IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

Volume 15 | Issue 2 | 2019

[Cite as: 15 IJLT, < page no. > (2019)]

NATIONAL LAW SCHOOL OF INDIA UNIVERSITY
BANGALORE

Price: Rs. 900 (in 2 issues)

The mode of citation for this issue of The Indian Journal of Law and Technology, 2019 is as follows:

15 IJLT, <page no.> (2019)

Published by:

Student Bar Association
National Law School of India University
Nagarbhavi, Bangalore – 560072
Website: www.ijlt.in
Email: ijltedit@gmail.com

Distributed exclusively by:

Eastern Book Company
34, Lalbagh, Lucknow - 226 001
U.P., India
Website: www.ebcwebstore.com Email: sales@ebc.co.in

IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

WWW.IJLT.IN

Volume 15 | Issue 2 | 2019

IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

Volume 15 | Issue 2 | 2019

Contents

ARTICLES

Artificial Intelligence Enabled Cyber Fraud: *A Detailed Look into Payment Diversion Fraud and Ransomware*

Alana Maurushat[*], *Abubakar Bello*[**] *and Braxton Bragg*[***]

Abstract *Cyber fraud is rampant. The recent Covid 19 pandemic is a good example of the same. Domain Tools in April 2020 identified over 65,000 websites have been identified as fraud scams related to Covid-19. Organisations have lost billions of money in online scams, and in particular with payment diversion fraud ('***PDF***') and ransomware. PDF is a type of cyber-attack where an entity is tricked into making a direct payment from its account to a false supplier/entity often using real-time payment methods. Ransomware is a type of malicious software that prevents users from accessing their system or personal files usually by locking them through encryption, and demands ransom payment in order to regain access. Based on the professional experience of the authors, coupled with current literature, there is a growing trend of automation, with the use of machine-learning and artificial intelligence. This article discusses PDF and ransomware in the context of mechanics and emerging trends for systematic attacks and response by private industry. These case studies illustrate the limited role that the law plays in the investigation and response to cyber fraud.*

[*] Alana Maurushat is Professor of Cyber security and Behaviour at Western Sydney University and a Board Director with the cybercrime investigations firms IFW Global.

[**] Dr. Abubakar Bello is Lecturer in Cyber security and Behaviour with a strong industry background in information security, risk management and digital forensics. He is also an expert in Nigerian cybercrime. Both are researchers with the Socially Engineered Payment Diversion Fraud (SocEngPDF) project.

[***] Braxton Bragg is a Research Assistant with SocEngPDF; he is a US-licensed attorney completing a Masters in Cyber security and previously held legal and accounting roles with private US firms. Thank you to student intern Kevin Tang for his research.

I. Introduction

Artificial Intelligence Enabled Cyber Fraud encompasses a wide range of traditional online fraud using new tools to automate aspects of the process. This article focuses on two primary online frauds: payment diversion and ransomware. We will go through each type of fraud, first explaining the concept, providing a case study, and then addressing threat vectors – commons ways in which the fraud is committed from financial data to accounting practices, to network intrusion to social engineering aspects. Automated AI aspects are explored within the threat vectors. The case studies are based on real cyber frauds, but the names, personal information, and case specific details have been generalised to protect the identity of the parties involved. This is especially important as these types of audits and investigations are often done over many years, and can involve civil litigation and criminal charges.

As many of these investigation case studies are based on the experiences of the researchers, we need to make clear the capacity and background of the researchers in question. Alana Maurushat is the Professor of Cybersecurity and Behaviour at Western Sydney University, as well as Board Director of the internally renowned cybercrime investigation company, IFW Global. IFW Global is renowned for taking down organised cybercriminal syndicates and recovering funds for individuals and organisations. This article is not underpinned by theory; it is based on first-hand experience of the authors in their roles as researchers, and expert consultants. Where possible, we have cited news articles, television programs, and white papers produced by the industry partners and organisations where the researchers work as expert consultants. Dr. Abubakar Bello is an expert in digital forensics and incident response. He works as a consultant to major companies and government agents. Braxton Bragg is a tutor with the Cyber security and Behaviour program at Western Sydney University, and is senior cyber security consultant with Gridware. He comes from a background in forensic accounting, incident response as well as cyber security compliance.

Maurushat and Bello are currently finalising two funded research projects: Socially Engineered Payment Diversion Fraud, and Ransomware. We have done qualitative interviews with over 30 organisations, and online quantitative analysis from an additional 150 organisations via an online survey – all of which have had recent experiences countering funds lost due to payment diversion fraud or ransomware. The findings of these research projects are not included in this article as the research hasn't been finalised and the work is currently under peer review. Some of the case studies in this article, however, have been built around the work done within these research projects, as well as from first-hand experience of the researchers in their capacity as investigators and consultancy work with industry.

There is a paucity of peer reviewed research articles globally that provide first-hand experiences of some of the problems that law enforcement faces when dealing with certain types of cybercrime, and even less for AI enabled cybercrime. There is a plethora of research on policing and legal approaches, for example, to online child pornography, and online copyright. There is significantly less research on policing and legal responses to online fraud and cyber attacks. Many of these wider cybercrime articles focus on fraud typographies,[1] reviewing of data found within media and

[1] Rodger Jamieson and others, 'Addressing Identity Crime in Crime Management Information Systems: Definitions, Classifications and Empirics' (2012) 28(4) Computer Law & Security Review 381.

blogs,[2] or they provide a statistical and economic analysis.[3] There are a number of reasons for speculation as to why this is the case – it could be that researchers are not as interested in online fraud as other forms of cybercrime, or, as per the experience of the authors, the police have limited budgets and are predominantly focused on crimes where the elements happen within a set jurisdiction. If law enforcement has a limited budget for expensive complex cases, they will focus on the areas where the harms are perceived as the greatest – online child abuse and elements related to national security. Cyber attacks such as payment diversion fraud and ransomware require rapid investigatory response if funds are to be recovered. Police are not set up to deal with these types of investigations. For this reason, private firms are called in to do most of the investigatory work alongside law enforcement. This private work is carried out by cyber security and cybercrime experts typically found in consultancy firms such as Price Waterhouse Cooper, EY, large major law firms, as well as smaller boutique of asset recovery firms. Private firms play an essential and dominant role in countering many types of cybercrime.[4]

The article first addresses Payment Diversion Fraud in Part 2, followed by Part 3 which addresses Ransomware. The next section, Part 4, outlines the criminal legal framework for these areas with fraud being the main area of relevant law. It outlines appropriate laws that deal with these types of fraud by looking at the Convention on Cybercrime, then at relevant provisions in Australian, Canadian and Indian criminal codes. Part 5 addresses why online fraud has one of the highest payouts of cybercrime with the least risk, and examines why law enforcement are ineffective at investigating organised online fraud, prosecuting offenders and recovering fraudulent funds to victims. This part has been written explicitly to capture the sentiments expressed in qualitative interviews from two funded research grants: Socially Engineered Payment Diversion Fraud, and Ransomware. Part 6 looks at ways to reform online fraud investigations. The final section, Part 7, offers concluding remarks. Annex at the end of this article contains a list of essential terms with their definitions.

