Computer misuse – growing threat or the price of progress?

The medium is the message –Marshall McLuhan

INTRODUCTION

In previous years, the use of words and images to inflict damage, create menace or discomfort to others lay in the province of defamation, whether criminal or otherwise. Such cases were relatively few in number and occurred with remarkable infrequency, although it must be said that many potentially defamatory actions tended to end in a quiet settlement and an apology posted far from the front pages where much of the libel and slander began.

With the advent of the World Wide Web in the early 1990s, the instance of computer misuse arose very slowly, largely due to the lack of computers and connectivity for the general public in those early years. The increasing sophistication and lowering of cost allowed the connectivity of computer users to increase exponentially in obedience to Moore's Law[1], which posits that computers double in power and capacity and halve in price approximately every 18 months.

Naturally, this led to the increase in sharing of ideas and knowledge at an astounding rate. However, this also led to the dissemination of defamatory images and text in a manner that penetrated the human consciousness in a manner not seen since the creation of the printing press 300 years before. Messages that once had to rely on print and television to be shared now began to move at lightspeed to computers. The muttering crank in the basement and the conspiracy theorist now had the means to lie, spread the lie, and yet cower in anonymity behind the keyboard.

However, it became even more pronounced and damaging around 2000, when the first smartphones came to the masses. It is salutary to remember that we have moved from IBM-DOS to Ubuntu, Windows 10 and iOS, from Nokia 6200 to the iPhone 7, and from ICQ and MySpace to Facebook, Twitter, Instagram and Whatsapp within – believe it or not – a decade[2].

The tool that has enabled this explosion of technology, its use and its misuse, sits in virtually every pocket. You all have at least one on you, or several, right now. Mobile computing devices, whether smartphone or tablet, have revolutionized our lives, our attention spans and our human interactions, in ways unimaginable 10 years ago.

---

[1] http://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html

[2] https://www.digitaltrends.com/features/the-history-of-social-networking/

By now you may be wondering why we are taking this backward glance to less connected times. The simple fact is that we have never been so bombarded, overwhelmed and saturated with information. The other side of the coin is that we have never been more unsure as to exactly which of the information that deluges us we can, or ought to, believe. In our quest to be better informed, we now are open to more dishonesty, character assassination and downright mendacity than ever before. Rightly or wrongly, we are a ping away from the juicy, salacious, and the defamatory. Some of us, in our desire to inform and be informed, have passed it along, or blasted it out there, often without care or consideration to the classic formula belonging to the man on the Black Rock minibus [3]. "Is it true, is it kind, is it necessary?"

THE LAW

For reasons we need not analyze during this presentation, the law relating to computer misuse took its time to emerge, especially since prior to the computer age the law concerned itself more with misuse of the telephone system under the Telecommunications Act[4]. However, section 86 of that Act, concerning misuse of the telecommunications network for the purposes of transmitting a false message, proved inadequate for the prevention of the new crimes that arose with the advent of mobile networks, such as the sharing of pornographic material, either for entertainment or for humiliation of a targeted person; or the dissemination of defamatory or inflammatory messages and images.

As a result, on the 18th July 2005, the **Computer Misuse Act**[5] was proclaimed. Its stated purpose was

> "*to make provision for the protection of computer systems and the information contained in those systems from unauthorised access, from abuse by persons authorised to have access and related matters."*

The **Act** was surprisingly visionary in its language and scope, when one considers that at that time the most used and misused computer applications - BlackBerry Messenger, Whatsapp, and Facebook Messenger – were either brand new or still in "proof of concept" stage. As legislation goes, it is quite short – 22 sections in all, plus a single Schedule – but its reach and import render it one of the most profound pieces of legislation, along with the **Minor Offences Act**[6], currently in the Consolidated Index.

Of immediate interest to lawyers is section 2 of the Act, which provides that

---

[3] Adapted, of course, from the case of *McQuire v Western Morning News* [1903] 2 K.B. 100 at 109 per Collins MR

[4] Capt 282B of the Laws of Barbados

[5] Cap 124B of the Laws of Barbados

[6] Cap 137 of the Laws of Barbados

*"**2.** This Act applies to an act done or an omission made*

(a) in Barbados;
(b) on a ship or aircraft registered in Barbados; or
(c) by a national of Barbados outside the territory of Barbados, if the person's conduct would also constitute an offence under the law of a country where the offence was committed."

Clause (c) has a direct bearing upon a Barbadian accused who may be overseas, but committing offences that apply here and elsewhere as computer misuse. One of the constant concerns under any legislation is the application to offenders who may be outside the jurisdiction, and this clause serves to include such persons within the scope and meaning of the **Act**.

Sections 4-12 concern the crimes popularly referred to as "computer hacking". All offences within the aegis of these sections are indictable in nature, and span the gamut from illegal access to computer systems, unlawful interference with data, interception of data by technical means, and the possession of the means to unlawfully penetrate computer architecture.

