Compete

Issue No. XXVI, January 2022

Intersection of Competition, Consumer Protection and Data Privacy Enforcement

Fair Trading Commission

Compete is published annually by the FAIR TRADING COMMISSION. This magazine highlights aspects of Competition Law and Policy in Jamaica; and it is distributed free of charge to readers in Jamaica as well as overseas.

ISSN 0799-3862

Printed by:

Pear Tree Press Limited
19 Chelsea Avenue, Kingston 10.

FAIR TRADING COMMISSION
Unit 42A, New Kingston Business Centre
30 Dominica Drive
Kingston 5

Tel (876) 960.0120-4
Fax (876) 960.0763
E-mail: ftc@cwjamaica.com
Website: www.jftc.gov.jm

Facebook.com/ftc.jamaica
Twitter.com/jamaicaftc
Linkedin

Magazine Team
Edited, designed and coordinated by:
Ann-Marie Grant, General Manager
Venessa Hall, Legal Officer
Kristina Barrett-Harrison, Research Officer
Desroy Reid, Competition Analyst

Cover designed by: The Creative IQ Club, Anchovy High School, St. James, Jamaica

Compete

Foreword

In this 26th Issue of **Compete**, we explore the theme *"Intersection of Competition, Consumer Protection and Data Privacy Enforcement."* The world has become increasingly digitized with the online space being the primary mode for consumers and businesses to engage each other. This shift to and rapid increase in online transactions is accompanied by privacy concerns about the ownership and use of consumer data. The magazine therefore explores the balancing of consumer protection concerns with competition issues arising in the context of ownership and privacy.

In the Seventh Global Forum on Competition in 2008 which discussed the interaction between competition policy and consumer protection policy, the Organisation for Economic Cooperation and Development reported that the two policies shared the common goal of enhancing consumer welfare. When a third regime, specifically data privacy enforcement, is introduced in the relationship tension may arise. Academic literature has identified that potential conflicts may arise where competition policy, consumer protection policy and data privacy policy regimes converge. An integrated approach is therefore required to ensure that the objectives of one policy area are not undermined by the actions taken by the other regimes.

The articles included in the magazine touch on several topics including protecting intellectual property in the digital age, the importance of data protection in the insurance sector in Jamaica, the economics of privacy and competition in the digital economy.

In addition to the articles, the magazine highlights some of the activities the Jamaica Fair Trading Commission (FTC) completed in 2021. These include (i) market studies on the audit services industry, payment services sector and the nursing homes sector; (ii) merger investigations into the fleet management and sale/lease of commercial equipment/vehicles, and insurance brokerage sectors; (iii) investigation into anticompetitive conduct in the betting and gaming sector; and (iv) Stakeholder consultation on financial consumer protection at the regional level.

We know you will enjoy this edition of **Compete** as much as we enjoyed compiling it.

Happy reading!

Kristina Barrett-Harrison
Chairperson, Magazine Committee

CONTENTS

INVESTIGATIONS, MARKET STUDIES, ADVOCACY

ARTICLES

Investigations, Market Studies, Advocacy

Mergers & Acquisitions

Fleet and equipment management

During 2021 the Fair Trading Commission (FTC) investigated, under section 17 of the Fair Competition Act (FCA), an Asset Sale Agreement between Ameco Caribbean, Inc. ('Ameco') and Jameco Equipment Company Limited ('Jameco') through which Jameco acquired Ameco.

Section 17 of the FCA prohibits agreements which contain provisions that have as their purpose the substantial lessening of competition, or have or are likely to have the effect of substantially lessening competition in a market.

The FTC examined the markets in which Ameco and Jameco and its affiliates operated and their relationship to each other prior to the acquisition to determine if there were any competition concerns emanating from the acquisition. Ameco provided fleet and equipment management solutions and industrial equipment supplies and servicing across Jamaica. Jameco, which was incorporated in December 2019 to hold the newly acquired entity, is an affiliate of the Stewart's Automotive Group (SAG). Prior to the acquisition, SAG sold parts and vehicles to Ameco, and approximately 40-50% of Ameco's vehicles were supplied by SAG.

For the assessment of the effect on competition, the following markets were determined to be relevant markets: fleet management; sale of commercial equipment/vehicles; and lease of commercial equipment/vehicles in Jamaica.

The FTC concluded that while the acquisition was unlikely to adversely affect competition in the current markets, because Ameco did not compete with Jameco or any business to which Jameco was affiliated with, a Restraint of Trade clause within the Agreement was likely to unduly restrict competition in the relevant markets in the foreseeable future and therefore could breached the FCA.

Upon the FTC's conclusion of the assessment, the parties revised the Agreement to adequately address the concerns identified by the FTC.

Insurance brokerage

In March 2021, the FTC completed its investigation into agreements for Sale and Acquisition between Billy Craig Insurance Brokers (BCIB) and MGI (Insurance Brokers) Limited through which BCIB acquired MGI.

The investigation was carried out pursuant to section 17 of the FCA, to determine the competition impact of the transaction. Specifically to determine, whether the agreements contain provisions that have as their purpose the substantial lessening of competition, or have or are likely to have the effect of substantially lessening competition in a market.

The relevant market was defined as the market for insurance brokerage services and it was concluded that the agreement were unlikely to have the effect of substantially lessening competition since it would not remove any significant competitive restraint in the market. The market includes several brokers which could offer a significant competitive restraint in the foreseeable future.

Market studies

Audit Services Industry

The FTC conducted an exploratory study on competition in the market for audit services. The study examined competition in the market for auditing services in Jamaica with focus on two areas: (i) trends in market concentration over the period 2013-2018; and (ii) industry-specific interactions between the top two leading auditing firms ('Big 2') and other auditors ('Non-Big 2') of the companies listed on the Jamaica Stock Exchange.

Over the review period, the audit services market was revealed to be highly concentrated with the Big 2 firms consistently generating in excess of 90 percent of the audit fees for the industry. The share of the market controlled by the Big 2 auditors exceeds the commonly accepted oligopoly threshold of 60 percent. From the study it was shown that the Big 2 firms are engaged in fewer audits but accounts for an increasing share of the revenue.

The results also show that clients rarely switched away from a Big 2 auditing firms to a Non-Big 2 firm. The Big 2 auditors are likely to gain larger clients from switching as evidenced by the four companies that switched from Non-Big 2 auditors.

Based on the findings of the study, further work is needed to examine the conditions of entry, expansion and exit to better understand and characterize the persistently high concentration levels observed in the audit services market during the review period.

Payment Services Industry

With the growth and expansion of the digital payment system in Jamaica, the FTC undertook a study of the payment services sector to gain an understanding of how the sector operates, and to assess the scope for and level of competition in the sector. Payment and settlement systems consist of different systems, platforms, payment products and services that allow for the transfer of money daily without having to use cash. They play a crucial role in economic activity by providing mechanisms for economic agents to settle their financial obligations arising from economic transactions.

The main findings of the study includes: (i) the market for acquiring merchants for the card networks (Visa and MasterCard) is concentrated, (ii) the market for issuing cards is competitive and the barriers to entry are relatively low, (iii) entry into the card network market is difficult due to the capital outlay required, the uniqueness of the network payment system that characterises the industry, the continued shift away from the alternatives such as cash, the brand development by the card networks that has endeared them to consumers and the longstanding relationships with issuers, (iv) consumers are able to act as constraints to the card networks but they have little incentive given the direct benefits they receive from the card networks at the cost of the merchants and indirectly themselves.

Nursing Homes Services Industry

Given the spotlight on care for the elderly during the Covid-19 pandemic, and the Staff's observation of an increased number of complaints emanating from the sector, the FTC conducted a study of the nursing care homes market in Jamaica. One of the main findings of the study is that it is difficult for individuals to gather relevant information to assess the desirability of a given nursing home. This has resulted in consumers being unable to make informed decisions. For example, a mystery shopper exercise highlighted (i) an unwillingness of nursing home operators to provide pertinent information to prospective customers over the phone and no such information is present on the websites or social media pages of operators; (ii) operators misrepresenting their registration status with the Ministry of Health and Wellness (the Ministry with responsibility for overseeing the sector); and (iii) the inadequacy of the resources allocated by the Ministry of Health and Wellness to monitor and/or resolve matters arising in nursing homes.

Advocacy

Advocating for competition is an important part of the work of the FTC. Through its advocacy efforts, the FTC has reviewed several legislation to determine their effect on competition and consumer welfare and, where needed, to advocate for the inclusion of competition principles.

Included in its reviews are the Electronic Transactions Act, the Electricity Act as well as the All-Island Electricity Licence.

During the year, the FTC continued to work with sector regulators to collaborate on policy development issues to enhance consumer welfare through competitive markets. Work continued with the Spectrum Management Authority, the Broadcasting Commission (BC), and the Betting Gaming and Lotteries Commission (BGLC).

At the request of the BC, the FTC commenced market studies of the cable TV sector and the operations of hyperscalers. Digital hyperscalers are e-commerce entities that dominate the public cloud and cloud services industries and expand their businesses into numerous related industries; for example, media and communication. Essentially the FTC is assessing the competitive effects of digital hyperscalers' participation in the communications markets in Jamaica, and the ability of local operators to compete with those hyperscalers.

Concerning the lotteries market, with two recent entrants and the intensification of competition through higher payouts, the BGLC asked the FTC to assess the competition dynamics in that market to determine whether regulatory intervention may be necessary.