---

2 *See* for example, Roderic Broadhurst and others, 'Crime in Cyberspace: Offenders and the Role of Organized Crime Group' (2013) <https://ssrn.com/abstract=2211842> accessed 6 May 2020.

3 *See* for example, Lina Fernandes, 'Fraud in Electronic Payment Transactions: Threats and Countermeasures' (2013) 2(3) Asia Pacific Journal of Marketing & Management Review 23.

4 *See* Alana Maurushat and Hadeel Al-Alosi, 'Policing Cybercrime – An Inside Look at Private and Public Cybercrime Investigations' in Philip Birch (ed), *Australian Policing: Critical Issues in 21st Century Police Practice* (Routledge, Forthcoming 2020).

II. Payment Diversion Fraud

A. What is Payment Diversion Fraud?

Payment Diversion Fraud is a type of cyber-attack where an entity is tricked into making a direct payment from its account to a false supplier/entity often using real-time payment methods.[5]

Payment Diversion Fraud has been around for several decades but didn't emerge as its current form until recently. Previously one would have described PDF as a man-in-the-middle-attack but it didn't connote what happened after the attack, namely a fraudulent act.[6] Other terms associated with PDF are supply chain fraud,[7] mandated fraud[8] and business email compromise.[9]

To date there is limited research and analysis on PDF in the public domain.[10] PDF is related to another concept in what is referred to as 'compromised' or 'poisoned' supply chains whereby at any point in the supply chain for a product development or service provided, there are multiple vulnerabilities that can be compromised.

Payment Diversion Fraud has a great economic impact on organisations, with U.K. law enforcement characterising it as the most harmful reported fraud with greater economic impact than Brexit[11] and the U.S. FBI describing it as one of the costliest forms of cyber-enabled fraud affecting U.S. companies. Earlier PDF used phone calls and phishing emails. More recently media have reported fraudsters gaining unauthorised access to an entity's network/phone/IoT—monitoring the network to observe business and

---

5 Ken Gamble, 'Payment Diversion Fraud – A disturbing new hacking trend hitting corporate Australia' (*Akolade*, 13 February 2018) <http://akolade-blog.blogspot.com/2018/02/payment-diversion-fraud-disturbing-new.html> accessed 6 May 2020.

6 Twenty Essex, "Man-in-the-middle" fraud: How to prevent it, who is at risk, and what to do when it all goes wrong' (*Lexology*, 25 April 2017) <https://www.lexology.com/library/detail.aspx?g=6c8cce34-0bfe-4aa6-86fc-edfa88e7c473> accessed 20 March 2019.

7 James L. Patterson, Kimberly N., Goodwin, and Jennifer L. McGarry, 'Understanding and Mitigating Supply Chain Fraud' (2018) 12(1) Journal of Marketing Development and Competitiveness 70.

8 Paul Dean and Rory Grout, 'Something rotten in the state of shipping: What you need to know about Mandate Fraud and the fraudulent redirecting of payments' (*HFW*, October 2017) <http://www.hfw.com/Something-rotten-in-the-state-of-shipping-what-you-need-to-know-about-Mandate-Fraud-and-the-fraudulent-redirecting-of-payments-October-2017> accessed 20 March 2019.

9 Federal Bureau of Investigation, *2017 Internet Crime Report* (2017).

10 Steven Powell, 'Critical Measures to Protect Against Rocketing EFT Fraud Risk Management' (2009) 9(11) Without Prejudice 48.

11 Mara Stein, 'UK Companies Plagued by Payment Diversion Fraud' (*The Wall Street Journal Blog*, 6 October 2017) <https://blogs.wsj.com/riskandcompliance/2017/10/06/u-k-companies-plagued-by-payment-diversion-fraud/> accessed 6 May 2020.

cultural patterns of the organisation before sending out what appears to be a legitimate request from a CEO/finance department/supplier in the form of an email, text, or similar requesting payment.

Payment Diversion Fraud is being committed by a range of criminals located around the world. It is not jurisdiction-specific, though many recent cases derived from our current research grant on PDF have involved payment being made to accounts in Hong Kong, Ukraine, South Africa, Ghana, Nigeria, India, and Brazil. Two anonymised incidences with company IFW Global involved physically tracing payments back to the source located in Nigeria and India (cyber and on the ground surveillance). Our mere cyber investigations of following money trails led to Hong Kong, Ukraine, South Africa, Ghana, and Brazil.

The methods used to enable a PDF attack tracks with a fairly-standardized process used in other types of cyber-attacks. The process progresses through the following sequence: conducting initial reconnaissance, conducting the initial compromise, establishing a foothold in the system, escalating privileges, conducting internal reconnaissance, moving laterally in the system, maintaining a presence in the system, and completing the mission. The main variant is the extent to which automation and artificial intelligence are now part of process.

i. Initial Reconnaissance of Organisation Through Public Information

In this phase, the threat actor will engage in initial reconnaissance of possible targets. Many times, this reconnaissance is performed using open source intelligence ('**OSINT**'). OSINT uses many sources generally available to the public on the internet[12] (eg Google searches, Linked-In searches, social media sources, news articles, and conference websites). The data gleaned from this intelligence gives the threat actor precursory knowledge of potential victim organisations, before ever deciding which organisations to attack. The gathering of information available to threat actors through this method is almost impossible to stop, as customers, vendors, and partners need to have a method of gaining information about organisations with whom they want to engage.

