

Guidelines for Prosecuting Cases Involving Malicious Communications: Section 9 of the Cybercrimes Act of Jamaica, 2015

INTRODUCTION

These guidelines set out the approach that Prosecutors should take when making decisions in relation to cases where it is alleged that criminal offences have been committed by the sending of malicious communication via the use of a computer. They are designed to give clear guidance to Prosecutors who have been asked for early advice by the Police, and to guide the process when reviewing those cases which have been charged by the police.

These guidelines cover matters where a “computer” is used to send data (including images, messages) to another person, and where such data is menacing, threatening, or obscene. Therefore it is not limited to the sending of such communications via social media. In this guidance, we will explore the broad definition given to the word computer as contained within the **Cybercrimes Act, 2015**.

These guidelines are primarily concerned with offences that may be committed given the nature or content of the data sent via the use of a computer. Where the computer is used simply to facilitate some other substantive offence that may be charged and prosecuted under another Act or at common law, Prosecutors should first proceed under the substantive offence in question unless the situation lends itself convenient to prosecute an offence also under this Act. For example, if the Accused is charged with Demanding Money with Menaces contrary to **section 42A** of the **Larceny** Act but the demand was made by way of a computer, one may elect to proceed under the Larceny Act instead of **section 9** of the **Cybercrimes** Act. Experience has shown that as a Prosecutor one always strives for simplicity in laying charges for trial.

GENERAL PRINCIPLES

Prosecutors may only commence a prosecution if a case satisfies the test set out in **The Decision to Prosecute: A Jamaican Protocol.** (Please see <http://www.dpp.gov.jm>.) The test has two stages: the first is the requirement of evidential sufficiency and the second involves consideration of the public interest.

As far as the evidential stage is concerned, a Prosecutor must be satisfied that there is sufficient evidence to provide a realistic prospect of conviction. This means that an objective, impartial and reasonable jury (or Judge sitting alone), properly directed and acting in accordance with the law, is more likely than not to convict. It is an objective test based upon the Prosecutor's assessment of the evidence (including any information that he or she has about the defence).

A case which does not pass the evidential test MUST NOT PROCEED, regardless of how serious or sensitive it may be. In other words, if the material available on file does not cover the ingredients of the offence, then you cannot ethically proceed. Where the evidential test is achieved, the Prosecutor must go on to consider whether a prosecution is required in the public interest.

In the majority of cases, Prosecutors should only decide whether to prosecute after the investigation has been completed. However, there will be cases occasionally where it is clear, prior to the collection and consideration of all the likely evidence, that the public interest does not require a prosecution. In those cases, Prosecutors may decide that the case should not proceed further.

It is imperative and most useful that cases involving the sending of communications/ data via a computer undergo early consultation between Police and Prosecutors, and the Police are encouraged to contact the prosecution at an early stage of the investigation.

WHAT IS A COMPUTER?

A computer is defined in **Section 2** of the **Cybercrimes** Act as any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs the automatic processing of data. It also includes a data storage facility, or electronic communication system. An electronic communication system is further defined as any system for creating, sending, receiving, storing, displaying, or processing electronic data. This definition is wide enough to capture such devices as thumb drives, smart phones, iPads, and tablets.

OFFENCE: USE OF A COMPUTER FOR MALICIOUS COMMUNICATION, SECTION 9 CYBERCRIMES ACT

There are three ingredients that must be proved by the material presented to an Investigator before a prosecution can be initiated under this section. They are:

1. That a person used a computer to send to another person data.

Send is not defined under any current legislation and as such arguably it may include the publishing of material by a person to a social media site.

2. That the data sent is **obscene or constitutes a threat or is menacing in nature**. These terms are also not defined by the legislation.

Material that is obscene is of a sexual nature or offends against society's morality and tends to deprave or corrupt minds open to immoral influences and into whose hands these publications would fall.

Threatening material is material that intimates that harm/danger/punishment will befall a person and may be similar to a menace.

Material that is menacing in nature tends to threaten with harm or danger.