The incumbent lottery operator has offered gaming products in Jamaica for over 20 years. In 2021, two operators entered the market, and signaled their intention to offer more favourable payouts than that offered by the incumbent. The incumbent subsequently sought approval from the BGLC to offer even more favourable payouts.

The BGLC asked the FTC to assess the matter amidst concerns that these higher payouts are likely to compromise the viability of the industry.

Select engagements with Regulators and Industry Groups

- **Jamaica All Island Chambers of Commerce** — the main issues raised include the practice of price gouging, quality of service and billing practices in the telecommunications and electricity sectors.
- **Ministry of Science Energy and Technology's (MSET's) Petroleum Tanker Driver Joint Working Group** — the primary objective of the Working Group is to make recommendations for improvements in employment conditions. Concerns were raised about whether the Fair Competition Act (FCA) imposes any restrictions that would prevent the joint negotiations on tanker drivers' wages and employment conditions. The group was assured that the FCA does not apply to arrangements for collective bargaining on behalf of employers and employees for the purpose of fixing terms and conditions of employment.
- **MSET** — through a report entitled "Recognizing the FTC's jurisdiction in the Regulatory Framework for the Petroleum Sector", the FTC sought to have a formal system developed within the regulatory framework for the petroleum sector which requires that the FTC be notified of conduct, which could adversely affect competition.

University Council of Jamaica — the FTC completed and submitted an opinion to the University Council of Jamaica (UCJ) on online marketing initiatives by overseas-based universities that provide educational services to Jamaicans who may not be aware of a given university's registration or accreditation status. The FTC opined that as these universities are not registered in Jamaica, their conduct falls outside the FCA's jurisdiction. Further, the UCJ is the appropriate entity to resolve issues regarding registration and accreditation.

FTC's CARICOM participations

Common financial consumer protection regime

In supporting the Caribbean Community (CARICOM) Secretariat's decision to develop a common financial consumer protection (FCP) regime to regulate the conduct of financial service providers (FSPs) and to protect clients of financial institutions in CARICOM, the Fair Trading Commission (FTC) responded to CARICOM's request for information on competition issues in Jamaica's financial markets.

CARICOM's objective is to develop a FCP regime "by promoting the modernization of the financial infrastructure and the development of fair and efficient financial markets" in the Caribbean Single Market and Economy (CSME).

The FTC's submission covered the FTC's experiences in handling competition issues, and views on legal and regulatory challenges in enforcing Jamaica's competition legislation, and the key issues currently of concern to financial sector consumers which should be addressed.

CCC/JAMBAR Workshop

The FTC participated as a resource discussant in the CARICOM Competition Commission (CCC) and Jamaica Bar Association Workshop entitled, "*Competition Law in the CSME & Compliance Considerations for Attorneys-at-Law*".

CARICOM CSME Task Force

The Executive Director chaired the Joint Meeting of Competition, Trade, Finance & Legal Officials to consider the recommendations relating to the CCC functioning in a proposed dual role: as the regional competition authority as well as functioning as the national competition authority for Member States that do not have an established competition authority.

Home My Transactions Guidelines Logout

FTC gets new case administration document system

Under Jamaica's Foundation for Competitiveness and Growth Project, LPA Corporate Solutions Limited (LPA), a software developer, was contracted to create a customized enterprise content management system for use by the FTC and the Consumer Affairs Commission (CAC).

The system, branded CADS (case administration document system) will enable the FTC and the CAC to better manage and control information and streamline business processes to increase productivity and efficiencies. It will bring all information together in a systematic way that helps users to make decisions faster. The content to be managed by the system includes information and data relating to complaints, cases, market studies, reports, surveys, statistics, communications with other Ministries, Departments and Agencies, and the administrative and operational functions of the FTC and the CAC.

Businesses and consumers will benefit from a user-friendly system when submitting complaints or requesting information. Additionally, they will be provided with a tracking number that will enable them to independently check for general status updates on matters submitted.

The scheduled date for the full deployment of the ECMS is February 2022.

FTC participates in ICN annual conference

The 20th Annual Conference of the International Competition Network (ICN) was held virtually from October 13 to 15, 2021. Hosted by the Hungarian Competition Authority, the conference covered a range of topics discussed by experts in the competition community. In addition, it provided insight into the intersection of competition, consumer, and data protection policies and discussed several topical issues and challenges in enforcing competition law in the post-COVID-19 world. The conference attracted 1,768 registered competition law experts and practitioners from 97 countries.

For the second consecutive year, all members of the FTC's Technical Staff benefitted from the rich discourse on competition issues. We were particularly interested in hearing the experiences of other competition agencies and learning from them on agency effectiveness and enforcing competition law in the context of a growing digital economy. Accordingly, the Staff attended sessions covering a diverse selection of interesting topics facilitated by the Cartel, Advocacy, Agency Effectiveness, Merger, and Unilateral working groups of the ICN.

The conference covered areas such as "Sustainable Development and Competition Law", "Enforcement Priorities in Action: An Agency Effectiveness Perspective", "Hands-on Defining Dominance in the digital Era" and "Digitalization, Innovation and Agency Effectiveness".

Additionally, Mr. David Miller, Executive Director, participated as a discussant in the Advocacy Working Group's break-out session entitled "Re-thinking the Advocacy Toolkit". His presentation focused on two questions: Is your Agency facing new issues with an advocacy dimension?; and What advocacy responses have you developed to address them? Mr. Miller described the Jamaican experience on the benefits to Jamaica's Government and business community from having a robust competition advocacy programme; the pandemic's impact on Jamaica's consumers of telecoms services; and the FTC's collaboration with sector regulators in identifying new ways to manage Jamaica's spectrum holdings.

Appointment of Commissioners


Donovan White | Chairman

The Minister of Industry, Investment & Commerce, the Honourable Audley Shaw, appointed the Commissioners of the Fair Trading Commission for the period March 15, 2021, to March 14, 2023.

The persons appointed are Mr. Donovan White, Director of Tourism; Mr. Robert Collie, Attorney-at-Law; Mr. Stuart Andrade, Financial Analyst; Ms. Dorothy Lightbourne QC, Attorney-at-Law; and Mrs. Suzanne Ffolkes-Goldson, Attorney-at-Law.

Mr. White has been appointed to serve as Chairman and Mr. Collie as Deputy Chairman. Both Mr. White and Mrs. Ffolkes-Goldson are serving for the first time as Commissioners, while Ms. Lightbourne, Mr. Collie, and Mr. Andrade were reappointed.

In furtherance of the merger between the FTC and the Consumer Affairs Commission (CAC), all the FTC Commissioners are also Directors of the CAC. The other CAC Directors are: Ms. Daena Ashpole, Ms. Michelle Parkins, Dr. Marina Ramkissoon, Ms. Joyce Young, Mr. Kwame Gordon, Mr. Damali Thomas, Mr. Oneil Grant, Mr. Collin Virgo and Mr. Vernon Derby.

The Staff of the FTC welcomes the new Commissioners and look forward to a fruitful working experience as we continue to promote competitive markets.

AIRPORTS AUTHORITY OF JAMAICA

THINKING DEVELOPMENT... MOVING AHEAD

Contributes substantially to the national economy, while promoting the expansion of air transportation and its related industries

Has successfully supported fair trading through competitive Request for Proposal processes for selection of private operators for Norman Manley International Airport and Sangster International Airport

Endorses the Fair Trading Commission's mandate for competition in the conduct of trade, business and the supply of services in Jamaica

Encourages competition with the view to provide customers with options and competitive prices for products and services including flights, ground transportation, retail concessions and other commercial offerings at Jamaica's airports

876-924-8835-7

aaj@aaj.com.jm

@AirportsJamaica

@airportsauthorityja

Airportsauthorityjamaica.aero

Youtube

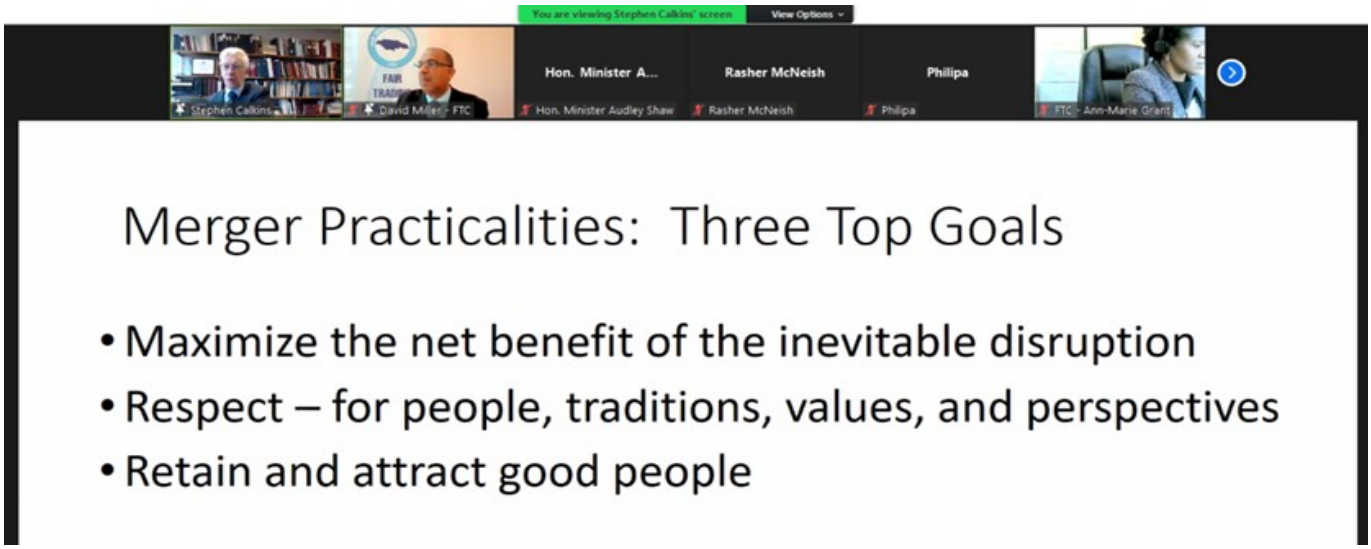
FTC 19th Shirley Playfair Lecture

On December 8, 2021, the Fair Trading Commission held the 19th Lecture in the Shirley Playfair Lecture series. Mr. Stephen Calkins, Professor of Law from the Wayne State University, delivered the Lecture under the theme "Integrating Competition Law and Consumer Protection Law: Optimizing Consumer Welfare."