Sometimes this process is automated in the same way that crawlers used by Google, and other search engines, retrieve results for search queries. The attacker does not have to necessarily invest large amount of time to discover

[12] MITRE Corporation, 'Acquire OSINT data sets and information' (*MITRE ATT&CK*, 14 December 2017) <https://attack.mitre.org/techniques/T1247> accessed 27 March 2019.

potential targets. Scripts using common web scraping computer programs can be combined with industry-specific lists of organisations to compile OSINT for targeting would-be victim organisations. Web scraping is also known as web harvesting or web data extraction - web scraping means extracting data from websites in a usable and structured format which is done through a variety of web tools. Social network sites like LinkedIn make this type of open source intelligence gathering easy and provide a wealth of information. The outputs can then be combined with other OSINT data points such as expected travel plans (eg via conference schedules, or news articles) to put attackers on notice of potential targets. AI-based machine learning algorithms can also be used to piece together these data points faster and more effectively to help target more victim organisations.

A simpler method of initial reconnaissance can begin with a phone call to a member of the targeted organisation. Telephone conversations can be used for finding intelligence, gaining trust and learning the behavioural aspects of employees at a firm. And AI techniques can be used to help with this technique too. Some security researchers are already concerned about new technologies such as Google's deep neural network-based Duplex service that can be trained to interact over phone lines with humans without the humans ever knowing a computer is involved.[13] In traditional AI systems, machine learning uses computers to process and learn from data. With neural networks programs try to emulate how the brain processes information with an input layer, output layer, and multiple hidden layers that interact with one another simultaneously. With deep learning the computer trains itself to process and learn from data. Deep neural networks are a method of a computer training itself to process and learn from data mimicking processing of a human brain, and in the case of AI, by additionally mimicking human behaviour. A substantial fear is that threat actors could train these services to conduct intelligence in a highly automated process.

There are other times when no initial reconnaissance is done. In these cases, the process would begin with the phase of establishing access in an organization's network, but this tends to be more common with ransomware rather than payment diversion fraud.

---

[13] Yaniv Leviathan, 'Google Duplex: An AI System for Accomplishing Real World Tasks Over the Phone' (*Google AI Blog*, 8 May 2019) <https://ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conversation.html> accessed 6 May 2020.

ii. Accessing a Weak Point

In this phase, the threat actor will gain some type of initial access to a potential victim organization's systems. Methods of establishing a foothold can include standard phishing emails, spear-phishing emails, man-in-the-middle (MITM) attacks, watering hole attacks, password spraying, or drive-by downloads. The various methods used to gain initial access into an organization's systems are called threat vectors and are discussed below in section 2.3.

iii. Accessing Escalated Privileges

Once initial access to the network is obtained, the next step in the cyber attack is to escalate privileges to allow movement through the network undetected. Privileged access, normally administrator-level, is needed because it allows the attackers to move freely within the environment and remove traces of ever being there. Sometimes rainbow tables and similar tools can help intruders steal credentials. On other occasions, attackers use threat vectors like spear-phishing emails from within the system to help them escalate privileges, usually allowing them to access any system on the network. Once the attackers gain elevated privileges, the network is effectively taken over and 'owned' by the intruders. This allows them to take on the next step of the attack by conducting internal reconnaissance.

iv. Conducting Internal Reconnaissance of the Organisation's Network

Many times, attackers can be in a network for months conducting internal reconnaissance. Recent intelligence reports show that the average time before a network intruder is detected, called the dwell time, in the APAC region during 2018 is 204 days, down from 498 days in 2017.[14] During this phase, attackers are looking for vulnerabilities and examining accounting practices, calendars, company directories, invoice and payment protocols, the tone and rhetoric of emails, and other information that can help achieve the fraud.

The median dwell time is reducing quickly due to organisations gaining a better understanding of best-practices in mitigating their cyber security risk and using more advanced security systems, which many times use AI-based processes. However, while organisations are using AI to help prevent and

[14] Fireeye Mandiant, 'M-Trends Report 2020' (2020) <https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html> accessed 6 May 2020.

detect attacks, attackers are also starting to use AI to make their attacks more effective. In 2017, cyber security firm Darktrace found that attackers were using AI, through machine learning algorithms, to observe average user behaviour in a client network in India.[15] The attackers were then able to use their AI software to mimic this average user behaviour, allowing them to stay undetected in the network for a longer period of time. This is just one example of AI being used to help attackers. Very recently, a report compiled by 26 authors from 14 institutions made predictions about the landscape of malicious use of AI over the next five years.[16] The report discusses scenarios including automation of vulnerability discovery and increased effectiveness of vulnerability exploitation. The report also discusses how the downward moving cost of AI will enable underfunded attackers to use advanced techniques. Overall, it paints a very bleak picture of how malicious use of AI could be employed by attackers in a variety of ways. Once attackers are in an organisation's systems, they normally take measures to ensure they can stay there.

v. Sustaining a Presence

At this stage, although the attackers are in an organization's network with unrestricted access, they must take steps to ensure they are able to sustain a presence long enough to complete the fraud. To accomplish this, sometimes they install malicious programs like root kits and backdoors that allow them to return as frequently as they want, even if they are detected. On other occasions they create ghost users, fake employees with elevated access, and hide those users from real administrators. There are also a variety of other techniques used to ensure continued access. At this point, the original attack vector used to gain access is no longer necessary, and an organisation that remedies the original vulnerability is often left in a worse position than they started. The organisation thinks the intruders are gone and its risk has diminished, but in reality, the attackers can come and go as they please.

vi. Figure out Precisely When and How to execute Payment Diversion Fraud

Using the information gleaned from the internal reconnaissance, the attackers will now create a game plan for conducting the fraud. They understand

[15] Steven Norton, 'Era of AI-Powered Cyberattacks Has Started' (*The Wall Street Journal Blog*, 15 November 2017) <https://blogs.wsj.com/cio/2017/11/15/artificial-intelligence-transforms-hacker-arsenal/> accessed 6 May 2020.

[16] Miles Brundage and others, 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation' (*Arvix*, 20 February 2018) <https://arxiv.org/pdf/1802.07228.pdf> accessed 6 May 2020.

how the invoice and payment process flows, whom, or what systems to communicate with, and how they will execute the fraud. But many times, they will conduct a test run before trying to 'swing for a six'.

vii. Testing a Payment Diversion Fraud with a Low Sum

In many cases, organisations affected by PDF will be hit by multiple payment diversions. The first one or two diversions will be attempted for low value amounts that are unlikely to set off any alarms. In the test runs, and the final fraud payouts, email hijacking or spoofing is the primary method of conducting the fraud. In both cases the attacker will often wait for an opportune time (eg when an account signatory is unavailable due to travel, or a vendor payment is expected and there is a time crunch on receiving the payment).

