority of *Hector*, requires to be open to criticism. The words "ethnic divisions" in paragraph (e) fail the vagueness test on the *McEwan* standard: no one can say in advance what publication "excites ... ethnic divisions", the words invite enforcement by "subjective moral or value judgments", and the constitutional text supplies a clearer formula, "hostility or ill-will", which the paragraph already uses.

<sup>93</sup> *ibid* [116]–[131] (Rajnauth-Lee JCCJ), quoting Lon L Fuller, *The Morality of Law* (Yale University Press 1964) 39–40 at [122], *R v Nova Scotia Pharmaceutical Society* [1992] 2 SCR 606 at [123], *Papachristou v City of Jacksonville* 405 US 156 (1972) at [128]–[129], and concluding at [130]–[131]. The majority judgment cites *Kolender v Lawson* 461 US 352 (1983) at [80]; the Court's protection-of-the-law jurisprudence is traced at [118]–[121] through *Attorney General of Barbados v Joseph and Boyce* [2006] CCJ 3 (AJ), *Maya Leaders Alliance v Attorney General of Belize* [2015] CCJ 15 (AJ) [47] and *Nervais* (n 43) [45].

<sup>94</sup> *ibid* [125].

<sup>95</sup> Timothy Endicott, *Vagueness in Law* (OUP 2000); Jeremy Horder, *Ashworth's Principles of Criminal Law* (10th edn, OUP 2022). Both are cited for their general positions; no pinpoint is given.

<sup>96</sup> Constitution of Guyana, art 8; *McEwan* (n 7) [147](vii) ("Section 153(1) (xlvi) is struck from the Summary Jurisdiction (Offences) Act, Chapter 8:02 of the Laws of Guyana").

Section 19(1) and (4) are valid. Section 19(2), read literally, is not. The content element includes words with no legal meaning, and the purpose element does not distinguish the malicious from the merely sharp. The subsection as a whole, however, has a core that is both clear and proportionate: the transmission of obscene or indecent material to or about a person with intent to harass. The Jamaican Act criminalises that core and the Jamaican Director of Public Prosecutions administers it with a published high threshold, adopting the observation in *Chambers v Director of Public Prosecutions* that satirical, iconoclastic or rude comment "should and no doubt will continue at their customary level"; the harm it addresses, the use of sexualised or threatening material to torment a person, is real, and it is the harm the Vice-President described in 2024 as "people who are exploiting women".<sup>97</sup> Section 19(3) has a defensible core too, the deliberate dissemination of a known falsehood that causes serious reputational harm, but it lacks the elements that would confine it to that core.

Two remedies are available, and the argument advanced here is that the first should be tried before the second is needed.

The first is construction. The principle of legality, as restated in *McEwan*, requires that penal words which trench on expression be read no more widely than their clear language compels.<sup>98</sup> Applied to section 18, that principle reads the adverb "intentionally" as governing the whole of the actus reus, so that the prosecution must prove that the accused intended the statement to advocate, incite or excite the consequence described, and not merely that he intended to publish it; the sedition structure, in which the tendency of the words sufficed, was the structure Parliament excised, and the Act should be read as if Parliament meant it. It reads paragraph (c) ejusdem generis with paragraphs (a) and (b), which concern force and treason, so that "any criminal offence against the President or any member of the Government" means an offence against their persons. It reads "ethnic divisions" in paragraph (e) as a synonym for the constitutional formula that follows it. Applied to section 19(2), the principle reads "obscene, vulgar, profane, lewd, lascivious or indecent" as a composite phrase whose meaning is fixed by its two legally defined members, so that the data must be obscene or indecent in the criminal-law sense, with "vulgar" and "profane" doing no independent work; it reads "with intent to humiliate, harass or cause substantial emotional distress" as requiring that the humiliation or distress of the complainant be the accused's purpose and not merely a foreseen consequence of speech that had another purpose; and it treats "substantial emotional distress" as a matter requiring proof and not assertion. Applied to section 19(3), the principle requires that the falsity be of fact and not of opinion, that the knowledge be actual, and that the damage or ridicule be more than trivial. And applied to both sections, *Hector* supplies a presumption: that Parliament did not intend, in an Act whose sedition clause it removed, to criminalise the criticism of public officers in the conduct of public administration, so that publications on matters of public interest about the acts of public officials are outside sections 18(1)(c), 19(2) and 19(3) unless they threaten violence or state a known falsehood of fact.