3. **AND**, that the material which is either obscene or a threat or menacing in nature, or all three, or a combination of the three, was sent **with the intention** to harass any person or cause harm or the apprehension of harm, to any person or property.

Intention may be proved by direct evidence such as statements of the suspect showing their intention or it may be inferred from all the circumstances.

These three elements referred to above must all exist in order for a section 9 offence to be created. It is also clear from this section that there is no requirement for the material published to be false or cause harm to a person's reputation and the like and as such fall under the heading of defamation. A section 9 offence may exist even where a statement is true which takes it outside the tort of defamation.

CATEGORY 1. THE TRANSMISSION OF DATA WHICH IS OBSCENE.

Communications via a computer which are obscene can be considered under the **Obscene Publications Act** or the **Cybercrimes Act, 2015**. In the year 1927, the **Obscene Publications (Suppression) Act** was passed. This Act created the offences of Possession, Distribution and Publication of obscene writings, drawings, and photographs etc. The penalty if convicted remains at the paltry sum of Jamaican \$40.00. Before the passage of the 2015 **Cybercrimes Act**, the publication or distribution of obscene images on the internet, or otherwise would give rise to a penalty of \$40.00.

WHAT IS OBSCENE DATA?

Obscene is not defined by the **Cybercrimes Act**. The definition of obscenity stated by Cockburn C.J in **R v Hicklin (1868) L.R. 3 Q.B. 360** was:

“the test of obscenity is this, whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall.”

The present common law meaning of obscene is to be found in the case of **R v. Anderson (1971) 3 W.L.R. 939**. It was stated therein that obscene is not confined to sexual content. The word obscene is not defined in the **Obscene Publications Act of Jamaica**. As such the common law definition is applicable. The words “indecent” and “obscene” convey the idea of offending against property, indecency being at the lower, and obscenity at the upper end of the scale. An indecent article is not necessarily obscene, but an obscene article is most certainly indecent. **R v Stanley (1965) 2 Q.B. 32**.

CATEGORIES 2 AND 3. DATA THAT IS THREATENING AND DATA THAT IS MENACING IN NATURE

THREATS

Communications which may constitute threats of violence to the person or property may constitute a number of offences, including those set out below.

A threat to kill contrary to **section 18** of the ***Offences against the Person Act Jamaica*** can be considered where the communication constitutes a direct threat to kill. This section reads:

“Whosoever shall maliciously send, deliver, or utter, or directly or indirectly cause to be received, knowing the contents thereof, any letter or writing threatening to kill or murder any person, shall be guilty of a felony, and being convicted thereof, shall be liable to be imprisoned for a term not exceeding ten years, with or without hard labour.”

Where the prosecution seeks to advance a case under **section 18** of the ***Offences Against the Person Act***, there must be evidence that the accused sent or delivered the writing to the complainant, and further it is a question of fact for the jury whether the contents of the writing amounts to a threat to kill or murder ***R v Boucher***, 4 C &P. 562; ***R v Tyler***, 1 Mood. 428. Cited in ***Archbold Pleading, Evidence & Practise in Criminal Cases 36th Edition at p.3615.***

Threats of violence to the person or damage to property may also fall to be considered under section 9 of the ***Cybercrimes Act, 2015.***

MENACES

This section prohibits the sending of data which is threatening or menacing in nature. The ***Cybercrimes Act*** does not define the term menace, and as such the common law definition will be applicable in the interpretation of the statute.

However, where the prosecution is seeking to prove that the message is of a menacing nature, before proceeding with such a prosecution, Prosecutors should heed the words of the Lord Chief Justice in **Chambers v DPP [2012] EWHC 2157 (Admin)** paragraph 30 where he said:

“... a message which does not create fear or apprehension in those to whom it is communicated, or may reasonably be expected to see it, falls outside,... for the simple reason that the message lacks menace.”

The case of **Chambers v DPP** also cited Sedley LJ in **DPP v Collins [2006] 1WLR 308** where he stated in the context of a message which was menacing that:

“... fairly plainly, is a message which conveys a threat – in other words, which seeks to create a fear in or through the recipient, that something unpleasant is going to happen...”

