Presentation by
Cordel Green
Executive Director of
the Broadcasting Commission - Jamaica
At

The Advertising and Marketing Law Conference
1st March 2018
Kingston

"The Digital Economy & Society: Emerging Issues for the Future Regulation of Content and Broadcasting Across Networks, Platforms and Devices"

(These views are not necessarily those of the Broadcasting Commission)

1. “CONNECTIVITY IS THE HANDMAIDEN OF OF ADVERTISING”

- I begin with the observation that Connectivity is the most transformational revolution in this century as electricity was in the last and railroad in the previous (McKinsey).

- All the devices we carry and those at home and work are connecting seamlessly (phones, ipads, ipods, wearable devices, screens, thermostats, DVRs, computers, cars etc.). And they will increasingly provide seemingly prescient service.

    - Example: an app will search your communication history to find out where you are; use GPS to confirm your location; use Google Maps to check traffic conditions, predict that you want to dine out, push restaurants in close location to your phone, choose a restaurant for you, work out the best driving route to the restaurant of your choice, and notify you when to leave should you want to get ahead of traffic.

- Citizens are accessing news, information, entertainment, education, geo-location/directions, home management and shopping, translations and many other services on and across multiple screens and devices, unfettered by platforms as technologies converge and interoperability becomes the norm.

- The technology companies (Google and YouTube, Netflix, Amazon, Apple etc.) are becoming the dominant providers of content. They now dwarf most of the traditional media companies. They control the “places” on the Internet where we gather and connect, without having any local presence or the need to own any infrastructure; and they are not subject to the same or any regulation as traditional media.

2. THE INFORMATION AGE IS "THE ERA OF MASS SURVEILLANCE"

- My second point is that we are living in the era of mass surveillance.

- The digital society is about free expression and the sharing of information. This increasingly involves the disclosure, collection, storage and monetization of personal data.

- The question now is who controls your data and what is it being used for?

- At a recent talk at the Harvard Kennedy School, Jim Waldo, the chap who invented JAVA, provided some insights:

    1. Everything is online. It's a rich data set for marketers who want to target a specific demographic.

    2. We can all be identified all the time we are on the internet (cookies, IP address, browsers).

    3. Fonts that are in the font cache can identify 90% of computers in the world (I did not know that!).

    4. The apps on your smartphone track you.

- Bruce Schneier, one of the world's foremost security experts"(Wired), tells us in his very insightful book, "Data and Goliath":

> "Your cell phone provider knows your location; vendors record your purchasing patterns; your email, texts, and social network activity are stored indefinitely; and all this information is used by [corporations] to manipulate, discriminate, and censor your experiences."

- Location data is being gathered by corporations such as Verve, the global leader in location-powered mobile marketing.

- Verve advertises its core business as :

> *'the ability to profile devices to turn disparate data signals into actionable insights which in turn inform highly refined audience segments. Equally important is the capacity to contextualize behavioral insights with place data to drive personalized recommendations for promotions and coupons.'*

- This is Code for using the location data from phones to 'build personal profiles of each of us'!!!! (See : https://www.prnewswire.com/news-releases/verve-completes-acquisition-of-sense-networks-software-and-intellectual-property-assets-from-yp-llc-300485998.html)

- And, it is becoming easier to extract location data:

- Bluetooth constantly broadcasts "Hi, I am here, and here is my phone ID number" and we are tracked using that broadcast.

- In a recent talk, Bruce Schneier claimed that advertisers are buying IMS trackers on Alibaba which they use to get onto mobile phones to push advertisements.
- Stingray is an example of an IMS tracker).[1] It was designed for the FBI and other law enforcement agencies. It is a device which mimics a

[1] It extracts the International Mobile Subscriber Identity, or IMSI, number, which each phone with a SIM card presents to a cell tower upon first connection. (see https://www.tomsguide.com/us/cellphone-tracker-stingray,news-21718.html)

wireless carrier cell tower in order to force all nearby mobile phones to connect to it. This is the technology that advertisers are using to push ads to our phones.