In an email hijacking, the attackers use a signatory's actual email account to send a request for a payment to be made to an account controlled by the attacker. Sometimes this payment is an expected payment, such as a previously intended payment to an actual vendor. On other occasions the payment will be to a fake vendor setup in the organization's systems by the attacker. Still other times the payment will be a non-expected payment to a real vendor diverted to an attacker-controlled account.

In an email spoofing, the attacker will use a spoofed or look-alike email address to request a payment. A spoofed account can be easily created using very little technical knowledge to make a recipient think the email actually came from a signatories account, although the attacker never actually had control over the real account.[17] Though there is almost always some type of access that has been gained by the attacker to enable enough internal organizational information to plan the attack.

In a look-alike email, the attacker will create an email address on an attacker-controlled domain that seems, to the average user, to come from a signatory's actual address. For illustration: a real account would be named *bob_smith@organisation.com*, but the look-alike email would be *bob_smith@organisatan.com* (emphasis on the changed letter). In both types of attacks, the attackers will also likely create or spoof email addresses on both the sending and receiving side, so they are able to communicate to both sides of the transaction thus enabling them to continue to perpetuate the fraud.[18]

---

[17] Dylan Tweney, 'How to Fake an Email From Almost Anyone in Under 5 Minutes' (*Hakernoon*, 26 October 2017) <https://hackernoon.com/how-to-fake-an-email-from-almost-anyone-in-under-5-minutes-12169dd44a92> accessed 26 March 2019.

[18] Gamble (n 5).

For example, the attacker would be impersonating a vendor to get an organisation to make a payment, while at the same time impersonating the organisation so that the real vendor doesn't know the fraud is occurring either. Other types of diversion could include creating fake vendors and creating payment instructions for an EDI system to divert funds. There are also many other tactics used during PDFs. But as we said, this is likely just a test run.

viii. Complete the Mission

Once the attackers have tested the plan for the fraud with a low amount that is not easily detected by normal accounting review procedures and is sure the fraud will work, they normally will try to make a large final payout. They will follow the same process as before, but this time, they will try to obtain an amount that will be material to the financial statements of the business, and will likely be discovered through normal account reconciliations. At this point, the attackers are finished with their activities and have likely left the network of the organisation for good. But organisations still need to ensure that a complete forensic analysis is conducted on their networks and end points to ensure that the attackers cannot return. Now we will explore some case studies to further describe real-life situations we have seen.

B. Case Study

The facts of these cases, while resembling real investigations, have been altered to protect the affected parties involved in what may be ongoing disputes and investigations.

i. Case A: Large International Company - Sport Equipment Retailer

Company X is an Asian based sport equipment retailer with annual turnover of USD 100 million. They are not, however, listed on the US stock exchange, and are not a publicly traded company.

Company X was notified in October 2017 by one of their suppliers, Supplier Y, that they had not received due payment of USD 2.1 million. Company X, however, claimed that they had paid Supplier Y in September 2017. Upon further investigation by both entities, it was discovered that Company X had been the victim of payment diversion fraud.

The CEO of Company X was flying to Malaysia on business in September 2017. An email generated from his iPhone 7 was sent to the company accounts receivable as he boarded Flight A. The email requested immediate payment of the attached invoice of USD 2.1 million as the CEO had

'forgotten to instruct payment' before he left the office for vacation. The invoice had been generated on Supplier Y letterhead with the details identical to previous invoices but for a change in Swift Code and banking details. The employee at accounts receivable read the email and made the payment. The payment of USD 2.1 million arrived in a bank account in Hong Kong registered to the name of a shell company (registered in Luxemburg) that was not affiliated with Supplier Y. From Luxemburg the money was sent to an additional three different shell companies with accounts located in various tax haven jurisdictions.[19]

An examination, audit, and investigation of the PDF revealed the following things. First, it was discovered that the data log files from the period of June 2015 up until May 2016 showed that Employee C had been compromised. Employee C had systems admin clearance and upon closer scrutiny appeared to have some slightly unusual activities for a period of close to a year. Employee C was also on the Company X's whitelist.[20] Employee C's accounts had been high-jacked. Slowly a very sinister pattern emerged. It was later revealed that Employee C's account had sent a phishing email to the CEO in December 2016 which resulted in the download of malicious software enabling the criminal(s) in question to install a rootkit onto the CEO's desktop computer. The iPhone 7 was also compromised but it remained unclear how this was achieved. This could have been done by the use of a known unpatched vulnerability as found on the dark net. A forensics examination of the phone did not reveal anything unusual though it was reported in September 2017 that Google successfully released a proof of concept attack against a Wi-Fi firmware vulnerability in Broadcom chips using a backdoor into the iPhone 7.[21]

Further scrutiny into payments made over a one-year period revealed that there were in fact three separate fraudulent payments made to third parties. The amounts started as nominal and involved fraudulent invoices from a range of what looked to be normal suppliers. In the first two instances, the email accounts from another senior employee were used. These appeared to be tests prior to the 'big heist' involving the USD 2.1 million using the CEO's email account and iPhone.

---

[19] Richard Murphy, 'World's Best Tax Havens' (*Forbes*, 6 July 2010) <https://www.forbes.com/2010/07/06/tax-havens-delaware-bermuda-markets-singapore-belgium.html#6a3819b825fc> accessed 25 March 2019.

[20] Whitelisting is the practice of explicitly allowing identified trusted entities access to a particular privilege, service, mobility, access or recognition.

[21] Michael Mimoso, 'Remote Wi-Fi Attack Backdoors iPhone 7' (*Threat Post*, 27 September 2017) <https://threatpost.com/remote-wi-fi-attack-backdoors-iphone-7/128163/> accessed 25 March 2019.