THE HIGH THRESHOLD AT THE EVIDENTIAL STAGE

There is a high threshold that must be met before the evidential stage in the **The Decision to Prosecute: A Jamaican Protocol** will be satisfied.

Prosecutors ought to bear in mind that what is prohibited under **section 9** of the **Cybercrimes Act 2015** is the sending of data which is threatening, menacing or obscene. Therefore a communication that is sent has to be more than simply offensive to be contrary to the criminal law. Just because the content expressed in the communication is offensive, done in bad taste, controversial or unpopular, or defamatory, this is not a sufficient reason to engage the criminal law. The comment of the Lord Chief Justice in the case of **Chambers v DPP [2012] EWHC 2157 (Admin)** is applicable to our legislative context. He stated, in relation to section 127 of the **Communications Act 2003 UK** which prohibited communication that was grossly offensive, as follows;

“Satirical, or iconoclastic, or rude comment, the expression of unpopular or unfashionable opinion about serious or trivial matters, banter or humour, even if distasteful to some or painful to those subjected to it should and no doubt will continue

at their customary level, quite undiminished by [section 127 of the Communications Act 2003 UK]”.

In Jamaica’s legislative context, **section 9** is specific in that it prohibits obscene communication, and therefore it is not concerned with whether the communication is offensive, but whether it has a tendency to deprave and corrupt.

CONTEXT AND APPROACH: THE MENTAL ELEMENT (MENS REA)

Prosecutors must bear in mind that before a decision is taken to prosecute, the context in which the communication is sent is of utmost importance in determining whether there exists evidence of a criminal intent to harass any person or cause harm or the apprehension of harm, to any person or property. The **Cybercrimes Act** requires proof of an intention to cause harm or the apprehension of harm and this is the highest level of subjective mens rea.

Recklessness or negligence concerning whether the sending of the information would cause harm is insufficient. This is a critical consideration before a decision to prosecute is made. In the context of social media where communication may be sent as banter, jokes, or even careless commentary, there must be evidence of a criminal intent. Therefore due regard will have to be given to the surrounding circumstances in which the message or data was sent to satisfy this element of the offence.

THE PUBLIC INTEREST STAGE

When the Prosecutor is satisfied that the evidential criteria is met, a prosecution will usually take place unless the Prosecutor concludes that there are public interest factors tending against prosecution which outweigh those tending in favour. Prosecutors must be guided by **The Decision to Prosecute: A Jamaican Protocol (<http://www.dpp.gov.jm>)** which contains the public interest test that informs the decision to prosecute.

CONSEQUENCES OF FAILING TO FOLLOW THE GUIDELINES

Prosecutors and Law Enforcement should be mindful that communications via computers and in particular via the use of social media is so vast in the 21st century that it cannot be quantified. It is truly global and without any borders – at the click of a button. Without adhering to these guidelines Law Enforcement, the Prosecuting authority and possibly members of the public who are potential complainants, could run the risk of placing a large number of cases in the Court arena which at first blush may pass the public interest test but when closely examined within the context of the guidelines would not pass the evidential test and therefore would not form the basis of a viable case to prosecute. It behoves all of us to remember that the process of assessing whether a matter should be prosecuted cannot be viewed back ways; that is from public interest to the evidential test. It must be emphasized that the evidential test as previously described ***MUST*** be passed before one considers the public interest test.

There is no room for emotion or anything else that is extraneous to the considerations previously outlined. ***That is the ethical imperative under which prosecutions are bound to take place.*** Always remembering that the burden of proving the case beyond a reasonable doubt in Court rests on the shoulders of the prosecution and it never shifts. The ultimate consequence of placing a matter before the Criminal Court that does not satisfy the evidential test will mean that a case will be thrown out.

I trust that by prescribing these guidelines it will assist in transparency and the understanding by Prosecutors, Law Enforcement and Members of the Public in the use of section 9 of the Cybercrimes Act, 2015.