- Schneier has also written that Verizon, Microsoft, and others are working on a set-top box that can monitor what's going on in a room, and serve ads based on that information." (Schneier p.56).
    - If there is nothing going on in your bedroom, there is nothing to fear. But, if there is lot of action, that's going to generate a lot of ads.
- We regulate how much advertising can interrupt a programme on TV. Now, we have to figure out how to regulate the number of ads that interrupt action in the bedroom!
    - And what if you are watching TV in the bathroom? What ads will pop up? ("Not washing your arms properly? Use "Arm Attack...it washes your arm even after you are done showering!").

3. Data Collection Vis-à-vis Data Correlation

- Radio and TV operators have always collected general demographic information which is used to determine the price for advertising in programmes at different time bands throughout the day.

- But, in the digital world, we are tracked in real time and the data is used to "build personal profiles of each of us." (Schneier, pp. 2-3).

- So, we have gutted the traditional media advertising model and replaced it with a personal and intrusive advertising model.

- Despite the intrusion, some people are only concerned if the data collected is identifiable. This is a mistake! Anonymized data is beguilingly innocuous. Technology now makes it possible to de-anonymize information easily. And by correlating data, an accurate picture can be established about anyone.

- Stanford computer scientists have revealed just how possible it is to identify a person's private information using only metadata – (See https://news.stanford.edu/2016/05/16/stanford-computer-scientists-show-telephone-metadata-can-reveal-surprisingly-sensitive-personal-information/. See also Schneier, pp. 24-25).

- A 2016 Stanford analysis revealed that:

    - Person A communicated with multiple local neurology groups, a specialty pharmacy, a rare condition management service, and

a hotline for a pharmaceutical used solely to treat relapsing multiple sclerosis.

- Person B spoke at length with cardiologists, talked with a medical lab, received calls from a pharmacy, and placed calls to a hotline for a medical device used to monitor a cardiac condition.

- Person C placed a long early morning call to her sister; two days later she made several calls to an abortion clinic. She made brief calls to the abortion clinic two weeks later, and then made a final call a month after.

- This would be valuable information for anyone who is advertising nutraceutical products, home care service, healing service, Palm Reading service or anyone running a foster care and adoption service.

- When the Internet of All Things and Artificial Intelligence (AI) really kick in - and our smart cars, smart refrigerators, smart stoves, smart beds and smart toilets start to get in on the action of generating “big data” - we might as well be all walking naked!!!!!!

4. The Price of "Connectivity"

- It has become clear that we are paying a hefty price for the benefits of connectivity.

- Our email, operating systems, online search engines, browsers and many apps are ostensibly "free".

- And to keep it that way, Internet Giants and Dwarfs must know our friends, what we say to them, what they say to us, the sites we visit, what we do online, where we are and more.

- But the bargain of surveillance in exchange for free service is unfair.

    - In an interview, former Google CEO, Eric Schmidt, said:

      "With your permission, you give us more information about you, about your friends...We know where you are. We know where you've been. We can more or less know what you're thinking about." (http://www.businessinsider.com/eric-schmidt-we-know-where-you-are-we-know-where-youve-been-we-can-more-or-less-know-what-youre-thinking-about-2010-10).

    - That statement is a distortion of "permission".

- Researchers at Carnegie Mellon University found that the average privacy policy is 2500 words and takes on average 10 minutes to read. (Out-Law.com).

- The majority of internet users do not read privacy policies before agreeing to them, and have little or no idea what the policies actually mean. (Morran, Dachis). Take Pokémon Go, as an example:

Pokémon Go Privacy Policy as at July 1, 2016

Collection and Use of Information

Our servers automatically record a User's IP address…browser type, operating system, the web page visited before accessing our Services, the pages or features of our Services which a User browsed, time spent on those pages or features, search terms, the links that a User clicked on, **and other statistics.**

Information that we collect from our users is considered to be a **business asset**.