Upon further scrutiny of Company X's network it was later discovered that there was a dormant piece of malicious code that sent messages back to what appeared to be a range of IP addresses in what was suspected to be the various command and controls of a botnet. This suggested that first, the network had been compromised for approximately a year. Second, that firewalls, anti-virus and all other cyber security software were ineffective at detection. Third, that the silent, hidden surveillance aspect involved automation, and possibly elements of artificial intelligence. Last, that a human would have been involved later for acts of specific, targeted social engineering such as the specific phishing email sent to the CEO. While it was impossible to ascertain with precision whether or not and how the botnet/ criminal got into the network it is probable that social engineering could have played a part.

ii. Case B: Small Company –Accounting Firm

Company Z is a small accounting firm with annual turnover of USD 2 million. In January 2019, Company Z received an invoice from Company V requesting payment of USD 20,000. Company V's normal email format was (the first name abbreviation).(the last name)@companyv.com. For example, n.nelson@companyv.com. Company Z received a fraudulent email from n.nelson@companyvv.com requesting the invoice to be paid. The fraudster had even gone so far as to register the domain name companyvv.com. While the invoice contained variant bank account details, this didn't cause any alarms on Company Z's part as many companies that they engage with have offices in different parts of the world where the bank details can change. Company V contacted Company Z in February requesting payment. At this point both Companies realised that a payment diversion had occurred. Upon further investigation it was revealed that Company V had been compromised through a mass phishing email sent to nearly all the email addresses in the company with more than one employee opening the link that downloaded malicious software onto their systems. It was further revealed that Company Z was not the only victim as a result of Company V having been compromised. Company V, however, did not alarm the criminal and instead, contacted an entity to conduct an investigation. The investigation revealed that the email had originated in the south of Nigeria. Meanwhile, payment was disguised to be going to a major bank in Norway, but was instead routed to a branch of the major Norwegian bank in Ghana which is relatively

close to Nigeria, a country world-renowned for cyber fraudulent scams and incidences.[22]

iii. Insights from Case Studies

As can be seen from the case studies, PDF affects businesses of all sizes and levels of sophistication. Spoofing was used in both cases, the first involved a text spoof and the second an email spoof. The content in the spoof texts and emails was carefully written to resemble traditional correspondence within the organisation. Most importantly, the amount targeted in both instances was very specific to the regular transactions of the organisations, and not a random amount generated. As will be seen later with ransomware, the amounts tend to be similar regardless of the size or annual turnover of the organisation.

C. Threat Vectors

The threat vectors used to initially infiltrate an organisation's network vary greatly. Some of the more common techniques are summarised below. Additionally, threat vectors used during the actual PDF attack process are discussed.

i. Phishing for Access

In this attack vector, a generalized email will be sent with a link to a fake site access page. This access page will be used to try and trick a user in an organization to hand over their credentials. This vector is highly generalized, and the only user specific information contained in the email would likely be the salutation, similar to the customisation in a standard mass email.

ii. Spear-Phishing for Information

In the spear-phishing for information vector, an attacker will send an email to a specific potential target.[23] The email will look like it is from a legitimate source and will use information gained during the initial reconnaissance phase to customize the email to entice the specific user to give their credentials to an attacker in order to gain access to the target systems. This type of attack is more advanced than just using someone's name in the salutation.

---

[22] Muktar Bello 'Investigating Cybercriminals in Nigeria: A Comparative Study' (DPhil Thesis, University of Salford 2018) <http://usir.salford.ac.uk/id/eprint/47190/> accessed 6 May 2020.

[23] MITRE Corporation, 'Spearphishing Attachment' (*MITRE ATT&CK*, 18 April 2018) <https://attack.mitre.org/techniques/T1193/> accessed 6 May 2020.

iii. Password Spraying

This vector is used to try commonly used passwords across many system access points in a short amount of time. The passwords tried come from lists of the most used passwords. An example would be to try and access all of the email accounts of an organization's users at the same time with a common password.

iv. Drive-by-download

This vector allows a malware to infect users' devices by exploiting simple security flaws. Attackers place the malware often on compromised websites, then the malware automatically downloads and installs itself on the victim's device once the website is accessed.[24] Drive-by-download links are also distributed in malicious emails.

v. System vulnerabilities

Technology giants and software vendors usually announce system vulnerabilities discovered and security patches available to mitigate security risks. Cybercriminals often exploit known vulnerabilities in unpatched system networks, providing them access to distribute ransomware payload on vulnerable devices.[25] For example, the WPA2 weakness and processor vulnerabilities.[26]

There are also threat vectors to be mindful of that are used in the actual payment diversion fraud itself. The following vectors are frequently used for PDF.

vi. Spear-Phishing For Escalated Privileges

In this vector, spear-phishing emails can be sent from actual organization-owned email addresses in order to gain escalated privileges for the attacker. The email sent will usually have a link to a site that social engineers the user in an organization to give away their credentials.

---

[24] Niels Provos and others, 'All Your iFRAMEs Point to Us' (Proceedings of the 17th conference on Security symposium, July 2018).

[25] Dan Goodin, 'Serious flaw in WPA2 protocol lets attackers intercept passwords and much more' (*Ars Technica*, 16 October 2017) <https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/> accessed 22 March 2019.

[26] Mathy Vanheof and Frank Piessens, 'Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2' (Proceedings of the 24th ACM Conference on Computer and Communications Security, 2017) <https://www.krackattacks.com/> accessed 22 March 2019; 'Meltdown and Spectre' (*Meltdown Attack)* <https://meltdownattack.com/> accessed 22 March 2019.

vii. Email Spoofing

As previously described, email spoofing can be used by either falsifying a real email address in the 'from' line of an email through spoofing techniques, or utilising an email from an attacker-owned domain that is similar in nature to the actual organization domain being targeted, but with a single character change in the domain name.

D. Concluding Remarks

Many of the methods used in payment diversion frauds are similar to methods and vectors exploited found in other types of cyber attacks such as ransomware which is explored below. The processes are highly automated and often involve machine-learning where human behaviour is imitated. A most recent PDF involved a deep fake where artificial intelligence was used to mimic the voice of a CEO requesting funds to be transferred to a third party.[27] We expect this type of AI enabled voice fraud to become more prevalent. To date, the authors have not seen such a toolkit available on the dark net but it is only a matter of time before one is made, and is available as an underground cybercrime tool kit and service.

III. Ransomware

A. What is Ransomware?

Ransomware is a type of malicious software that prevents users from accessing their system or personal files usually by locking them through encryption, and demands ransom payment in order to regain access.[28] As will be explored below, the methods and vectors have some overlap with PDF.

Ransomware, belonging to the crypto virology nest, was first introduced in 1989 and physically distributed via floppy disks at a conference event.[29] As there are no specific laws prohibiting the creation of malicious code and software, some individuals create ransomware as tools that hackers can purchase.[30] There are, however, laws that criminalise the use of prohibited

---

[27] Jesse Damiani, 'A Voice Deepfake Was Used to Scam a CEO Out of $243,000' (*Forbes*, 3 September 2019) <https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/#63c6a1ca2241> accessed 7 May 2020.