In opening the programme, Mr. David Miller, Executive Director of the Fair Trading Commission, shared a quote from Dr. Lori Playfair, daughter of the late Shirley Playfair. Dr. Playfair stated that she and her sister Lisa view the Lecture "as a great learning experience for policymakers and consumers. Advocacy and education were our mother's passions and our nation should continue to benefit from these lectures".

The Lecture, which was described by the audience as informative, insightful, and engaging, explored the role and advantages of a single authority enforcing competition law and consumer protection law. Mr. Calkins drew on experiences primarily from the Irish Competition Authority and the United States Federal Trade Commission (USFTC) and described issues, concerns and challenges from institutional, legal, operational, marketing, and staffing perspectives while highlighting the benefits that may redound to the business community and consumers.

Drawing from a USFTC report on Internet Service Providers, Mr. Calkins emphasized that "deception (misleading behaviour) can lead to increased market power and the concern is that the market power of firms can make deception worse … [It] is useful to have one agency deal with these issues".



He gave illustrative examples of competition issues and consumer protection issues, described how they may intersect and provided insights on the appropriate tools that should be used, when these tools should be used, and the relevant circumstances. In recognition of the benefits that can be had from merging the two agencies, Mr. Calkins highlighted, as traditional benefits, (1) marketing (2) being able to look at both sides given that the distinction between competition and consumer protection is often times blurred, and (3) acquiring and developing skills and tools that are applicable to both areas.

Mr. Calkins concluded by identifying three goals of the practicality of merging: (1) Maximise the net benefit of the inevitable disruption. (2) Respect - for people, traditions, values, and perspectives. (3) Retain and attract good people.

Minister Audley Shaw, Minister of Industry, Investment, and Commerce, delivered pointed remarks on the purpose and expectations of creating a single authority that will enforce both the competition law and the consumer protection law. Of that authority he stated that it "will engender improved operational efficiencies, and drive a highly productive relationship among consumers, businesses, and the economy."

The Lecture was followed by a vibrant Question and Answer session. The audience posed questions primarily on the institutional, policy and legal perspectives while exploring different operational areas relating to staffing and marketing the single authority.

In closing the Lecture, Mr. Miller extended a special thank you to the Staff who planned and staged the event. In reflecting on Mr. Calkins' statement from his Lecture, that there generally exists a high level of knowledge and expertise in agencies, Mr. Miller commended the Staff for their high-quality work and commitment, highlighting that the Staff's expertise and competencies cover their core responsibilities as competition practitioners, information and communication technology, as well as public relations and staging events such as the Lecture. Mr. Miller added that "The FTC will continue to use its global ties by leveraging relationships with persons like Stephen Calkins to strengthen competition law in Jamaica."

Converging Points of Interface: Competition, Data Protection and Privacy Laws

By **Venessa Hall** | Legal Officer | FTC

Arguably, competition law, data protection law, and privacy laws are distinct disciplines. However, with the rise of big data, there has been an awakening of new considerations within the competition law sphere concerning the role data protection and privacy principles should play in competition law assessments. This article will discuss the interplay between these disciplines and the importance of competition law broadening its toolkit to identify competition concerns in the digital economy.

In recent years, the digital economy has grown exponentially due to rapid technological advancements and the expansion of internet access globally. This growth has resulted in business models based on the collection and processing of big data. The creation of big data is facilitated by the rise of internet platforms, e-commerce, and smart devices. Big data, according to De Mauro et al (2016), is the information asset characterized by such a high volume, velocity, and variety to require specific technology and analytical methods for its transformation into value.

The collecting, processing, and exploiting of personal data for commercial use may be seen as a consumer protection matter instead of one for competition law enforcement. This is so as consumer protection focuses on conduct involving businesses that have a direct impact on consumers (Brill, 2011). Consumer law safeguards the informed, free choice of consumers and the welfare of individual consumers. While competition law was designed to protect consumers from unfair practices, such as abuse of dominance, price-fixing, and exclusive dealing, and encourage competition among rivals. Thus, competition law leads to innovation and benefits consumers as they would have better choices among suppliers. Competition law, therefore, protects all consumer welfare in the economy.

Consumers may be unaware that by using online services, they are surrendering their data. There is often a lack of

transparency concerning the extent to which personal data is being collected, processed, and passed on to third parties. Personal data has become the new currency for the digital economy and is considered a valuable form of payment to companies (O'Callaghan, 2018). While personal data has obtained economic value, it also encompasses intrinsic privacy concerns for individuals. Thus, it is therefore not only a question of the interplay between competition law and consumer protection law but also data protection law.

Data protection law safeguards the rights of the data subjects (individuals). It enforces the requirement of the data subject's consent regarding the processing of their data. This is so, particularly where the data is being processed for direct marketing purposes or where the data is being transferred to third parties. Competition, consumer, and data protection laws share the overarching aim of protecting the welfare of individuals in the modern economy.

From a competition law perspective, the ability to collect, process, and exploit data has positive competitive effects. By using big data, businesses can be more creative and innovative. Also, big data collect the choices of internet users. Businesses knowledgeable of consumers' needs can target their individual preferences. The pro-competitive effects of businesses using big data are increased efficiencies and productivity gains. Consumers benefit by receiving improved customer experience, better product choices, and perhaps lower prices.

Therefore, one of the characteristics of the digital economy is firms undertaking various strategies to obtain and sustain data advantage as they get large volumes of personal data. This personal data will assist advertisers to better target consumers with behavioural advertising. Notably, within competition law, there have been concerns that big data can also confer market power and competitive advantage. This is evidenced by several mergers and acquisi-

tions in the digital markets that have demonstrated that competition law consideration may be needed, particularly given the possible control of one firm over a large data set (OECD, 2016).

Facebook's acquisition of Whatsapp is one such example, where the acquisition brought to the fore the issue of privacy considerations in the assessment of competition law. Whatsapp messaging service had millions of users because it was entirely private and highly secure. It also competed with Facebook groups or messenger services and other messaging apps. On the other hand, WhatsApp was free or payment of a nominal fee, depending on the jurisdiction. This nominal fee charged by WhatsApp was in exchange for an ad-free service without any data collection compared to the free use of Facebook messaging with the data collection for target advertising purposes (OECD, 2016).

The raised competitive concerns for competition authorities because Facebook was eliminating a rival and would degrade the privacy protections offered by Whatsapp over time. The degradation of privacy policies could affect aspects of product quality or an increase in product prices. This price would be that consumers would be required to provide more personal data (Cowen, Barraclough & Koran, 2021). Privacy has become a dimension of product quality and, based on the growth of the digital economy, a warranted inclusion in the assessment of anticompetitive conduct. This has been recognized by several competition agencies. Notably, in 2019, Germany's competition authority prohibited Facebook from combining user data from different sources. The competition authority noted that Facebook's terms and conditions allowed them to collect user data even outside of Facebook. All data collected on Facebook, by Facebook-owned services (Whatsapp and Instagram), and from third-party websites can be combined and assigned to the Facebook user account. Facebook was therefore found to have a dominant position in the German market for social networks and abused its dominant position based on the extent to which it collected, merged, and used data constituted an abuse of its dominant position. The competition authority highlighted that many users were not aware of how the selection of certain privacy settings impacted the collection of their data. The competition authority, therefore, prohibited Facebook from continuing this practice without first obtaining the user's consent.

In a report published September 2021, the Australian competition authority has indicated that Google dominates the online advertising market resulting in harm to publishers, advertisers, and ultimately consumers. It was determined that more than 90% of clicks on Australian advertisements in 2020 were at least partly as a result of one of Google's offerings. The Australian competition authority has requested new rules from its legislators to address the imbalance of advertisers to consumer data to have a healthy digital ecosystem. These new rules would include forcing the separation of data between business units or the sharing of data with competitors.

Consumer, competition, and data protection laws have different objectives and scope of applications. However, competition law considerations related to the misuse of data privacy policies are growing in importance. Harm to consumers occurs when the conduct of businesses erodes effective competition, and the usurping of consumer choices is of paramount concern to competition authorities. Accordingly, competition authorities will have to evolve to assess and enforce competition concerns that arise due to the peculiarities of the digital economy.■

The Interplay of Competition and Data Privacy in Zero Price Markets

By **Michelle Phillips** | Legal Officer | FTC

With the prevalence of digital technology and the internet it is now more important than ever that Competition Authorities consider the interplay between competition, data privacy and consumer protection. Competition Authorities should put measures in place to incorporate data protection measures in competition remedies such as incorporating data protection elements into competition law remedies.