Section 11 of the Act bears special scrutiny, especially in light of recent allegations in other jurisdictions of unlawful and unauthorized access to restricted computer systems by state and non-state actors. The fines for such activity range from BD$50,000 to $100,000, and the terms of imprisonment can reach a maximum of 7 years. For ease of reference, the list of computer systems that are considered by law as "restricted" are

(a) Archives Department;
(b) Barbados Defence Force;
(c) Central Bank of Barbados;
(d) Customs Department;
(e) Director of Public Prosecutions;
(f) Electoral and Boundaries Commission;
(g) Financial Intelligence Unit;
(h) Forensic Laboratory.
(i) Immigration Department;
(j) Inland Revenue Department;
(k) Lands and Survey Department;
(l) Land Tax Department;
(m) Licensing Authority;
(n) National Insurance Department;
(o) National Library Service;
(p) Office of the Attorney-General;
(q) Queen Elizabeth Hospital;
(r) Registration Department;
(s) Royal Barbados Police Force;
(t) the Supreme Court of Judicature; and

(u) any

(i) statutory corporation;
*(ii) company incorporated under the **Companies Act**; or*
(iii) other entity

*that provides a utility service within the meaning of the **Utilities Regulation Act.***

One may wonder why, in addition to the obvious Government-related systems and databases, the Schedule includes "companies incorporated under the **Companies Act**". Apart from the status of companies as legal persons, it should be borne in mind that corporate Barbados provides the very heart of commercial activity as well as providing services for public entities. As such, any interference with those systems would have a clear and negative impact on national commercial interests, and loss of investor confidence. A few lines of code in the wrong place at the wrong time would carry disastrous consequences for the island, hence the relatively heavy fines and prison terms associated with hacking and unlawful penetration of local systems.

At this point, our analysis of the **Computer Misuse Act** has been concerned with matters outside the ordinary scope of legal practice. It is now that we shall pay special attention to matters of everyday application and within the criminal law and cases.

Section 13 of the **Act** speaks to matters very much of the moment : the dissemination of pornographic images specific to children. As you are aware, the definition of "child" refers to anyone under the age of consent, prescribed in the Sexual Offences Act[7] as 16 years of age. To return briefly to the history of the internet in Barbados, from its introduction circa 1992 to 2000, internet access was assessed by the World Bank at 4% of the local population. By 2015, that access had reached, by the Bank's admittedly conservative estimate, 76.1% and rising[8]. This was due in no small measure to the popularity and increasing availability of smartphones, possessing ever-faster processors, cameras of increasing resolution and capability, and a network that is now at Long Term Evolution (LTE) standard, the fastest and most capable standard currently available to commercial users.

The other aspect for consideration is that these highly capable devices are easily available to schoolchildren, the majority of whom, it must be said, confine their use to strictly legal content. However, the minority who use their phones to record and upload pornographic and illegal activity are able to readily share their content with anyone who possesses the relevant application and the inclination to view and pass along that content with consummate ease, thanks to the aforementioned technology.

---

[7] Cap 154 of the Laws of Barbados

[8] http://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=BB

This section of the **Act** retains a certain dubious distinction: subsection 13(3) represents a successful attempt to define child pornography. This distinction should be viewed in the context of a particularly clever Justice of the Supreme Court of the United States, Potter Stewart, who when confronted with a need for a similar definition confined himself to the remark, "I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description; and perhaps I could never succeed in intelligibly doing so. But I know it when I see it."[9]

For purposes of reference, the definition is set out below:

> *"(3) For the purposes of subsection (1),*
>
> *(a) "child pornography" includes material that visually depicts*
>
> *(i) a minor engaged in sexually explicit conduct; or*
>
> *(ii) a person who appears to be a minor engaged in sexually explicit conduct; or*
>
> *(iii) realistic images representing a minor engaged in sexually explicit conduct;*
>
> *(b) "publish" includes*
>
> *(i) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way;*
>
> *(ii) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a); or*
>
> *(iii) print, photograph, copy or make in any other manner, whether of the same or of a different kind or nature, for* the purpose of doing an act referred to in paragraph *(a)*."

it should be noted that under the provisions of the **Act**, the act of production, dissemination, and/or possession of child pornography carries with it a maximum penalty on indictment of a fine of BD$50,000 or 5 years imprisonment for an individual, and for a corporation, the company can be fined BD$200,000. As we are aware, the directors of the company, and the employees therein, remain liable to imprisonment for the five year term.