[28] 'Ransomware' (*Malwarebytes*) <https://www.malwarebytes.com/ransomware/> accessed 7 May 2020.

[29] Ronny Richardson and Max M. North, 'Ransomware: Evolution, Mitigation and Prevention' (2017) 13(1) International Management Review 12.

[30] Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar, 'Malware and Automated Computer Attacks' in *Cybercrime and Digital Forensics: An Introduction*

tools/devices. Devices have been widely defined to include algorithms which, depending on how the ransomware is written, are illegal to possess, as well as to use. Over the last three-decades, ransomware has evolved into an arsenal in the hands of cybercriminals and for as low as USD 750, cyber attackers can obtain a huge collection of ransomware to attack their victims over the internet.[31] Artificial Intelligence engineered malware is now emerging where a bot will mimic human behaviour in a way specifically designed for the target.[32]

Presently, cybercrime is listed as one of the most reported frauds, and in the majority of cases reported, cybercriminals used ransomware to obtain money from the victims.[33] Hackers primarily target sensitive information and data, deploying ransomware to a victim's device, encrypting files and information and often locking the victim out of the system.[34] There are also instances where ransomware is used as a decoy attack: while victim scrambles to pay for the decryption key for their data, the attacker often accesses the victim's data and publishes the data on illegal websites for further financial gain.[35]

Despite the fact that viruses have been around for as long as computers have, ransomware proves substantially different due to its ability to use cryptographic algorithms designed to block users' access by holding data or even the entire device hostage until a ransom is paid. This type of extortion racket with fiscal motive is unlike other malware attacks, since victims are made aware of the exploit and then given mandate directions on how to regain access. Payment often comes in bitcoins, making it easier for the perpetrators to remain unidentified.

(Routledge, 2017) 501.

31 Kim Crawley, 'Ransomware For Sale On The Dark Web Is A Killer Bargain For Criminals' (*The Threat Report*, 12 November 2018) <https://www.thethreatreport.com/ransomware-for-sale-on-the-dark-web-is-a-killer-bargain-for-criminals/> accessed 19 March 2019.

32 Kevin Townsend, 'IBM Describes AI-Powered Malware That can Hide Inside Benign Applications' (*Security Week*, 13 August 2018) <https://www.securityweek.com/ibm-describes-ai-powered-malware-can-hide-inside-benign-applications> accessed 7 May 2020.

33 Nick Robinson and Tareq Hadad, 'Pulling fraud out of the shadows: A spotlight on the Middle East' (*PwC*, 2018) 30 <https://www.pwc.com/m1/en/publications/documents/economic-crime-fraud-survey-2018.pdf> accessed 7 May 2020.

34 Jinal P. Tailor and Ashish D. Patel, 'A Comprehensive Survey: Ransomware Attacks Prevention Monitoring and Damage Control' (2017) 4 International Journal of Research and Scientific Innovation 116.

35 Philip O'Kane, Sakir Sezer and Domnhall Carlin, 'Evolution of Ransomware' (2018) 7(5) IET Networks 321 <https://doi.org/10.1049/iet-net.2017.0207> accessed 7 May 2020.

As a self-propagating malicious program, ransomware essentially involves five stages (as illustrated in Figure 1 before the functionality of a user's device or organisation's information systems are compromised.

Figure 1: Ransomware lifecycle

i. Initiation and setup phase

In the first stage, the cybercriminal or attacker identifies the target for the attack such as an individual, or organisation. The attacker gathers relevant information on the target from open sources (websites, social media, newspapers) to launch a successful attack. The setup may involve creating and deploying websites, emails and bogus information to lure or trap the target.

ii. Infection phase

The second stage involves the main activities in the ransomware attack process. The attacker selects the attack medium and vector to aid the delivery of the ransomware. The internet serves as the primary medium to reach the targeted victims. Attackers often use social engineering tactics and phishing to gain access to the victim's device and network. In phishing, users usually receive spam emails marked as urgent but containing malicious links and codes. Other methods of infection include, but are not limited to, software update, drive-by-downloads, and installers. Once the target's system is infected by the malicious program, the next stage (encryption) becomes activated.

iii. Encryption phase

In this phase, the malicious program searches the victim's device, system, or network to encrypt specific files and folders. Some ransomware encrypt system disk drives and network shared drives, and delete any backup folders

and restore points. In the encryption stage, the malicious program often collects and sends details of the victim's device or system to the attacker.

iv. Extortion phase

After the encryption process is completed, the victim usually receives an email or a prompt for the ransom payment. The victims are often given a deadline for payment to receive a decryption key to restore the data and systems back to normal, and failure to make payments will result in the total loss of data. Attackers use pseudo-anonymous methods to obtain payment from victims to prevent the authorities from tracking them. Typically this involves the use of cryptocurrencies such as Bitcoin and Monero.

v. Decryption phase

This is the final stage in the ransomware cycle. If the targeted victim makes payment to the attacker's pseudo wallet, a decryption key is sent to the victim for data retrieval. However, decryption and restoration of the data is not guaranteed to the victim as the attackers often go back to the extortion phase to gain more from the victim.

B. Case Study

Ransomware has grown to be one of the most advanced and destructive diabolical type of malware, able to cause worldwide catastrophes, from crippling critical infrastructure such as health, transport, and financial services to shutting down manufacturing processing plants. In 2017, the WannaCry breed of ransomware alone infected more than 2,00,000 computers in 150 countries within a day. With the advancement of ransomware and exploit kits in the hands of cybercriminals, more and more prominent attacks are witnessed on a regular basis. Herjavec[36] observed that the global annual cost of cybercrime by means of ransomware to cause damage, fraud, identity theft, and stolen personal and financial data is predicted to exceed trillions of dollars by 2021. The value of the compromised data often leaves ransomware attack victims with no choice but to pay the stated ransom to cybercriminals. The cases below provide some insights on the negative financial effect of ransomware.