In the last 20 or so years, there has been a dramatic global shift to the use of digital technology and the world-wide web. So much of what we do in our daily lives takes place online; we shop, bank, transact business, have video meetings in real-time, connect with friends and relatives and search and obtain information online, and the list goes on.

With this shift came the emergence of the zero-price market in the early 2000s. A zero-price market is a market where there is no charge /users of goods or services do not pay for the use of said goods or services.[1] Examples of these zero-price markets include Google, Facebook, and Instagram. These zero-price markets have exploded in recent years, operating under the precept that the services they provide are free of charge.

Changes these zero-price market digital platforms have made to our society have had several benefits for consumers. These benefits include providing individuals with convenient, ready access to information and the ability to connect globally via email, voice and video calls, etc. in ways that may not have been possible or practicable before.

These benefits have not come without costs and consequences. There is no monetary sum to use these platforms, but there is a "charge/cost" for using them- your personal data. Enterprises that operate in zero-price markets use algorithms to collect data from you while you use their platform. They then use this information to predict your behaviour and personality traits and use and/or sell this personal data to advertising companies and others. The more data the platform collects, the better advertisers can target their audience and influence their behaviour.[2]

The data collected by these platforms is the consideration, the quid pro quo, it is what is exchanged or given by persons, the hidden "cost/ price" for using these so-called "free" platforms. This form of "payment" is extremely valuable both to platform operators and to advertisers.

Leading digital platforms rely on the collection, storage, and analysis of large volumes of consumer data to drive their services as well as their profits. This is where privacy issues creep in surrounding these zero-market digital platforms.

While most consumers are aware that they are "giving" their information for use by the platform, it is doubted that most know the extent to which this data is collected, stored, processed or how it is subsequently used.[3] Issues,

therefore arise concerning whether consumers are fully informed as to the collection of their personal data or whether same is at least in part an involuntary "surrender" of information; the storage and use of their personal information; whether said information is being stored on a secured server; and in relation to the subsequent sale or use of this consumer information.

Access to data in these zero-price markets will likely boost competition. However, the reverse is true for privacy. Increased competition may increase the level of privacy in these markets, due to for example two platforms that offer a similar service aiming to distinguish themselves in terms of the increased privacy they offer to users of their platform. However, mergers between competing firms could reduce the level of privacy and/or privacy-protective product options available to consumers subsequent to a merger.

The ability to acquire, store, process, analyze and use large volumes of data gives dominant firms a comparative advantage in the digital market. Additionally, the accumulation and use of the data has the potential to increase the market power of large digital firms. The concern that Competition Authorities have with these zero market platforms is that an undertaking in a position of dominance may engage in conduct to strengthen its market power and/or to prevent or impede barriers to entry or expansion. Since market power is generally measured in relation to costs or the ability of a firm to raise prices, competition agencies will have to come up with another measure for market power for zero-price market entities.

A way in which undertakings may attempt to strengthen their market power and/or raise barriers to entry or expansion is by self preferencing. Self preferencing involves actions of enterprises that are designed to favour their own products or services, that are often vertically integrated, over those of their competitors.[4] It involves leveraging the power and data collected from one side of the platform, for example on the consumer side, to gain a competitive advantage and strengthen their position on another side- for example on the advertising side.[5] An example of this was seen in Google's plan to get rid of third-party cookies in Google Chrome. This would cut off other parties' ability to track users in Chrome, while Google would keep that data and advantage for itself.[6] This would appear to increase privacy, but it would allow Google to add to its user -data advantage and make it harder for rivals to compete with it.[7] Self preferencing is a form of discriminatory conduct that is potentially harmful to the competitive process with the potential effect of excluding competitors and constituting an abuse of a dominant position depending on its effect on consumers and rivals.

As the internet and these zero market platforms play a greater role in our society, it is increasingly important for competition authorities to consider the dynamics between the competitive process and data privacy (which has implications for consumer protection) in these markets. Some recommendations are incorporating data protection elements into competition law remedies; assessing market power in relation to personal data as well as quality of service, innovation, and privacy; creating conditions for genuine competition on privacy and heightening merger notifications or merger controls including assessment on the impacts on data. By recognizing the weaknesses and taking steps to remedy them, it is hoped that privacy and competition can co-exist in harmony in these zero-price markets.■

Endnotes

[1] Baker McKenzie- Competition in the Digital Economy an African Perspective

[2] Louise O'Callaghan, The Intersection between Data Protection and Competition Law: How to Incorporate Data Protection, as a Non-Economic Objective, into EU Competition Analysis.

[3] Julie Brill, The Intersection of Consumer Protection and Competition in the New World of Privacy- Competition Policy International Volume 7, Number 1 , Spring 2011

[4] Baker McKenzie- Competition in the Digital Economy an African Perspective

[5] Ibid.

[6] Antitrust and Privacy are on a Collision Course available at Antitrust and Privacy Are on a Collision Course | WIRED

[7] Ibid.

[8] http://privacyinternational.org/learn/competition-and-data

FINANCIAL SERVICES COMMISSION

The FSC is committed to financial literacy, which ultimately leads to financial inclusion.

Planning for retirement means you won't become a burden to your family, friends or society.

But you have to invest wisely!

Invest wisely now AND plan for retirement.

Always check before you invest.

Contact the Financial Services Commission.
We're here to regulate, protect, and educate.

FINANCIAL SERVICES COMMISSION

Promoting Integrity in the Jamaican Financial Sector

Tel: 876-906-3010

Website: www.fscjamaica.org
Email: inquiry@fscjamaica.org

@fscjamaica

The Economics of Privacy

By **Peter-John Gordon** | Lecturer | University of the West Indies, Mona

Economists while acknowledging the importance of the non-economic aspects of privacy nevertheless concentrate on the Economics of Privacy, even though they face challenges in applying their usual tool kit. The definition of privacy is problematic because privacy sensitivity differs from person to person, therefore what should be private varies. Privacy does affect economic outcomes in a number of areas: pricing, selection, advertising, identity theft among others. Privacy issues usually arise at the boundaries of private and public spaces. Navigating these boundaries require trade-offs which are both tangible and intangible. The ubiquitousness of sensor technologies and mobile computing are constantly blurring the lines between online and offline, between physical and digital, and therefore between private and public.

The growing use of social media and other online activities, have transformed individuals from mere consumers, to also producers of information. These data include their demographic profile, physical places and websites visited, preferences as revealed by purchases, pictures and other posts etc. These data have great value, commercial and otherwise. Such data make targeted advertising possible. Political uses have been made of such data – recall Cambridge Analytica's use of information gathered by Facebook in the 2016 US presidential election.

Individuals can both benefit from and be hurt by sharing their personal information. Benefits include receiving more targeted advertisement and increasing the accuracy of their online searches. Harm can be experienced when these data are used to decrease their utility - higher prices, discrimination, and identity theft etc.

Pricing privacy/personal information is difficult. There are no data markets where individuals can sell their personal information. Approaching the pricing issue from the supply side: should the price reflect the amount the data subject (person whose personal information is collected) would accept in exchange for her information, should it reflect the amount she would pay to prevent her information becoming public, or should it

Should privacy be treated like any other good and therefore the use of market forces would be appropriate…?

be related to the expected cost she would suffer if her information became public? From the demand side: should the price reflect the profit the data holder (person who collect these data) can make from personal information? What should be the underpinning philosophical determining the sharing of surplus generated? Should privacy be treated like any other good and therefore the use of market forces would be appropriate; or should privacy be seen as a fundamental right, requiring regulation? Should the data subject who owns the data be favoured or the data holder who has invested in its capture and storage?

These questions have lead many economists to see privacy not as the absence of sharing, but rather as control over sharing. Posner (1981) declares that privacy is redistributive.

Economists are primarily concerned with maximizing social welfare - the sum of consumer surplus (the difference between the maximum a consumer would be willing to pay and what she actually pays) and producer surplus (profit). In many instances others are affected (externalities), either positively or negatively, and their welfare must also be considered.

Economic theory and empirical findings do not allow us to unambiguously state that privacy protection, leads to a net positive or a net negative effect on social welfare. The outcomes are context specific.

Data subjects are mostly ignorant of privacy threats - when their private

information is being collected, whom it will be shared with and for what purpose. Few are sophisticated enough to understand the landscape e.g. knowing what information magic cookies access on their devices.

Private information falling into the wrong hands could lead to dangers including blackmail, embarrassment, identity theft or worse. The Aite Group estimates that during 2020, forty-seven percent of Americans experienced financial identity theft amounting to US$712.4 billion. People are reluctant to deposit their biodata in a repository if they are not confident about its security: could their fingerprint find its way from the repository to a crime scene? All of these negatives make consumers reluctant to share personal information.

Sharing of personal information online does have positive externalities which benefit society as a whole; for example when these data, including pharmaceutical drug use are aggregated they could unveil unexpected interactions (White et al. 2013) and act as early alerts for epidemics (Dugas et al. 2012).

Merchandisers having specific information on each consumer makes it possible to approach perfect price discrimination. Mikians et al. (2013) find price differences of between 10 percent and 30 percent for identical products based on location and characteristics (e.g. browser configurations) of online visitors. Economic theory tells us that perfect price discrimination results in the same aggregate welfare as perfect competition with the only difference being that all the surplus goes to the seller and buyers receive zero. From a welfare maximizing position this is perfectly acceptable, however while some consumers are made better off, others are forced to pay higher prices. Such consumers would rather conceal their private information.