<sup>97</sup> Office of the Director of Public Prosecutions (Jamaica), *Guidelines* (n 56) 6–7, quoting *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin); 'Amendments to Cybercrime Act will not target social media commentators – Jagdeo' *Kaiteur News* (Georgetown, 7 September 2024).

<sup>98</sup> *McEwan* (n 7) [125].

The second remedy is severance under article 8. If the courts decline the narrowing construction, the words "vulgar, profane" in section 19(2), the words "or embarrassment" in section 19(3)(b), the words "any criminal offence" in section 18(1)(c) and the words "ethnic divisions among the people of Guyana or" in section 18(1)(e) can each be declared void without disturbing the offences around them. That is the course *McEwan* took with a single sub-paragraph of section 153, and it is the course that respects the Assembly's evident purpose of keeping the offences while abandoning the sedition model.

E. Jurisdiction over speech abroad

One more feature of the second architecture needs mention, and it is jurisdiction. Section 18(1) applies to a person "whether in or out of Guyana", and section 27(1) gives the courts jurisdiction over an offence under the Act where the act constituting it is carried out "wholly or partly in Guyana", "by any person, whether in Guyana or elsewhere", or on a Guyanese vessel or aircraft; section 27(2) then deems an act carried out in Guyana where the person was outside Guyana but a computer system or storage medium in Guyana "is affected by, or contains information about, the act" or "the transmission or effect of the act, or the damage resulting from the act, occurs, in whole or in part, within Guyana".<sup>99</sup> Read literally, section 27(1)(b) is a claim of jurisdiction over every offence in the Act, including the speech offences, wherever and by whomever committed. The Convention on Cybercrime asks parties to establish jurisdiction on the territorial, flag and nationality principles; it does not ask for this.<sup>100</sup> The 2024 announcement of reform was directed in part to the difficulty of serving documents on persons overseas "using cyberspace to commit offences in Guyana", which confirms that the provision is intended to be used against persons abroad.<sup>101</sup> A charge under section 19 against a commentator abroad whose post is read in Guyana is, on the words, within the courts' jurisdiction; whether a magistrate's court can, consistently with article 144, try such a charge without a properly pleaded territorial nexus is the question the Diamond application has raised, and it is left there.

VI. The investigative powers and privacy

A. Part III against the Convention

Part III of the Act contains the procedural powers. Table 2 sets them beside the Convention.

| Section | Power                                                                                                                                                      | Authority and threshold                                                              | Convention on Cybercrime parallel                                      |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| 25      | Service providers to store traffic data for ninety days, extendable by a judge to one year; subscriber information kept for ninety days after service ends | Statutory duty; extension by a judge on the ex parte application of a Superintendent | none: art 16 provides for preservation on order, not general retention |

<sup>99</sup> Cybercrime Act 2018, ss 18(1), 27(1)–(2).  
<sup>100</sup> Convention on Cybercrime, art 22(1).  
<sup>101</sup> Ministry of Legal Affairs (Guyana), 'Nandlall announces revision of cybercrime law' (Georgetown, 25 September 2024).