---

[9] Jacobellis v. Ohio, 378 U.S. 184 (1964)

The next offence that has been prevalent under the **Act** is commonly referred to as "revenge porn" wherein an accused has allegedly exposed intimate images, recordings or text made of a former romantic partner with the intention of embarrassing the other party. Section 14 of the Act expressly prohibits "malicious communication" of

> *"…a message, letter, electronic communication or article of any description that*
>
> *(a) is indecent or obscene;*
>
> *(b) is or constitutes a threat; or*
>
> *(c) is menacing in character,*
>
> *and he intends to cause or is reckless as to whether he causes annoyance, inconvenience, distress or anxiety to the recipient or to any other person to whom he intends it or its contents to be communicated, he is guilty of an offence and is liable on summary conviction to a fine of $10 000 or to imprisonment for a term of 12 months or to both."*

Naturally, the burden of proof in these matters remains on the prosecution, who must show the malicious intent on the part of the defendant. It should be noted however, that while the anecdotal evidence indicates that revenge porn is a prevalent occurrence, its victims are understandably reluctant to report the offence to the police, since no-one is readily comfortable with strangers, even in law enforcement, viewing images of themselves that are sexually explicit in nature.

Clause (c) of section 14, communications that are "menacing in character" takes on a peculiar resonance when it comes to persons making public comment about persons in positions of authority, or celebrities. A certain robust flavor characterizes online engagement with politics and current affairs, but when a line is crossed into threats of violence or allegations of lurid nature that are demonstrably false, the **Act** comes into play in terms of sanction.

SIGNIFICANT CASES

Criminal

The first case under which the accused were faced with charges under the Computer Misuse Act was that of Commissioner of Police v Yarde et al, c. 2007. The Defendant was in a relationship with the virtual complainant, during which time intimate photographs were taken. When the relationship ended, it was understood that the photographs would remain confidential. Unfortunately the images came into the public

domain, resulting in the defendant and others being charged for disseminating the images online. The fact that the parties were first time offenders meant that they were not subject to fines nor imprisonment; they performed community service for the offence.

Another case of note was Commissioner of Police v Omar Watson, occurring in November 2014. This case arose when the accused allegedly sent sent a message via social media that was of a menacing nature. As of this time, the matter is still sub judice.

Other cases

The most recent and perhaps most famous local case arising from misuse of social media was that of Commissioner of Police v Gittens, Morris & Price, where in October 2013, the Nation Newspaper published a photograph of two schoolchildren allegedly having sex, which was obtained from a circulated Whatsapp post. While the charges were filed under the **Protection of Children Act**[10], consideration was given to preferring charges against those who circulated the photographs, but ultimately this was not done, given the sheer number of persons identified as having shared the offending video and images.

Civil

Aggrieved persons retain the option to pursue the civil remedies of damages and injunctive relief. The leading case on this matter comes from Trinidad and Tobago, Therese Ho v Lendl Simmons[11], the facts of which are well known to most of us. The plaintiff sued the defendant for breach of confidence, arising from his publishing of intimate photographs of them both to several persons, which subsequently went viral.

The learned trial judge, Frank Seepersad J, examined the equitable principle of breach of confidence, citing "Lord Greene MR in *Saltman Engineering Co. Ltd .v. Campbell Engineering Co Ltd (1948) 65 RPC 203* and Megarry J in *Coco .v. AN Clarke (Engineers) Ltd* [1969] RPC41:

- The information must have had the necessary quality of confidence, that is, it must not be something which is public property and public knowledge.
- There must have been an obligation of confidence in the circumstances under which the information was imparted.
- There must have been an unauthorised use of that information by the party communicating it to the detriment of the of the confider."

---

[10] Cap 146A of the Laws of Barbados

[11] H.C. 1949 of 2014, per Frank Seepersad J., reported in full at http://www.guardian.co.tt/news/2015-10-26/therese-ho-vs-lendl-simmons-court-ruling

In finding the Defendant liable for his breach of the Plaintiff's confidence, Seepersad J also cited several English and Australian authorities for the proposition that, although the parties could not claim a right to privacy, the fact of intimacy would be sufficient to give rise to a duty of confidentiality between them. The plaintiff was granted an injunction against further dissemination of the images, damages in the sum of TT$ 150,000.00 and costs.

Conclusion

It has become quite clear that some people have adopted the view that the internet provides some right to shame, denigrate and defame people with impunity. The Computer Misuse Act operates to combat that thinking by providing victims of this behavior with the means to seek the protection of the Courts and the provision of criminal sanction against the more egregious offenders.

I close with the words of Seepersad J, which applies just as well to the criminal prosecution of computer based misconduct as well as in the civil and equitable arena.

"Technological advances have dramatically increased the ease and speed with which such communication and/or sexually graphic images can be disseminated to the world and the process of capturing and disseminating an image to a broad audience can now take place over a matter of seconds by a few finger swipes.

"There is a disturbing trend to immortalise almost every facet of daily life by taking photographs and uploading them unto social media sites. Such activity should also be cautiously reviewed, since the material that is posted may cause a serious compromise to the subject's personal security as profilers and deviants can predict movements and patterns of behaviours.

" We must ask ourselves the question, "how are we to build a developed nation when we encourage and celebrate disrespect?" Respect for individuals, regardless of gender, ethnicity, sexual orientation, for the law and for authority, must define the way we live and interact with each other."