Failure to share information could force others to rely on statistical discrimination, e.g. privacy regulations on criminal records may lead employers to substitute their own biases which disadvantage certain groups (Strahilevitz 2008). Privacy in other situations could be beneficial. African American landlords in New York City received approximately 12 percent less for equivalent rental (Edelman and Luca 2014) and preventing auditioning panels for orchestral positions from seeing applicants increased the probability of women being hired (Golding and Rouse 2000). Information gleaned from social media allow employers to discriminate on subjects which might be prohibited by law from being raised at interviews e.g. religious affiliation or sexual orientation.

One school of thought claims that privacy retards technical progress e.g. Electronic Medical Records (EMRs) invented in the 1970s which replaces paper records with computer files, had the potential to reduce annual cost by US$34 billion (Hillestad et al. 2005), but by 2005 only 41 percent of US hospitals had adopted it (Goldfarb and Tucker 2012). Miller and Tucker (2009, 2011) claims that state privacy regulations restricting the release of health information reduced EMR adoption by more than 24 percent and that a 10 percent increase in its adoption could reduce infant mortality by 16 deaths per 100,000 births. Another school of thought claims that the explicit protection of information makes adoption more likely, as without such protection people will be unwilling to use that technology.

Information collected by Governments can be very useful to researchers, however again there is the tension between the utility of such data and privacy concern. Edward Snowden's dumping of classified information in 2013 revealed the sort of data which intelligence agencies were collecting. This lead to a public outcry about privacy. Surveillance for national security and law enforcement purposes can conflict not only with civil liberties but also with economic interest – in 2015/16 there was a legal battle between the FBI and Apple Inc. concerning unlocking the security feature of an iPhone recovered from a shooter in an incident in which 22 persons were killed.

Privacy protection enhances the welfare of the person who share her data and society under some conditions while in other circumstances privacy protection can be deleterious to that person and others.■

Continues on page 34.

Consumer Protection in the Digital Age

Contributed by the **Consumer Affairs Commission**

According to United Nations Conference on Trade and Development (UNCTAD), developing countries account for 95 per cent of global Internet use with the highest growth rate in the least developed countries. In 2018, the milestone year, 51.2 per cent of the global population using the internet with 3.9 Billion consumers online.

In his address to The Digital Economy Report of the United Nations Conference on Trade, the UN Secretary General, Antonio Guterres described the occasion as an opportunity which examines the implications of growing cross-border data flows, especially for developing countries. The conference proposes to reframe and broaden the international policy debate with a view to building multilateral consensus[1].

In response, some of the richer economies have already undergone significant ground work in integrating social services, banking, production, logistics and supply chain management and all aspects of e-commerce. Other governments of developing countries, to some extent, are developing the prerequisites towards building out a digital economic plan which is being accelerated by the pandemic. With integrated online platforms new businesses have emerged, which offer economic operators along the supply chain and consumers numerous opportunities to reduce production time and mitigate risks often associated with traditional business protocols. However, the new digital frontier requires a more intense and robust integrated risk management system in order to reduce the potential harmful exposure to consumers.

Within the context of the theme, *"Intersection of Competition, Consumer Protection and Data Privacy Enforcement"*, the Consumer Affairs Commission (CAC) has over the years sought to balance its consumer protection portfolio with contemporary issues, among them data privacy and its enforcement. While the issue of enforcement is currently a challenge, the Commission actively educates consumers about the digital landscape so they can be informed and empowered to make informed decisions.

Data

Data is a very important asset whether from a business or consumer perspective. In the "old economy", data was used as a source of information to target consumer behaviour based on spends. In the "new economy" digital platforms utilise big data via search engines to track consumer behaviour online. This has therefore given rise to the Internet of Things (IoT). Evidence of this is seen in the increasingly and ubiquitous nature that technology is used to target consumers. This occurs through the ordinary things (such as televisions, phones, computers, etc.) that consumers use on a daily basis. It also gives rise to the issue of access and inclusion. Jamaica's banking institutions have put in place digital technology to facilitate their customers to conduct transactions outside of the banking hall. However, many seniors and technologically challenged individuals do not know how to use the technology nor do they have access. Therefore, this consumer segment has been placed in a vulnerable position[2].

The Internet of Things and Big Data

The reality is that as access to markets and opportunities become increasingly determined by algorithms, more and more data (Big Data) will

be demanded. The need to capture and mine this data has been aggressive and will no doubt intensify, especially as it relates to the areas of:

- Health - Registration and use of hospital clinics; treatment of diseases, medication, frequencies, etc.
- Technology - Smart phones, computers, laptops, televisions, automobiles, security systems (anything using technology)
- Financial - Banking, credit/debit cards (purchases), loans, investments, etc.
- Lifestyle - Shopping/purchases, subscriptions, survey/polls, entertainment, social media, etc.

Consumers must therefore be conscious of the fact that they are the owners of that data. Large online companies use their data and monetise the information without consumers being compensated. Therefore, they should demand mutual benefit, both in terms of what is currently happening as well as in the future.

In the past, the Commission has addressed these issues via its flagship event which is World Consumer Rights Day under various themes:

- 2014 Your Phone, Your Rights
- 2017 Empowering Consumers in the Digital Age
- 2018 Making Digital Marketplaces Fairer: Access, Security and Protection
- 2019 Become a Responsible Consumer: Empower Yourself

While there are legitimate concerns about the misuse of Big Data, the Consumer Affairs Commission is also a proponent of its use, especially as it relates to research purposes. The CAC was amongst the first Government agency to open up its price data for use to the public.

Data Privacy and E-Commerce Rights

The success of e-commerce is dependent on the active engagement of consumers and its future depends on their trust. According to Consumers International (CI) ***"Consumer Checklist for International Commerce Deal",*** one recommendation to address this situation is the establishment of an international agreement on cross border e-commerce which protects consumers and brings them real benefits. CI also notes that trade deals have the potential to deliver lower prices and greater choice to consumers and, in the case of e-commerce, measures to make it easier and safer for them to buy online.

It is against this background that similar requirements for purchasing from store front establishments must be enacted as it relates to e-commerce transactions[3].

There are existing issues regarding cross-border transactions. Specifically, consumers should have the opportunity to return a product and receive a refund if it has not been damaged. Therefore, access to fair and effective dispute resolution if something goes wrong after making a purchase online should also be a feature of this type of transaction. However, an official channel or agreement does not exist to facilitate redress except contacting the vendor. Until a cross-border complaints channel is officially established, the Consumer Affairs Commission recommends filing a complaint with the Better Business Bureau (BBB). The BBB accepts complaints if purchases have been made in the United States, Canada and Mexico.

Marketing to e-commerce consumers must also be guided by rules. Marketing and consumer reviews should be truthful and transparent. The needs of marginalised or vulnerable consumers and consumers with disabilities should be considered in website design and e-commerce processes such as payments and delivery. Larger fonts and acceptable colours should be used on small screens – often the only choice for low income consumers. In addition, responsible marketing, warnings and age verification should be used to protect vulnerable consumers. Furthermore, WC3 a web design and application site notes that ecommerce website should be designed to increase it's accessibility to the disabled user as much as possible.

Effective processes should be established for the exchange of information, conducting joint investigations, recalls and enforcement actions. Negotiations about e-commerce should be transparent and multi-stakeholder dialogue should be encouraged nationally and internationally. Negotiating proposals and consoli-

dated texts should also be made available to the public so that consumers know what is being negotiated on their behalf.

Jamaica's Data Protection Act 2020 is slated to take effect in 2022. Consistent with the EU guidelines on data privacy, the Act provides guidelines on how personal data should be collected, processed, stored, used and disclosed in physical or electronic form. It also requires that data should only be collected for specific lawful purposes with explicit consent of the individual, and not to be used in any way other than what it was intended.

The Act also states that data must not be transferred to a State or territory outside of Jamaica unless it ensures a sufficient and adequate level of protection of the individual rights from whom the data has been collected.

In its 2020 Report on the Digital Economy, UNCTAD's director of technology and logistics, Shamika N. Sirimanne, said that "the absence of a global data governance hinders countries ability to protect the privacy of people from both private sector and government use of data, and to address concerns related to law enforcement and national security"[4].

Through its implementation, it is expected that consumers will enjoy the same protection they have in physical markets as it relates to access, safety, information, redress, choice, privacy and representation. It is acknowledged that Jamaica's data protection laws will be in its infancy stage come 2022. Nonetheless, with the necessary cooperation among partners and stakeholders, Jamaica's consumers will be better empowered to protect themselves in the digital age.■

Endnotes

[1] https://unctad.org/system/files/official-document/ditccplp2021d2_en_0.pdf

[2] https://unctad.org/system/files/official-document/der2019_en.pdf

[3] https://www.consumersinternational.org/media/155222/consumerchecklistforinternationale-commercedeal.pdf

CYBERLAW & COMPETITION

A look at the challenges posed by Mega ICT Companies

By **Nicole Foga** | Attorney-at-Law | Managing Partner, Foga Daley

Cyberlaw focuses on the issues and challenges that arise from the use of the Internet and the legal relationships that are formed in the so called "Cyberspace". Essentially, cyberlaw is the law of the Internet and while cyberlaw is sometimes considered something akin to science fiction, it is an area grounded in standard legal principles that are adapted for application in a digital environment. From a civil law perspective, it encompasses contract law through electronic commerce, intellectual property law through digital rights, defamation through online publications, particularly over social media, international law through its multi-jurisdictional digital platforms, but also includes data privacy and protection and competition law, the subject of this article.