| Section   | Power                                                                                                                                                        | Authority and threshold                                                            | Convention on Cybercrime parallel                                                           |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| 28        | Search and seizure, including extension to other systems and rendering a system inaccessible; seizure valid ninety days, extendable to one year              | Judge, ex parte, Superintendent, reasonable grounds for suspicion                  | art 19(1)–(3)                                                                               |
| 30        | Compelled assistance by any person with knowledge of the system or its security measures, including accessing and using it and producing intelligible output | Request of the officer executing a warrant; failure is an offence                  | art 19(4), which adds "as is reasonable"                                                    |
| 31        | Production order for data, traffic data or subscriber information                                                                                            | Judge, ex parte, Superintendent, "reasonably required"                             | art 18                                                                                      |
| 32        | Expedited preservation order, ninety days, extendable to one year                                                                                            | Judge, ex parte, Superintendent, reasonable grounds to believe the data vulnerable | art 16                                                                                      |
| 33        | Disclosure of traffic data sufficient to identify the provider or path                                                                                       | Judge, ex parte, Superintendent                                                    | art 17                                                                                      |
| 34 and 35 | Confidentiality of orders; prohibition of disclosure of data acquired                                                                                        | Statutory; offences                                                                | art 16(3), art 20(3), art 21(3)                                                             |
| 36        | Immunity from civil and criminal liability for disclosures pursuant to enforcement                                                                           | Statutory                                                                          | none                                                                                        |
| 37        | Order to remove or disable access to data "in contravention of this Act or any other written law"                                                            | Judge, ex parte, Superintendent                                                    | none                                                                                        |
| 38        | Remote forensic tools installed on or attached to a computer system                                                                                          | Judge, ex parte, Superintendent, data "cannot be collected" otherwise              | none: arts 20 and 21 concern real-time collection and interception, not covert installation |

Source: Cybercrime Act 2018, sections 25 to 38; Convention on Cybercrime, articles 16 to 21.<sup>102</sup>

The Convention makes its procedural powers subject to article 15, which requires that they be "subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties ... and which shall incorporate the principle of proportionality", and which specifies that such safeguards "shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the

<sup>102</sup> Cybercrime Act 2018, ss 25–38; Convention on Cybercrime, arts 16–21. Section 26 (a twelve-month limitation period for summary proceedings) and s 43 (admissibility of electronic data) are omitted from the table.

duration of such power or procedure".<sup>103</sup> Measured against that standard, Part III gets one thing right throughout and four things wrong.

What it gets right is that every coercive power is placed in the hands of a judge, on the application of a police officer of at least the rank of Superintendent, on a stated threshold. That is judicial supervision, grounds justifying application and a limitation of the class of applicant, and it is more than the Convention's minimum. The complaint in the debate that a judge would be permitted "to act upon a suspicion of a crime" mistook the ordinary standard for a search warrant for an innovation.<sup>104</sup>

The first weakness is section 25. The Convention's model is preservation: a competent authority orders a specified person to preserve specified data for up to ninety days, and the confidentiality of the order is protected.<sup>105</sup> Section 32 enacts that model. Section 25 adds something the Convention does not require, a general statutory duty on every service provider to retain the traffic data of every subscriber for ninety days, and subscriber information for ninety days after the end of the service, whether or not any investigation exists. That is data retention, not preservation, and it is a standing interference with the correspondence of every subscriber that article 146(1) protects in terms, justified in advance and without individual grounds. It may be reasonably required; ninety days is short; but it should be recognised for what it is.

Section 30 is the second. The Convention permits an authority to order a person with knowledge of a system "to provide, as is reasonable, the necessary information".<sup>106</sup> Section 30 goes further in two respects: it requires the person, on the request of the officer, to assist by "accessing and using the computer system or electronic data storage medium to search electronic data" and by "obtaining an intelligible output ... in such a format that is admissible for the purpose of legal proceedings", which in modern conditions means decrypting; and it makes failure to comply "without lawful excuse or justification" an offence carrying a year's imprisonment.<sup>107</sup> The words "as is reasonable" were dropped. Whether the privilege against self-incrimination is a "lawful excuse" is a question the section leaves open; article 144(7) provides only that a person tried for a criminal offence "shall not be compelled to give evidence at the trial", which does not in terms reach the investigation.<sup>108</sup>

Section 37 is the third. A judge may, *ex parte*, order a service provider or "any other entity with a domain name server" to remove or disable access to data that is being stored, transmitted or made available "in contravention of this Act or any other written law".<sup>109</sup> No notice to the person who published the data is required, no hearing is provided, and no time limit or review is attached. The order is a prior restraint on publication, obtainable without the publisher being heard, on the strength of a contravention of "any other written law". The Convention has no such provision. A takedown power directed at child pornography and at the fraudulent websites of section 17 is plainly reasonably required; a takedown power of general application to any content that any written law forbids, exercised in the publisher's absence, is not, and the section should

<sup>103</sup> Convention on Cybercrime, art 15(1)–(2).