We may disclose any information about you…to **government or law enforcement officials or private parties** as we, **in our sole discretion**, believe necessary or appropriate...

Following termination or deactivation of your…Account, Niantic, its clients, affiliates, or service providers may retain your information...and user content **for a commercially reasonable time period…**

- Adapting Lord Denning's 'Big Red Hand Test', such privacy clauses would need to be printed in red ink, with a red hand marked "danger" pointing at each line, before they could be held to be sufficient (*Spurling v Bradshaw [1956] EWCA Civ 3*).

5. Monetisation of Personal Information

- Yet, with the intrusion, comes a counter-intuitive response. There are signs that the public is changing its attitude towards the protection of personal information.

- In a March 2016 Intel study, the majority of respondents worldwide (54 percent) indicated a willingness to share their personal data in exchange for money.

- It seems everyone is waking up to the reality that personal data is the 'oil of the twenty-first century'.

- But, it appears there is a wide gap between enterprise valuation of personal data and individual valuation.

- Internet services such as Google and Facebook use the personal data of users not only to customise their experience but for targeted advertising which contributes upwards of 80% of their revenue.

- Google's advertising revenue was US$67 billion in 2015 (http://www.statista.com/statistics/266249/advertising-revenue-of-google/). Facebook's was approximately $18 billion in 2015, a 44% increase over the previous year.(https://techcrunch.com/2016/01/27/facebook-earnings-q4-2015/).

- The advertising revenues per user (ARPU) for Google was $45 on average , in 2014 (See http://www.statista.com/statistics/306570/google-annualized-advertising-arpu/) and for Facebook it was approximately $12 in

2015 (an increase from $9.45 in 2014)
(http://www.statista.com/statistics/234056/facebooks-average-advertising-revenue-per-user/).

- Compare this to how people value their personal information. In 2010 a study in Korea found that Korean nationals over the age of 18 were willing to accept between US$500 and US$1500 as the equivalent to the value of their personal information.

- Clearly, there is a wide gap between users' expectation of value and the per user value to corporations.

- A point to note, is that the dominant model of data collection without any monetary benefit is set to be disrupted.

- Companies already exist, such as Datacoup, which offer aggregated data to advertisers and pay users for their personal data in proportion to the demands of advertisers.

- This raises the interesting policy question whether personal information should be treated as property.

    - The law recognizes the distinct tort of misappropriation of personality but this is limited to the commercial value of the image and likeness of celebrities. But are regular people not now celebrities who amass legions of "followers," "friends" and "fans" in twitter-land, Facebook, Instagram and other social media?

- It is therefore not an unreasonable proposition that in a world where there is increasing commercial value in information about ordinary persons, and "…a strong tendency to 'propertize' everything in the realm of information", ordinary people should be assigned a property right in personal information about themselves (Lessig).

- Blockchain, the technology behind bitcoin is a candidate for empowering individuals to monetize personal data, using smart contracts. Block chain will makes it possible for:

  - A shift from silos of data to treatment of each data item as an actual unit of value. [See "Data Item Pair" (DIP) disclosed in patent application USPTO 8862506, which defines the smallest necessary and sufficient unit of tradeable data].

  - So, the individual will be able to monetize the precise data that she wishes to sell or the data buyer wishes to purchase.

- But we will have to proceed cautiously because the commodification of personal information can work against the consumer's interest:

  - Each of us has a customer score which has been assigned to us by data brokers, based on a range of factors including online purchases, social media interactions, survey data, personal financial information etc. Our score card influences the ads that we are allowed to see as we browse the Internet" (Schneier, 130).

- So, we are all at risk of profile-based advertising and profile-based business decisions. Our own personal data will be used against us to predict our individual price point sensitivity which can be exploited by corporations in their negotiation of price terms and value with us individually.