At first blush competition law and cyberlaw appear to be two disparate areas of law but upon closer examination, it becomes clear that given societies' increasing reliance on the Internet and its underlying Information and Communication Technologies (ICTs), the two areas of law now routinely intersect.

There were 4.8 Billion active internet users worldwide in July, 2021 (i.e., approximately 60% of the world's total population) and of this total, 92.1% of the users accessed the Internet via mobile devices[1].The total number of social media users in July 2021 was recorded as 4.48 Billion persons, approximately 57% of the global population[2]. Given the sheer volume of internet users it is inevitable that competition issues will arise.

It is well accepted that competition spurs innovation, efficiency, and creativity. ICT companies are often at the forefront of innovation and investment, particularly at this time in the 21st century when, due in no small way to the current pandemic, countries are being transformed into digital economies at an accelerated pace. It is noteworthy that seven (7) of the top ten (10) largest companies in the world, based on market capitalization, are either technology companies or companies which rely on digital service delivery[3]. The largest company in the world with a market capitalization of US$2.1Trillion is Apple Inc., while Microsoft Corp, with a market capitalization of US$1.8Trillion is the third largest company in the world. Amazon.com Inc with a market capitalization of US$1.6 Trillion and Facebook Inc with a market capitalization of US$839 Billion are respectively the 4th and 6th largest companies in the world.

An interesting paradox is the fact that innovative ICT companies rely heavily on their patents, trademarks and branding, all forms of intellectual property, which grant their creators / owners sensitive monopolies to develop their products. A question for consideration is: At what point are the monopolies granted to ICT companies in the form of Intellectual Properties Rights (IPRs) no longer an incentive to innovation, but rather a means to bar new entrants into a market? In the first quarter of 2021, Amazon reported 200 million paying Prime members worldwide and in June 2021 it had over 2.7 billion combined desktop and mobile visits[4]. Facebook had approximately 2.89 Billion monthly

active users as of the second quarter of 2021 and is the biggest social network worldwide[5]. Given the size and market volume of these mega jurisdictional companies and the increasing dependence of the world's population on their products and digital services, one wonders how best they can be monitored and regulated against anti-competitive practices. These are some of the issues which are being grappled with by competition regulators all over the world.

This article now focuses on the response of the European Commission (EC) which has been extremely proactive as a competition regulator, particularly in regulating online companies. For example, in 2020 the EC brought actions against two of the top ICT Firms. By press release of 16 June 2020, the EC announced that it had opened formal anti-trust investigations against Apple to determine whether Apple's rules for application developers on the distribution of applications via the Apple App Store violate EU competition rules. It was stated that:

> *"The investigations concern in particular the mandatory use of Apple's own proprietary in-app purchase system and restrictions on the ability of developers to inform iPhone and iPad users of alternative cheaper purchasing possibilities outside of apps.*
>
> *The investigations concern the application of these rules to all apps, which compete with Apple's own apps and services in the European Economic Area (EEA). The investigations follow-up on separate complaints by Spotify and by an e-book/audiobook distributor on the impact of the App Store rules on competition in* ***music streaming*** *and* ***e-books/ audiobooks****."*

A formal antitrust action was initiated in November 2020 by the EC against Amazon for distorting competition in online retail market. In its 10 November 2020, press release on the matter, the EC stated:

> *"The Commission takes issue with Amazon systematically relying on non-public business data of independent sellers who sell on its marketplace, to the benefit of Amazon's own retail business, which directly competes with those third party sellers.*
>
> *The Commission also opened a second formal anti-trust investigation into the possible preferential treatment of Amazon's own retail offers and those of marketplace sellers that use Amazon's logistics and delivery services."*

In April 2021, the EC came to the preliminary conclusion that Apple had "abused its dominant position for the distribution of music streaming apps through its App Store and distorted competition in the music streaming market". On April 30, 2021, the Executive Vice-President of the EC issued a statement noting that:

> *"There has been an exponential growth of the number of apps but there are essentially two main app stores: Apple's App Store and the Google Play Store. Both of them provide access to millions of apps developed by hundreds of thousands of developers. Apple's App Store specifically hosts more than 1.8 million apps…*
>
> *Apple devices are used by millions of Europeans. And users are very loyal. They don't switch easily. For example, owners of an Apple device are not likely to switch to another device with Google Play Store just because music streaming is more expensive on the Apple App Store. So Google Play Store is not an effective alternative to reach the millions of Apple device owners that can only use the Apple App Store to buy their apps. To reach Apple users, music streaming providers have to go via the Apple App Store and accept the rules Apple imposes on them.*
>
> *Our preliminary finding is that Apple exercises considerable market power in the distribution of music streaming apps to owners of Apple devices. On that market, Apple has a monopoly. The company not only controls the only access to apps on Apple devices. It also offers a music streaming service, Apple Music that competes with other apps available in the Apple App Store, such as Spotify or Deezer….*
>
> ***Competition intervention in digital markets must***

be sufficiently timely to have an impact. It is reassuring that music streaming services competing with Apple Music continue to operate still today. But we are also seeing clear signs that Apple's conditions in its App Store affects their business development. *" (My emphasis)*

As recently as 4 June 2021, the EC announced that it had launched an investigation into Facebook to determine whether, "*Facebook violated EU competition rules by using advertising data gathered in particular from advertisers in order to compete with them in markets where Facebook is active such as classified ads. The formal investigation will also assess whether Facebook ties its online classified ads service "Facebook Marketplace" to its social network, in breach of EU competition rules."*

The actions of the EC are quite instructive and any successes obtained may act as a roadmap for competition regulators worldwide. Of course, for small island states like Jamaica with limited resources, the fact that these companies are all incorporated and based overseas can act as a real barrier for investigation and enforcement actions by competition authorities with little to no extraterritorial jurisdiction. Nevertheless, it is timely for us to re-examine our own competition laws to see how they may be better strengthened and adapted to address the legal and regulatory challenges of cyberspace and the pervasiveness of mega digital platforms.■

Endnotes

[1] https://datareportal.com/global-digital-overview

[2] https://datareportal.com/social-media-users

[3] Ranked: The Biggest Companies in the World in 2021 (visualcapitalist.com)

[4] https://www.statista.com/statistics/829113/number-of-paying-amazon-prime-members/

[5] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

The Adequacy of the Data Protection Act 2020 for MSME's

tTech highlights the Cybersecurity measures that MSMEs need to consider

By **Christopher Reckord** | Chief Executive Officer | tTech Limited

For decades, smart and highly resourceful organizations have been leveraging personal data of either their customers, prospective customers and other personal data in general for a wide range of profitable uses. The advent of the internet and a vast slew of sophisticated digital technological advancements has increased the collection and use of personally identifiable information exponentially. Personal data means any information whether by itself or together with other information which can be used to identify an individual.

Jamaica's Data Protection Act 2020 seeks to protect the personal and private information of Jamaicans. In summary, this law covers how (a) personal data is obtained (b) how this data can be processed (c) personal data can be used for (d) the collected data is to be accurate and kept up to date (e) that the personal data not be kept for longer than is necessary for the purpose (f) that personal data is processed in accordance with the rights of the customer (data subject) (g) personal data must be protected using appropriate technical and organizational measures and finally (h) where the data can be stored and transferred to.

There have been valid concerns raised related to the impact that this law might have on micro, small and medium enterprises (MSME) which is why we have played our part to assist in highlighting the Cybersecurity measures that those MSMEs that process personal data need to consider in order to be compliant with the technical measures stipulated in the seventh standard in the law. The law states:

"*The seventh standard is that appropriate technical and organisational measures shall be taken — (a) against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*; … "

A simplified outline of the roadmap to a secure environment

Here is my high level 5-point strategy that, if fully implemented, can reduce the risk of cybersecurity breaches by 85%. I had some fun with the heading of each area to keep it engaging.

Take Stock – Document all the IT hardware and software you own, where they are and who has access them. Ensure that all the soft-

ware that you use is legally yours to use.

Lock Shop – Enable the most secure configuration of the software and devices that you have. Remove all default passwords from the hardware and software you own. Implement multifactor authentication for access to sensitive data. Encrypt your data while at rest and in transit. Secure your internet & Wifi with the aid of VPNs and firewalls.

Use Plenty Protection - Anti-malware software should be installed to protect your computers, important data and to protect the privacy of your customers data. Have at least 3 backups of important data (2 local and 1 remote) Traditional antivirus on its own cannot provide adequate protection, more is required. Endpoint detection and response (EDR) is the most advanced endpoint protection with a wide range of capabilities including the collection, correlation, and analysis of endpoint data, as well as coordinating alerts and responses to immediate threats. EDR not only includes antivirus, but it also contains many security tools like firewall, whitelisting tools, monitoring tools, etc. to provide comprehensive protection against digital threats.

Patch it - Operating systems, IT Appliances and other important IT assets should be regularly updated to fix known vulnerabilities. Cybercrime is now a multibillion dollar global business and they are always looking for bugs, holes and vulnerabilities in every bit of technology that we use. We must patch up these holes. From an individual user level, too many of us receive notifications for updates and we either just ignore them or click "Do it later".