<sup>104</sup> Hansard (20 July 2018) 24.

<sup>105</sup> Convention on Cybercrime, art 16(1)–(3).

<sup>106</sup> Convention on Cybercrime, art 19(4).

<sup>107</sup> Cybercrime Act 2018, s 30(1)(b), (d), (2).

<sup>108</sup> Constitution of Guyana, art 144(7).

<sup>109</sup> Cybercrime Act 2018, s 37.

be read as confined to data whose storage or transmission is itself an offence under the Act.

Section 38 is the fourth and the most serious. It authorises a judge, on the same *ex parte* application, to permit the police to "utilise a remote forensic tool for the investigation" where data required for an investigation "cannot be collected without the use of a remote forensic tool"; a remote forensic tool is "an investigative software or hardware installed on or attached to a computer system that is used to perform a task".<sup>110</sup> This is the power to hack. The Convention does not contain it: articles 20 and 21 address the real-time collection of traffic data and the interception of content with a service provider's cooperation, and article 21 confines interception to "a range of serious offences to be determined by domestic law".<sup>111</sup> Section 38 has no such confinement; it applies to an investigation into "an offence under this Act or any other law", which includes every summary offence in the statute book. The section carries safeguards that show its drafter was aware of the danger: the application must name the suspect and describe the target, the tool, "the extent and duration of its utilisation" and the reason; modifications to the system must be limited to those necessary and undone afterwards; a record must be kept; the information obtained must be protected; and the authorisation ceases when the data is collected or the grounds disappear.<sup>112</sup> What it lacks is what article 15 calls limitation of duration: there is no maximum period, no requirement that the target ever be told, no report to any independent body, and no confinement to serious crime. A power to install software covertly on a citizen's telephone, exercisable for the investigation of any offence and never disclosed to its object, is the paradigm case of a measure that must be shown to be "reasonably required" in the interests of public order under articles 143(2)(a) and 146(2)(a), and the Act does not attempt to show it.

### ***B. The constitutional protection of privacy***

The Constitution of Guyana has no free-standing right to privacy. What it has is article 143, which provides that "no person shall be subjected to the search of his or her person or his or her property or the entry by others on his or her premises" except by consent or under a law reasonably required for the listed purposes, and the final limb of article 146(1), "freedom from interference with his or her correspondence".<sup>113</sup> Both are qualified in the same way, by laws "reasonably required" in the interests of defence, public safety, public order and the rest, so that the *de Freitas* structure applies to them as it applies to expression. The search and seizure of a telephone is a search of property under article 143; the retention of traffic data, the production of subscriber information, the disclosure of the path of a communication and, above all, the installation of a remote forensic tool are interferences with correspondence under article 146(1). To these must be added article 154A, under which every person is entitled to the rights enshrined in the treaties listed in the Fourth Schedule, which include the International Covenant on Civil and Political Rights, the rights being enforceable by application to the Human Rights Commission.<sup>114</sup> The Covenant's protection of privacy and correspondence therefore has a domestic footing, though not one enforceable in the High Court under article 153.

<sup>110</sup> Cybercrime Act 2018, s 38(1), (7).

<sup>111</sup> Convention on Cybercrime, arts 20, 21(1).

<sup>112</sup> Cybercrime Act 2018, s 38(2), (4)–(6).

<sup>113</sup> Constitution of Guyana, arts 143(1)–(2), 146(1).

<sup>114</sup> Constitution of Guyana, art 154A(1), (4) and Fourth Schedule (listing, among other instruments, the "Covenant on Civil and Political Rights").