The cases below involve ransomware that utilises automated software, with some use of machine-learning, but AI in the strictest sense has not

[36] Herjavec, '2019 Official Annual Cybercrime Report' (Herjavec Group, 2019) 12 <https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf> accessed 7 May 2020.

yet been used in ransomware, though researchers suspect that this is only a matter of time. AI models for cyberattack in the future will identify targets through facial recognition, geolocation, and voice recognition as well as mimic such human behaviours. The AI component of ransomware will most likely rest in the initial compromise of a system. Once compromised, the ransomware can sit stealthily, gathering data and waiting to declare its presence, and ask for a ransom to be paid.

i. Case A – CryptoLocker Ransomware

CryptoLocker was first used in a cyberattack from September 2013 to May 2014. Its success led to the emergence of other ransomware variants and subsequent cyberattacks.[37] CryptoLocker was propagated via spam email with an infected attachment; primary targets were businesses and professionals. Once the victim's system was infected, encryption was executed and a ransom fee via MoneyPak or an equivalent in Bitcoin current was demanded for payment within 72 hours.[38] About 1.3% of the victims affected by the ransomware paid the ransom, but not all users received a decryption key.[39] CryptoLocker ransom payment was estimated at USD 27 million in just the first two months and had infected 2,34,000 computers by April 2014.[40]

ii. Case B – WannaCry Ransomware

In May 2017, WannaCry ransomware was targeted at computers running Microsoft Windows operating system. The ransomware attack was wide spread infecting more than 2,00,000 systems in over 150 countries across health care, government, and telecommunication organisations.[41] The WannaCry attack lasted for a few days and was contained when a security researcher activated a kill-switch to stop the spread and locking of

---

[37] Josh Fruhlinger, 'Recent Ransomware Attacks Define the Malware's New Age' (*CSO*, 20 February 2020) <csoonline.com/article/3212260/recent-ransomware-attck-define-the-malwares-new-age.html> accessed 18 June 2020.

[38] Kevin Liao and others, 'Behind closed doors: Measurement and analysis of CryptoLocker ransoms in Bitcoin' (Proceedings of the 2016 APWG Symposium on Electronic Crime Research, June 2016) <https://asu.pure.elsevier.com/en/publications/behind-closed-doors-measurement-and-analysis-of-cryptolocker-rans> accessed 7 May 2020.

[39] Mark Ward, 'Cryptolocker victims to get files back for free' (*BBC*, 6 August 2014) <https://www.bbc.com/news/technology-28661463> accessed 18 June 2020.

[40] US Department of Justice, 'US Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator' (2 June 2014) <https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware> accessed 7 May 2020.

[41] ibid.

devices.[42] Some victims paid the ransom demanded and three months after the WannaCry ransomware attack, about £108,000 was withdrawn from the associated Bitcoin wallet.[43]

iii. Case C – Georgia ransomware

The US has been known to be one of the most targeted countries for cyber-attacks. For example, the state of Georgia experienced ransomware cyber-attacks consecutively in 2018 and 2019. In March 2018, the city of Atlanta also experienced a ransomware attack where the attackers demanded ten Bitcoins from the government.[44] Atlanta city did not pay the ransom, but the damages and expenses to restore the systems back online resulted in millions of dollars and a long time dealing with the loss of data.[45] One year later, in 2019, Jackson County was hit with a ransomware cyberattack that crippled the IT network and systems in government offices.[46] However, unlike the city of Atlanta, Jackson County paid a hefty ransom to the attackers to obtain access to their information after the lockout.[47]

iv. Insights from Case Studies

The case studies highly the different threat vectors and manners of escalation in ransomware. Ransomware may vary in the same ways as other forms of malware such as viruses and worms. Unlike PDF, ransomware is spread randomly from system to system and amounts tend to be similar irrespective of the size and capacity of the organisation.

---

[42] Sir Amyas Morse KCB, Comptroller and Auditor General, National Audit Office, United Kingdom, 'Investigation: WannaCry cyber attack and the NHS' (Department of Health, 24 October 2017) <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf> accessed 7 May 2020.

[43] O'Kane (n 35).

[44] Lily Hay Newman, 'Atlanta Spent $2.6 M to Recover From a $52,000 Ransomware Scare' (*Wired*, 23 April 2013) <https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/> accessed 7 May 2020.

[45] Jon Fingas, 'Atlanta ransomware attack may cost another $9.5 million to fix' (*Endgadget*, 6 June 2018) <https://www.engadget.com/2018/06/06/atlanta-ransomware-attack-struck-mission-critical-services/> accessed 21 March 2019.

[46] Catalin Cimpanu, 'Georgia county pays a whopping $400,000 to get rid of a ransomware infection' (*ZD Net*, 9 March 2019) <https://www.zdnet.com/article/georgia-county-pays-a-whopping-400000-to-get-rid-of-a-ransomware-infection/> accessed 21 March 2019.

[47] Linn F. Freedman, 'Jackson County, Georgia Pays Hackers $400,000 After Ransomware Attack' (*The National Law Review*, 14 March 2019) <https://www.natlawreview.com/article/jackson-county-georgia-pays-hackers-400000-after-ransomware-attack> accessed 21 March 2019.

C. Threat Vectors

Ransomware attack requires a vector for the covert deployment of an infection to the victim. The attack vectors for ransomware vary in complexity and effectiveness,[48] and the most prevalent ones are:

i. Malicious emails / Social Engineering

This is one of the most common attack vectors often distributed via phishing. In some attack scenarios, an attacker employs social engineering to lure the victim into opening a malicious email attachment that will enable the execution of the ransomware payload.

ii. Brute force - Remote Desktop Protocol

On the network level, an attacker gains admin access to server credentials with remote access. Once within the network, the attacker could exploit administrative tools and vulnerabilities to distribute and infect other devices within the network.

iii. Exploit Kits

These are software packages used to create vulnerabilities within a system or network in order to perform malicious activities. For example, Eternal Blue was used in the 2017 WannaCry ransomware attack that infected over 2,00,000 systems globally.

iv. Malvertising

Targeted adverts are usually displayed to potential victims based on their search history or certain web preferences. As an attack vector, malvertising displays advert with hidden malware links but mirrored as a normal advert specifically placed by a cybercriminal. Attackers often use malvertising on highly reputable websites to target their victims.[49]

---

[48] Aaron Zimba, 'Malware-Free Intrusion: A Novel Approach to Ransomware Infection Vectors' (2017) 15(2) International Journal of Computer Science and Information Security 317.