The Regulator's Dilemma

- All of what I have discussed creates a dilemma for regulators, which I have captured in equation:

PET x LLDL x CPI (Consumer Price Index?)

Proliferation of Exponential Technologies*Low levels of Digital Literacy*Commercialisation of Personal Information.

- I have no solution in sight for this dilemma, save for the sage words of US Supreme Court Judge, Mr. Justice Fortas in ***Fortnightly Corp.*** *v* ***United Artists Television, Inc***., 392 U.S. 390, 402 (1968):

"The situation calls not for the judgment of Solomon but for the dexterity of Houdini."

CONCLUDING THOUGHTS

- These are not recommendations, it's too early for that. These are what I hope will be useful points to consider as we work towards building a framework which is fit for the times.

1. The underlying goal of content regulation remains relevant in the digital age. It is concerned with protecting against harm and building trust so that citizens can confidently participate in the digital society and economy.
2. The issues requiring policy and regulatory attention include:
    - Ethical advertising, particularly as it relates to the targeting of children online;
    - We will need to formulate Intensity ratings as virtual reality and augmented reality make advertisements and other content more experiential and immersive.
    - We must protect against media manipulation which cause harm such as internet addiction and other problematic internet use.
    - We will have to mediate between the reasonable commercial use of personal information and the tendency of corporations to exploit information asymmetry.
        - We must strike the right balance in deciding the tradeoffs between ethics, data and commercial viability.

- We must develop a framework to deal with Internet Service Providers who operate as Content Companies.

    - Companies like Google and Facebook sit at the center of the surveillance society. This gives them the most powerful and privileged position in modern civilization.

    - Given their disproportionate power over public opinion, why shouldn't those companies be regulated? Media regulation was borne out of the experience leading up to World War II when the media manipulated public opinion to support the Nazis.

3. Finally and most importantly, we will have to prioritise Digital Literacy as the most immediately practicable regulatory response to digital age challenges and opportunities.

    - "Pinchie Dead" Broadcasting Commission ad illustrates a treatment of digital literacy which is creative and effective.
    - 2+ million views
    - Viral
    - Probably the only message from a content regulator which is capturing the creative imagination of children, which will hopefully translate into desirable behavior when they interact with media.

Bibliography

Adam Dachis, "Do You Read Privacy Policies (and Do You Understand Them)?" *Lifehacker*. November 30, 2012. http://lifehacker.com/5964185/do-you-read-privacy-policies-and-do-you-understand-them

Alison, I. "Imogen Heap shows how smart music contracts work using Ethereum," *International Business Times*, October 4, 2015, http://www.ibtimes.co.uk/imogen-heap-shows-how-music-smart-contracts-work-using-ethereum-1522331.

Berger, G. *et al.*, *UNESCO's Series on Internet Freedom: Global Survey on Internet Privacy and Freedom of Expression*. Paris: United Nations Educational, Scientific and Cultural Organisation, 2012. Accessed September 2, 2014. http://unesdoc.unesco.org/images/0021/002182/218273e.pdf

Bogart, S; Rice, K. "The blockchain report: Welcome to the Internet of value," Needham and Company LLC, October 21, 2015, http://storj.io/TheBlockchainReport.pdf, accessed January 4, 2016. **View in article**

Deloitte. **Tech Trends 2016.**
www2.deloitte.com/global/en/pages/technology/articles/tech-trends.htm

Deloitte analysis and CoinDesk, "Bitcoin venture capital," http://www.coindesk.com/bitcoin-venture-capital/, accessed January 4, 2016. **View in article**

Deloitte University Press Tech Trends 2014;

Diamandis, P. Robot Revolution: These Are the Breakthroughs You Should Watch; http://singularityhub.com/2016/03/15/robot-revolution-these-are-the-breakthroughs-you-should-watch.