### **C. The Data Protection Act 2023 and its non-commencement**

The safeguards that Part III presupposes were, in the ordinary design of a modern cybercrime regime, to be supplied by data protection legislation. The telephone company that objected to the sedition clause in 2018 asked in the same letter "What about the passage of the Data Protection Act?", observing that in other Caribbean countries such legislation had been "needed as auxiliary legislation to support the efficiency of cybercrime" laws.<sup>115</sup> Guyana enacted the Data Protection Act 2023 on 16 August 2023 as Act No 18 of 2023.<sup>116</sup> It is a comprehensive statute. It states principles of processing, provides rights of access, rectification, erasure and objection, regulates transfers abroad, and establishes a Data Protection Office headed by a Commissioner appointed by the President, whose functions include monitoring and enforcing the Act, auditing the processing of personal data, and monitoring "the processing of personal data and, in particular, sensitive personal data, and any other matter affecting the privacy of persons in respect of their personal data".<sup>117</sup> Sensitive personal data includes information on a person's "sexual orientation or sexual life", "criminal record" and "proceedings for any offence committed or alleged to have been committed".<sup>118</sup> The Act does not exempt law enforcement wholesale. Section 32 exempts personal data processed for "the prevention or detection of crime" or "the apprehension or prosecution of offenders" from the first data-protection principle and from the right of access only "to the extent to which the application of those provisions to the data is likely to prejudice" those purposes, and the Act is alert to expression: no warrant may issue under it in respect of data processed for journalism unless a prior determination by the Commissioner has taken effect.<sup>119</sup>

Section 1 provides that the Act "shall come into operation on the day the Minister may, by order, appoint, and different days may be appointed in respect of different provisions".<sup>120</sup> No such order had been made when the Digital Identity Card Act was brought into force by commencement order on 31 March 2026, and the press reported at the time that the Data Protection Act "is yet to come into force because the requisite commencement order has not been issued".<sup>121</sup> No later order had been located at the date of writing [VERIFY: the Official Gazette for any Data Protection Act 2023 commencement order after 31 March 2026]. The consequence for the subject of this paper is precise. The Cybercrime Act gives the police the power to compel the production of subscriber information, to obtain the retained traffic data of every subscriber, to seize and copy the contents of telephones, and to install software on them. The Data Protection Act would subject the retention, storage, security and onward use of that data by the police, by service providers and by the Data Protection Office itself to enforceable principles and to independent supervision, which is the "other independent supervision" that article 15 of the

<sup>115</sup> 'GPA says sections in Cybercrime Bill "criminalizing freedom of expression" must go' *iNews Guyana* (Georgetown, 2 May 2018); Hansard (20 July 2018) 23.

<sup>116</sup> Data Protection Act 2023 (Guyana), Act No 18 of 2023, Official Gazette (Legal Supplement A), 16 August 2023 (hereafter "Data Protection Act 2023").

<sup>117</sup> Data Protection Act 2023, Parts II–IV (ss 4–30), s 72(1)–(3), s 73(a), (e), (g).

<sup>118</sup> Data Protection Act 2023, s 2 ("sensitive personal data", paras (h), (j), (l)).

<sup>119</sup> Data Protection Act 2023, ss 32(1), 87(3).

<sup>120</sup> Data Protection Act 2023, s 1.

<sup>121</sup> 'Digital ID law now active, but data protection act still not operational' *Demerara Waves* (Georgetown, 31 March 2026) (the Digital Identity Card Act commencement order "was published in the Official Gazette on March 26 and named on March 31 as the date on which the law took effect").

Convention contemplates alongside the judge. Until it is commenced, Part III is a book of powers without the book of safeguards that was written to accompany it. Commencement of the 2023 Act is the single most effective privacy reform available to Guyana, and it requires no amendment of the 2018 Act at all.

## VII. Proposals

The proposals are of two kinds, and the courts need not wait for Parliament before acting on the first.

The courts, beginning in the magistrates' courts where these charges are tried, should apply the narrowing constructions set out in section V: intention in section 18 governing the whole offence; paragraph (c) confined to offences against the person; "ethnic divisions" read as the constitutional formula; the content element of section 19(2) confined to material obscene or indecent in the criminal-law sense; the purpose element read as purpose; "substantial emotional distress" as a matter of proof; section 19(3) confined to knowing falsehoods of fact causing more than trivial harm; and, across both sections, the *Hector* presumption that speech about the conduct of public administration is not within them absent a threat of violence or a known lie. The Director of Public Prosecutions, whose advice ended the prosecution of the businessman's video, could give that presumption administrative form by published guidance of the kind the Jamaican Director issued for section 9 in 2017, requiring that charges under sections 18 and 19 be referred to her Chambers before they are laid.<sup>122</sup> Section 37 should be read as confined to data whose storage or transmission is itself an offence under the Act, and section 30 as subject to a lawful excuse that includes the privilege against self-incrimination. Section 16 should be read as set out in section IV: consent to the act charged, knowledge or recklessness as to its absence, and no application to images taken in public of persons with no reasonable expectation of privacy.