Be Aware, Be VERY aware – The human factor is massively important and is often the weakest link. Train all users and train them often on data security, email attacks and your policies and procedures. IT Security professionals consider Security Awareness Training as the most effective protection from ransomware. Because the criminals are continually trying to make employees click on malicious links or open up infected attachments, an important part of the training is showing users what these phishing emails and what these links look like.

The World Economic Forum's Global Risk Report for 2021 placed cybersecurity failure among the greatest threats facing humanity within the next ten years. Let that sink it. Are you prepared? ■

BGLC
BETTING GAMING & LOTTERIES COMMISSION

Ensuring the integrity, accountability, compliance, propriety and sustainability of Jamaica's gambling industry.

The Betting Gaming & Lotteries Commission safeguards the interests of gambling industry operators, players, the general public and government.

BGLC Regulates:

- **Betting** – **Bookmakers** (Betting Lounges, Licensed Betting Offices, Sports Betting Sales Outlets, Betting Agents, Bet Writers, Terminal Operators)
  - **Racing Promoters** (Off Track Betting Parlour, Off Track Betting Parlour Operator, Racing Promoter Terminal Operator)
- **Gaming** – **Gaming Machine Operators** (Gaming Lounges [Slot Machines], Non-Gaming Lounges [Operators of locally manufactured machines or Local & Slot Machines], Technical Service Providers [TSPs], Operators of Prescribed Premises, Prescribed Workers)
- **Lotteries** – Lottery Promoters, Lottery Agents, Lottery Sales Outlets
- **Prize Competitions**
- **Charitable Lotteries** – Raffles, Bingos

Betting, Gaming & Lotteries Commission
78CEF Hagley Park Road, Kingston 10 | Tel: (876) 630-1353 | WhatsApp: (876) 224-2452 | Email: info@bglc.gov.jm | Web: www.bglc.gov.jm

#GameResponsibly @BGLComm @bglcja @BGLCJamaica YouTube #Responsible Gaming

THE IMPORTANCE OF DATA PROTECTION IN THE INSURANCE INDUSTRY

Contributed by the **Financial Services Commission**

A cyber-attack can be defined as where one tries to gain unauthorized access to an Information Technology (IT) system for the purpose of theft, extortion, disruption or other nefarious reasons. It has been reported by a number of international credible news agencies and publishers that the year 2020 exceeded all previous records concerning (i) the loss of data arising from breaches into a company's computer system, (ii) the level of sophistication (as demonstrated by the use of emerging technologies such as machine learning, artificial intelligence, and 5G) and (iii) the numbers of cyber-attacks on companies, government, and individuals. It has been estimated that, in America, every eight (8) minutes there is a cyber-attack. It is also well documented that with many persons relying on the internet for work, school, church, shopping, banking, and to be in touch with loved ones and friends, cyber-crime activities have increased.

The victims of these attacks vary and span the cross section of organisations and businesses including universities, hospitals, IT firms, meat manufacturer, a gas pipeline company and even insurance companies. Some notable examples of insurance companies affected in 2021 are;

- Geico, America's second-largest auto insurer was attacked by cybercriminals. This breach went on for couple months,
- CAN Financial Corporation, one of America's largest insurance companies experienced the theft of its data and the loss of control of its network after a ransomware[1] attack, and
- Tokio Marine Insurance Singapore, a subsidiary of Tokio Marine Group announced it was hit by a ransomware attack.

While the above examples include ransomware attack, there are many other forms of cybercrime. Insurance companies, by the nature of their business, collect and store a huge amount of personal data, which is needed by these companies to provide their financial consumer with the appropriate policies and price. This reservoir of data held by insurance companies includes information relating to the policyholders' identification, health, finances, employment, academics and physical assets. It is this wealth of data that make insurance companies an attractive target for cyber-attacks.

Any type of data breach at an insurance company can be devastating to the company as a successful cyber-attack can erode the policyholders' confidence in the company and damage its reputation and erase its profitability. A data breach can also result in an increase of insurance fraud. Given that data processing is extremely critical to an insurance company's key operations such as acquiring and pricing a new policyholder as well as settling claims, investment in a data protection system, which is appropriate to the company's size, risks and complexity, is essential and must not be delayed.

The tenet of data confidentiality and protection has been one of the bedrocks of the Financial Services Commission (FSC) since its formation in 2001 and the financial industries that the FSC regulates. Section 15 of the Financial

[1] Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid.

The tenet of data confidentiality and protection has been one of the bedrocks of the Financial Services Commission

Services Commission Act mandates every staff member of the FSC to regard and deal as secret and confidential all information relating to insurance companies and the other FSC-regulated entities. Additionally, it is an offence for any staff to not comply with this requirement and he / she could be imprisoned. As a member of the International Association of Insurance Supervisors (IAIS) the FSC adheres to international standards and best practices. As a result, the FSC, among others, has implemented the following:

- Third parties acting on the behalf of the FSC (presently or in the past), are required by legislation to protect confidential information in the FSC's possession,
- Policies and procedures for information sharing with other financial regulators, and
- Insurers and insurance intermediaries must have policies and processes for the protection and use of information on customers.

While in Jamaica, there has been no notable cybercrime involving an insurance company, neither the FSC nor the insurance companies can become complacent. The FSC recently issued its ***Concept Paper for Proposed Legislative Amendments to Strengthen Market Conduct Requirements for Insurance Companies & Intermediaries to Safeguard against Unfair Trade Practices.*** This paper includes requirements that will strengthen the protection and the privacy of information obtained from all customers. The legislative process to amend the Insurance Act has begun and when completed, insurance companies and intermediaries will be mandated to comply with, but are not limited to, the following:

- There must be policies and procedures which include provisions that stress the importance of the appropriate use and the privacy of personal data of customers,
- Appropriate technology must be in place to adequately manage and protect the confidentiality of personal and other information that the insurer and intermediary hold on customers;
- Suitable records management systems and controls are acquired and employed to fulfil adequately these regulatory and statutory obligations, and
- The maintenance and safe-keeping of records must be in such a manner as to restrict inappropriate access, while ensuring confidentiality.

In addition to the above-mentioned proposed legislative amendment to the Insurance Act 2001, the Data Protection Act was passed by the Jamaica Parliament in May 2020 and is scheduled to be in effect in 2022. The act seeks to safeguard the privacy and personal information of Jamaicans. The Data Protection Act provides guidelines on how personal data should be collected, processed, stored, used and disclosed in physical or electronic form. Insurance companies will have to comply with this Act. Section 129 of the Insurance Act 2001 requires that every local insurance policy complies with the laws of Jamaica.

Given (i) the significance of data and the processing of such data to insurance companies, and (ii) the increasing number and sophistication of cyber-attack, insurance companies must recognise their need to establish policies, procedures and mechanisms to protect the IT systems; confidentiality of data belonging to their policyholders and beneficiaries, and electronic communications between the companies and its customers.

In order to maintain their reputation, profitability and the trust of their clients, insurance companies and intermediaries must pursue and implement robust data protection policies and procedures and endeavour to more than satisfy the requirements mandated by the various legislation as well as those stipulated by the FSC.■

Protecting Intellectual Property in the Digital Age

By **Lilyclaire Bellamy** | Executive Director | Jamaica Intellectual Property Office

The issue of protection in the digital age, touches and concerns all aspects of our lives, the ubiquitous chip has made protection an important priority for everyone.

The concept of protection is one of the core considerations in two of the most well know intellectual property law conventions. These two conventions provide the requirements that form the foundation and core of the intellectual property laws in not only Jamaica, but globally. They are the Paris Convention for the Protection of Industrial Property (1883) and the Berne Convention for the Protection of Literary and Artistic Works (1886)

"The Paris Convention applies to industrial property in the widest sense including patents, trademarks, industrial designs, utility models (a kind of 'small-scale patent' provided by the law of some countries), service marks, trade names (designations under which an industrial or commercial activity is carried out), geographical indications (indications of source and appellations of origin) and the repression of unfair competition."[1]

The Paris Convention is given expression in the Industrial Property laws of Jamaica, including but not limited to the Trade Marks Act, and the Patents and Designs Acts.

"The Berne Convention speaks to the protection of literary and artistic works and the rights of the authors. The Convention is based on three basic principles and contains a series of provisions determining the minimum protection to be granted, these include:

- "national treatment", meaning that the same level of protection that we offer in Jamaica has to be granted to others who are parties to the Convention
- "automatic protection", meaning that there is no need to do anything formal, once the work has been created the protection begins;
- protection being granted even if not protected in the country where the work originated.

(a) protection must include "every production in the literary, scientific and artistic domain, whatever the mode or form of its expression" (Article 2(1) of the Convention).

(b) the author has certain exclusive rights including but not limited to: the right to make adaptations; the right to perform in public; and the right to make reproductions, are a few of the rights that are granted."[2]

"Moral rights" are also an important aspect of the Berne Convention and the need for at least fifty years of protection are the major provisions of the Convention, all aspects of which are captured in Jamaica's Copyright Act.

The Paris and the Berne Conventions encapsulate the basic protection mechanisms for intellectual property but there have been significant changes to how we operate and do business since the 1800s and it is no doubt this recognition of the changes that signaled the need for what is commonly referred to as the 'WIPO Internet Treaties'. These are the WIPO Copyright Treaty (WCT) (1996) and the WIPO Performances and Phonograms Treaty (WPPT) (1996).