Frank, A. Pokémon Go has Full Access to Players' Accounts on Jul 11, 2016 at http://www.wsj.com/articles/pokemon-go-creator-closes-privacy-hole-but-still-collects-user-data-1468363704

Google. "Google Privacy Policy." Last modified December 18, 2017. http://www.google.com.jm/policies/privacy/

Green, C. (2014). "How can the regulator balance concerns about the use of data vs. the desire for economic progress" http://www.broadcastingcommission.org/resources/speeches-presentations?start=20

Hachman, M. The price of free: how Apple, Facebook, Microsoft and Google sell you to advertisers.;2015 http://www.pcworld.com/article/2986988/privacy/the-price-of-free-how-apple-facebook-microsoft-and-google-sell-you-to-advertisers.html

Houston *et al*., (2010) "Creditor Rights, Information Sharing, and Bank Risk Taking" Cited in Pyykko, E. (2012) "Data protection at the cost of economic growth?" *European Credit Research Institute Commentary No. 11*. Accessed September 2, 2014. http://www.ceps.eu/book/data-protection-cost-economic-growth

J Spurling Ltd v Bradshaw, [1956] EWCA Civ 3

Kim, J. & Yeo, J. Valuation of Consumers' Personal Information: A South Korean Example; J Fam Econ Iss (2010) 31: 297.

Lemley, M.A., (2001) "Romantic Authorship and the Rhetoric of Property", 75 TEX. L. REV. 873, 898-99, 902. doi: 10.2139/ssrn.44418

Lessig, L., (1999) "The Architecture of Privacy", VAND. J. ENT. L. & PRAC., http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf

Liem, C., Petropoulos, G. The economic value of personal data for online platforms, firms and consumers. http://blogs.lse.ac.uk/businessreview/2016/01/19/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers/

Morran, C. "1-In-5 Internet Users Always Read Privacy Policies, But That Doesn't Mean They Understand What They're Reading". *Consumerist*. November 28, 2012. http://consumerist.com/2012/11/28/1-in-5-internet-users-always-read-privacy-policies-but-that-doesnt-mean-they-understand-what-theyre-reading/

Niantic. Pokémon GO Privacy Policy (last updated July 1, 2016). https://www.nianticlabs.com/privacy/pokemongo/en

Out-Law. "Average privacy policy takes 10 minutes to read, research finds," Out-Law.com. October 6, 2008. http://www.out-law.com/page-9490

Piscini, E; Guastella, J; Rozman, A; Nassim, T. Block Chain: The Future of Trust. http://dupress.com/articles/blockchain-applications-and-trust-in-a-global-economy/

Schneier, B.(*1963). Data And Goliath : the Hidden Battles to Collect Your Data and Control Your World. New York, N.Y. :W.W. Norton & Company, 2015. Print.*

Schatsky, D; Muraskin, C. *Beyond bitcoin*, Deloitte University Press, December 7, 2015,http://dupress.com/articles/trends-blockchain-bitcoin-security-transparency/, accessed January 4, 2016. **View in article**

Smith, S. Empowering Individuals To Monetize Personal and IOT Data Using Smart Contracts and The Block Chain. https://www.linkedin.com/pulse/empowering-individuals-monetize-personal-iot-data-knowledgelevers

Tennison, J. What is the impact of blockchains on privacy? **https://theodi.org/blog/impact-of-blockchains-on-privacy**

Westin, A., *Privacy and Freedom.* Reviewed by Osbourne Reynolds Jr. New York: Atheneum, 1967. 101-106

World Economic Forum. (2012) *Rethinking Personal Data Project, Workshop Summary: Unlocking the Economic Value of Personal Data- Balancing Growth and Protection.,*(Brussels) Accessed September 2, 2014. http://www.weforum.org/reports/big-data-big-impact-new-possibilities-international-development

Zyskind,G; Nathan, O; Pentland, A. Decentralizing Privacy: Using Blockchain to Protect Personal Data, http://web.media.mit.edu/~guyzys/data/ZNP15.pdf