The second kind is amendment, and it should be targeted. Section 16 should acquire a reasonable-expectation-of-privacy limb, as the 2015 draft had; an extension to images that appear to show the person and to images of sexual activity; a definition of consent distinguishing consent to capture from consent to share; a threat-to-share offence, since section 19(4) reaches threats only where a benefit is extorted; and exemptions for journalism in the public interest, the investigation of crime, medical purposes and prior consensual publication.<sup>123</sup> Section 18(1)(c) should be deleted or confined to violence against the person; "ethnic divisions" should be deleted from paragraph (e); the word "intentionally" should be placed so that it governs the consequence; and subsection (4), the orphaned proviso of the sedition clause, should be replaced by a general saving for the discussion of any matter of public interest. In section 19 the words "vulgar, profane, lewd, lascivious" should be deleted, the penalties should be tiered so that the extortion and coercion offences carry more than the harassment offence, and subsection (3) should either be repealed in favour of the civil law of defamation, which is the direction the Guyana Press Association urged in 2018, or be confined by a requirement of serious harm and defences of truth and public interest. Prosecutions under sections 18 and 19 should require the consent of the

<sup>122</sup> Office of the Director of Public Prosecutions (Jamaica), *Guidelines* (n 56); 'Court dismisses cybercrime charge against US businessman' *Stabroek News* (Georgetown, 28 February 2026).

<sup>123</sup> Compare Sexual Offences Act 2003 (UK), ss 66B(4) (threat to share), 66C (exemptions); UN Convention against Cybercrime, art 16(2).

Director of Public Prosecutions. In Part III, section 30 should restore the words "as is reasonable"; section 37 should provide for notice and a hearing, or for prompt review; and section 38 should be confined to offences carrying a stated minimum penalty, limited in duration, subject to eventual notification of the target, and reported annually to the National Assembly. The Data Protection Act 2023 should be commenced.

The alternative course, repeal and replacement on the model of the United Nations Convention, has been announced and then overtaken. Repeal would discard the integrity core, which is sound and which the United Nations Convention would reproduce in any event; it would discard section 16, which the Convention's article 16 vindicates; and it would leave the persons now relying on the Act, the complainants in the Telegram investigation among them, without a statute while a replacement was drafted. It would also, if the 2024 announcement is a guide, be replacement in the wrong direction, since the stated purpose of the revision was that the penalties for violation "must be condign".<sup>124</sup> The defects of sections 18 and 19 are defects of breadth. They are cured by subtraction, not by aggravation, and an amending Act of a dozen clauses would cure them.

## VIII. Conclusion

The Cybercrime Act 2018 was argued over for two years about a clause it no longer contains, and passed in a night with the clause beside it unexamined. The result is a statute of two architectures. The first, sections 3 to 13 and the procedural core of Part III, is a competent domestic rendering of the Convention on Cybercrime, and it needs only marginal repair. The second, sections 14 to 19, is where the Act touches expression, and there its success is uneven.

Section 16 succeeds. It fills a gap that the Sexual Offences Act left open, it chose the consent model before the international instruments did, and it is a proportionate restriction on expression under article 146 read with *de Freitas*, subject to a narrowing construction that the principle of legality supplies and to amendments that would perfect rather than rescue it. Sections 18 and 19 do not succeed as drafted. Section 18 carries the shadow of the excised sedition clause in its structure and in its proviso; section 19 makes vulgarity and profanity elements of a crime and punishes the deliberate lie and the sharp truth alike; and both are being used, on the reported record, against speech about public officials that the Privy Council in *Hector* and the Caribbean Court of Justice in *McEwan* have placed beyond the reach of a penal statute so drawn. The argument advanced here is that the courts can, and should, read both sections down to their defensible cores now; that article 8 permits the severance of the words that cannot be read down; and that Parliament should then do by targeted amendment what construction can only approximate. Part III, finally, confers powers that in two respects exceed the Convention's model and in one respect, section 38, exceed anything the Convention contemplates, and it does so in a legal order whose data protection statute has been enacted and left uncommenced. The balance the Act was meant to strike is not beyond reach. It requires a narrower section 19, a section 18 without its ghost, a section 38 with a clock, and a commencement order.