According to WIPO, "the WCT, is a special agreement un-

der the Berne Convention which deals with the protection of works and the rights of their authors in the digital environment. In addition to the rights recognised by the Berne Convention, the WCT grants certain economic rights, recognises, and addresses the issue of computer programs and the protection of databases, both of which are entitled to protection under copyright."[3]

The WCT basically, it could be argued, expands on the provisions of the Berne Convention and makes it more relevant to the 21st Century. The other internet treaty the WIPO Performances and Phonograms Treaty (WPPT) 1996, focuses on the rights of performers and producers in the digital environment. WIPO summaries the treaty in the following way:

"*The WIPO Performances and Phonograms Treaty (WPPT), deals with the rights of two kinds of beneficiaries, particularly in the digital environment:* ***(i)*** *performers (actors, singers, musicians, etc.); and* ***(ii)*** *producers of phonograms (persons or legal entities that take the initiative and have the responsibility for the fixation of sounds). These rights are addressed in the same instrument, because most of the rights granted by the Treaty to performers are rights connected to their fixed, purely* ***aural performances*** *(which are the subject matter of phonograms).*

As far as ***performers*** *are concerned, the Treaty grants performers* ***economic rights*** *in their performances* ***fixed in phonograms*** *(not in audiovisual fixations, such as motion pictures):* ***(i)*** *the right of reproduction;* ***(ii)*** *the right of distribution;* ***(iii)*** *the right of rental; and* ***(iv)*** *the right of making available."*[4]

Recent amendments to the suite of intellectual property laws in Jamaica and the intention to accede to additional WIPO administered intellectual property conventions has signaled the recognition and importance of intellectual property in providing for a 'safe space' within which to operate and do business in Jamaica. Each of the IP laws includes a component that recognises the need for enforcement and so there are penalties for breaches of all the IP laws this seeks to encourage the recognition and protection of the works of all creatives

The laws are important and include not only protection clauses but also enforcement clauses.

Responsibility is at the feet of the owner to protect the exclusive rights granted to them under intellectual property laws and therefore, enforcement is necessary as this signals to offenders that there are consequences for breach of these rights.

It should also be noted that the under the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), additional rights are provided for creators of intellectual property rights, which are significant as it affects all the members of the World Trade Organizations (WTO) and basically adds to the existing IP treaties, so even if you are not a member, the TRIPS Agreement still provides obligations that you need to meet.

But you may be wondering of what relevance are all these WIPO conventions? The reality for us here in Jamaica and for the member states of WIPO, the provisions of these treaties which have been subsequently enacted into law is that it secures certain rights and privileges which we are all able to benefit from.

In closing it would be fair to say that intellectual property is protected in the digital age and this protection continues and is still evolving to address new trends and developments.■

Endnotes

[1] Summaries of Conventions, Treaties and Agreements Administered by WIPO 2013, Summary of the Paris Convention for the Protection of Industrial Property (1883) page 8

[2] https://www.wipo.int/treaties/en/ip/berne/summary_berne.html

[3] https://www.wipo.int/treaties/en/ip/wct/summary_wct.html

[4] https://www.wipo.int/treaties/en/ip/wppt/summary_wppt.html

Continued from page 20: **The Economics of Privacy**

Bibliography

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. 2016 "The Economics of Privacy." Journal of Economic Literature, 54(2), 442–492

Aite Group, March 2021 Report: "U.S. Identity Theft: The Stark Reality", Boston

Dugas, Andrea Freyer, et al. 2012. "Google Flu Trends: Correlation with Emergency Department Influenza Rates and Crowding Metrics." Clinical Infectious Diseases 54 (4): 463–69.

Edelman, Benjamin, and Michael Luca. 2014. "Digital Discrimination: The Case of Airbnb.com." Harvard Business School, Negotiation, Organizations & Markets Unit Working Paper 14-054.

Goldfarb, Avi, and Catherine E. Tucker. 2012. "Privacy and Innovation." Innovation Policy and the Economy 12 (1): 65–90.

Goldin, Claudia, and Cecilia Rouse. 2000. "Orchestrating Impartiality: The Impact of 'Blind' Auditions on Female Musicians." American Economic Review 90 (4): 715–41

Hillestad, Richard, et al. 2005. "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs." Health Affairs 24 (5): 1103–17.

Mikians, Jakub, Laszlo Gyarmati, Vijay Erramilli, and Nikolaos Laoutaris. 2013. "Crowd-Assisted Search for Price Discrimination in e-Commerce: First Results." In Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies, 1–6. New York: Association for Computing Machinery

Miller, Amalia R., and Catherine E. Tucker. 2009. "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records." Management Science

Miller, Amalia R., and Catherine E. Tucker. 2011. "Can Health Care Information Technology Save Babies?" Journal of Political Economy 119 (2): 289–324.

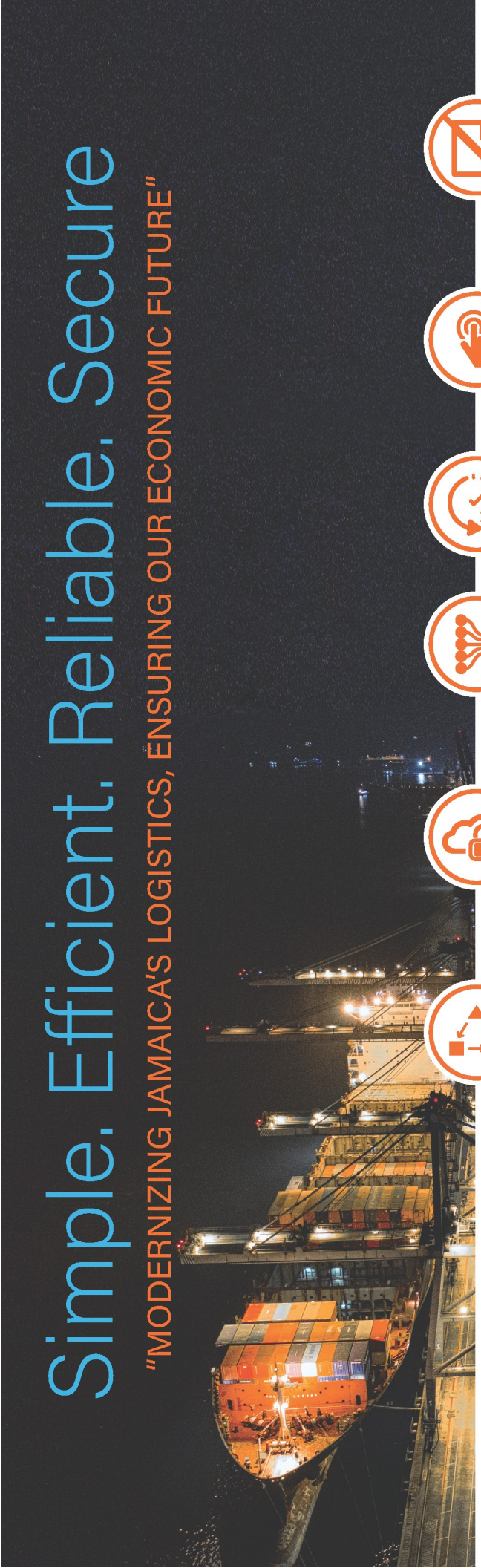
Posner, Richard A. 1981. "The Economics of Privacy." American Economic Review 71 (2): 405–09.

Strahilevitz, Lior Jacob. 2008. "Privacy versus Antidiscrimination." University of Chicago Law Review 75 (1): 363–81.

White, Ryen W., Nicholas P. Tatonetti, Nigam H. Shah, Russ B. Altman, and Eric Horvitz. 2013. "Web-Scale Pharmacovigilance: Listening to Signals from the Crowd." Journal of the American Medical Informatics Association 20: 404–08.

Simple. Efficient. Reliable. Secure

"MODERNIZING JAMAICA'S LOGISTICS, ENSURING OUR ECONOMIC FUTURE"



Key Features:

Paperless Environment

Our aim is to remove as much paper as possible across the port community's logistics processes. This will yield significant cost savings in addition to security and efficiency improvements for all involved.

Accessibility

The system is accessible anytime and anywhere. All you need is an Internet connected device and putting the user/s in charge of where and when they access the application.

High Availability

The PCS utilizes best-in-class technology to ensure that the system is running and is also accessible 24/7/265

Streamlines Processes

Representatives of various organizations from across the port community have been collaborating to review and redefine the industry's many business processes and ensured the most efficient process is applied industry-wide.

Data Security

The PCS utilizes best-in-class intelligent security tactics to collect, store and transmit the industry's data, while protecting it from security breaches of various types and origins.

Interoperability

The major benefit of the PCS is allowing all industry stakeholders to share information electronically, providing outstanding benefits which include drastic productivity increases, reduced paper-pushing efforts and errors, in addition to slashed transportation costs.

Pcs_support@portjam.com
https://www.facebook.com/JamaicaPCS/
https://twitter.com/jamaicapcs
https://www.instagram.com/jamaicapcs/

JAMAICAPCS

YOUR FUTURE LOOKS GREAT!

Spectrum MANAGEMENT AUTHORITY

LEARN MORE AT:

WWW.SMA.GOV.JM/

We're Social

smagovjm

smaja.

SHAPING YOUR FUTURE WITH WIRELESS...

BAND PLANNING AND FREQUENCY ALLOCATION

MONITORING OF THE SPECTRUM AND INSPECTION OF FACILITIES

LICENCING MANAGEMENT

ENFORCEMENT

INTERFERENCE MANAGEMENT

AN AGENCY OF THE MINISTRY OF SCIENCE ENERGY AND TECHNOLOGY

...fuelling growth