<sup>124</sup> Ministry of Legal Affairs (Guyana), 'Nandlall announces revision of cybercrime law' (Georgetown, 25 September 2024).

## Table of Cases

### Caribbean Court of Justice

- *Attorney General of Barbados v Joseph and Boyce* [2006] CCJ 3 (AJ)
- *Maya Leaders Alliance v Attorney General of Belize* [2015] CCJ 15 (AJ)
- *McEwan v Attorney General of Guyana* [2018] CCJ 30 (AJ)
- *Nervais v The Queen* [2018] CCJ 19 (AJ)

### Judicial Committee of the Privy Council

- *de Freitas v Permanent Secretary of Ministry of Agriculture, Fisheries, Lands and Housing* [1999] 1 AC 69 (PC), (1998) 53 WIR 131
- *Hector v Attorney-General of Antigua and Barbuda* [1990] 2 AC 312 (PC)
- *Ramadhur v Ramadhur* [2020] UKPC 7
- *Suraj v Attorney General of Trinidad and Tobago* [2022] UKPC 26

### Eastern Caribbean Supreme Court

- *Rambally & Sons Ltd v Attorney General of Saint Lucia* (High Court of Justice, Saint Lucia, Civil Suit No 355 of 1999, 19 September 2000)

### England and Wales

- *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin)
- *Derbyshire County Council v Times Newspapers Ltd* [1993] AC 534 (HL)
- *R v Hicklin* (1868) LR 3 QB 360

### Canada

- *R v Nova Scotia Pharmaceutical Society* [1992] 2 SCR 606

### United States

- *Kolender v Lawson* 461 US 352 (1983)
- *Papachristou v City of Jacksonville* 405 US 156 (1972)

## Table of Legislation and Instruments

### Statutes — Guyana

- Anti-Money Laundering and Countering the Financing of Terrorism Act 2009, Act No 13 of 2009
- Anti-Terrorism and Terrorist Related Activities Act 2015, Act No 15 of 2015
- Constitution of the Co-operative Republic of Guyana, Cap 1:01
- Criminal Law (Offences) Act, Cap 8:01
- Cybercrime Act 2018, Act No 16 of 2018
- Data Protection Act 2023, Act No 18 of 2023
- Interception of Communications Act, Cap 47:03
- Sexual Offences Act, Cap 8:03 (Act No 7 of 2010)
- Summary Jurisdiction (Offences) Act, Cap 8:02

### Statutes — other jurisdictions

- Computer Misuse Act, Chap 11:17 (Trinidad and Tobago)
- Criminal Justice and Courts Act 2015 (UK), ss 33–35 (repealed)
- Cybercrimes Act 2015 (Jamaica), Act 31 of 2015
- Online Safety Act 2023 (UK), ss 188, 190
- Sexual Offences Act 2003 (UK), ss 66B–66C

### **Treaties and international instruments**

- Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) 2296 UNTS 167, ETS No 185
- International Covenant on Civil and Political Rights, as listed in the Fourth Schedule to the Constitution of the Co-operative Republic of Guyana
- United Nations Convention against Cybercrime (adopted 24 December 2024 by UNGA Res 79/243; opened for signature at Hanoi 25 October 2025)

### **Other**

- Cybercrime Bill 2016 (Guyana), Bill No 17 of 2016
- Digital Identity Card Act (Guyana) commencement order, Official Gazette, 26 March 2026 (as reported)
- Guyana, National Assembly Debates (Hansard), 93rd Sitting of the First Session of the Eleventh Parliament (20 July 2018)
- Office of the Director of Public Prosecutions (Jamaica), *Guidelines for Prosecuting Cases Involving Malicious Communications: Section 9 of the Cybercrimes Act of Jamaica, 2015* (15 May 2017)
- Parliament of Trinidad and Tobago, *Final Report of the Joint Select Committee on the Cybercrime Bill, 2017* (Fourth Session, Eleventh Parliament, 2019)
- Statutory Instrument 2024/31 (UK), Online Safety Act 2023 (Commencement No 3) Regulations 2024, reg 2

## **Bibliography**

### **Primary sources**

- Department of Public Information (Guyana), 'Cyber Crime Bill will offer shield of protection for nation's youths – AG Williams' (Georgetown, 21 July 2018)
- Ministry of Legal Affairs (Guyana), 'Nandlall announces revision of cybercrime law' (Georgetown, 25 September 2024)
- United Nations Office on Drugs and Crime, 'UN Cybercrime Convention – Full Text' and 'UN Convention against Cybercrime' (status page), unodc.org (read 4 September 2026)
- 'Amendments to Cybercrime Act will not target social media commentators – Jagdeo' *Kaieteur News* (Georgetown, 7 September 2024)
- 'Caterer charged with uploading woman's nude images' *Stabroek News* (Georgetown, 31 August 2023)
- 'Case dismissed against man over cyber "humiliation" of Home Affairs PS' *Stabroek News* (Georgetown, 27 July 2023)
- 'Controversial sedition clause removed as amended Cybercrime Bill passed' *Kaieteur News* (Georgetown, 21 July 2018)
- 'Cops probing "Guyanese ONLY" Telegram group being used to share nudes' *News Room* (Georgetown, 6 January 2023)

- 'Court dismisses cybercrime charge against US businessman' *Stabroek News* (Georgetown, 28 February 2026)
- 'Court halts cybercrime prosecution to address novel challenges to speech-based offences in Guyana' *Demerara Waves* (Georgetown, 21 December 2025)
- 'Cyber Crime law to prohibit child porn, sharing of nude images' *Demerara Waves* (Georgetown, 28 December 2015)
- 'Cybercrime Act to be repealed – AG' *Stabroek News* (Georgetown, 19 December 2022)
- 'Cybercrime Bill passed' *Guyana Chronicle* (Georgetown, 21 July 2018)
- 'Cybercrime bill targets child porn, hacking, identity theft' *Stabroek News* (Georgetown, 29 December 2015)
- 'Digital ID law now active, but data protection act still not operational' *Demerara Waves* (Georgetown, 31 March 2026)
- 'GPA says sections in Cybercrime Bill "criminalizing freedom of expression" must go' *iNews Guyana* (Georgetown, 2 May 2018)
- 'Gov't converted Cybercrime Bill to protect their interest – Opposition Leader on Clause 18' *iNews Guyana* (Georgetown, 30 April 2018)
- 'Man charged with using computer system to humiliate woman' *Stabroek News* (Georgetown, 9 September 2023)
- 'Man on \$150k bail for publishing nude pictures of ex-girlfriend' *Kaieteur News* (Georgetown, 23 July 2024)
- 'One witness called in cybercrime trial of photographer' *Stabroek News* (Georgetown, 6 January 2023)
- 'PPP/C proposing deletion of sedition clause from cyber crime bill' *Stabroek News* (Georgetown, 20 July 2018)
- 'Sedition and cybercrime' (editorial) *Stabroek News* (Georgetown, 30 April 2018)

## Secondary sources

- Citron DK and Franks MA, 'Criminalizing Revenge Porn' (2014) 49 Wake Forest L Rev 345
- Endicott T, *Vagueness in Law* (OUP 2000)
- Fuller LL, *The Morality of Law* (Yale University Press 1964)
- Horder J, *Ashworth's Principles of Criminal Law* (10th edn, OUP 2022)
- McGlynn C and Rackley E, 'Image-Based Sexual Abuse' (2017) 37 OJLS 534
- Robinson T, Bulkan A and Saunders A, *Fundamentals of Caribbean Constitutional Law* (2nd edn, Sweet & Maxwell 2021)