[49] Xinyu Xing and others, 'Understanding Malvertising Through Ad-Injecting Browser Extensions' (Proceedings of the 24th International Conference on World Wide Web, May 2015) <https://doi.org/10.1145/2736277.2741630> accessed 7 May 2020; Yuliya G. Zabyelina, 'Can criminals create opportunities for crime? *Malvertising* and illegal online medicine trade' (2016) 18(1) Global Crime 31 <https://doi.org/10.1080/17440572.2016.1197124> accessed 7 May 2020.

v. Drive-by-download

This vector allows a malware to infect users' devices by exploiting simple security flaws. Attackers place the malware often on compromised websites, then the malware automatically downloads and installs itself on the victim's device once the website is accessed.[50] Drive-by-download links are also distributed in malicious emails.

vi. System vulnerabilities

Technology giants and software vendors usually announce system vulnerabilities discovered and security patches available to mitigate security risks. Cybercriminals often exploit known vulnerabilities in unpatched system networks, providing them access to distribute ransomware payload on vulnerable devices.[51] For example, the WPA2 weakness and processor vulnerabilities.[52]

vii. Network propagation

Organisations and individuals are always connected to networks to enable the seamless sharing and transfer of data. Ransomware is also capable of spreading from computer to computer over a network. On a shared network, an attack on a victim's device is easily distributed to every connected device and service within the same network. For example, the NotPetya breed of ransomware infected every machine on the Maersk global network.[53]

viii. Propagation through shared services

Online services could also propagate ransomware. For example, infections on a home computer could easily be transferred to an office or to other connected computers if the ransomware places itself inside a shared folder.

Ransomware distribution channels are endless, and the distributors are becoming more crafty. One click could be all it takes to become a victim. Technical controls for screening and spread prevention, including having adequate backups are important to survive a ransomware attack.

---

[50] Provos (n 24).

[51] Goodin (n 25).

[52] Vanheof and Piessens (n 26); 'Meltdown and Spectre' (n 26).

[53] Catalin Cimpanu, 'Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack' (*Bleeping Computer*, 25 January 2018) <https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/> accessed 7 May 2020; Lee Mathews, 'NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million' (*Forbes*, 16 August 2017) <https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#5b32046e4f9a> accessed 7 May 2020.

IV. Legal Framework

The Convention on Cybercrime, an agreement between member nations of the European Union, is the only international agreement in the area of cybercrime. It is unique in that it is open for signature by non-EU states. The United States, Canada, and Australia, for example, have signed and ratified the Treaty. By contrast, India has neither signed nor ratified the convention.

The convention may be divided into three key divisions: substantive law, procedural requirements, and international cooperation. All signatories to the convention must criminalize certain activities. The convention creates four main categories of substantive offences:

1. offences against the confidentiality, integrity, and availability of computer data and systems, comprising interference and misuse of devices (computer hacking offences);
2. computer-related offences, such as forgery and computer fraud;
3. content-related offences, in particular the production, dissemination, and possession of child pornography; and
4. offences related to copyright infringement.

Both socially engineered and AI enabled fraud generally involves both the computer hacking offences and computer-related fraud offences. Particularly any access, modification, or interference of a computer is criminalised. Also, misuse of devices may also be criminalised. Here devices can be defined as a hacking tool such as Zeus Malware Kit or a ransomware kit. These are algorithms and not a physical tool or kit. The 'misuse of a device' does not involve the malicious use of a hacking tool, one need only to prove intent to use the device for an illegal purpose such as fraud. This can be tricky where a device has dual purpose, but in the case of crimeware kits such as Zeus and ransomware kits, there is no dual purpose and intent is easily proven.

As seen in the examples in Sections 2 and 3, not all socially engineered frauds involve both hacking and fraud offences. They may only involve one or the other depending on the circumstances. The mere sending of a deceptive email with intent to commit fraud would not be criminalised under the Convention or under Canadian law. It would, however, be criminalised under Australian law. The Australian Criminal Code has a provision of dishonest use of a computer or device with intent to commit fraud. Of course, most jurisdictions in the world criminalise fraud, whether it is committed online or offline.

The Table below looks at the Convention provisions as well as the Canadian and Australian provisions. These two jurisdictions have been highlighted merely because of the authors' familiarity with these two jurisdictions.

Council of Europe Convention on Cybercrime 2001	**Canada Criminal Framework Criminal Code 1985**	**Australia Criminal Framework Criminal Code 1995**
Offences against the confidentiality and availability of computer data and systems	Generally, Canada uses broad language to capture the obligations under the Convention.	Generally, Australia has very detailed provisions that address specific aspects of the Convention's obligation. What is criminalised is clear.
Article 2—Illegal access	Section 342.1 of the Criminal Code	Division 477 – Serious Computer Offences Sections 477.1-477.3 Sections 478.1-4
Article 3—Illegal interception	No direct equivalent	Subdivision B – Interference with telecommunications 474.3 – 474. 11 Division 477 – Serious Computer Offences Sections 477.1-477.3 Sections 478.1-4
Article 4—Data interference	Section 430 (1.1) of the Criminal Code	See Above.
Article 5—System interference	No direct Equivalent	Division 477 – Serious Computer Offences Sections 477.1-477.3 Sections 478.1-4
Article 6—Misuse of devices	Section 326 (1)(b) of the Criminal Code Section 327 (1) of the Criminal Code	Section 408E (Computer hacking and Misuse)
Computer-Related Fraud and Forgery		
Article 7 Computer – Related Forgery	Section 366	Part 10.8 Financial Information Offences
Article 8 Computer – Related Fraud	Section 366	Sections 480.1-480.6

The Convention also addresses the procedural aspects of cybercrime. The main categories here are:

1. expedited preservation of stored computer data;
2. expedited preservation and partial disclosure of traffic data;
3. production orders;
4. search and seizure of stored computer data;
5. real-time collection of traffic data; and
6. interception of content data.

In theory the procedural aspects allow collaboration between law enforcement in different jurisdictions to gather intelligence, and obtain and preserve evidence. The reality, however, is that criminals use anonymising technologies such as TOR, TAILS, and VPNs and making traceback extremely difficult. The money is equally difficult to trace as it moves from one bank to another in notable tax haven jurisdictions or moves through cryptocurrency.[54] The difficulties in traceback and cryptocurrencies are explored in the following section.

V. Insurmountable Challenges

International law enforcement co-operate on a range of investigations and prosecutions of criminals related to cybercrime. Recent examples include the take down of two dark net markets, Hansa and AlphaBay.[55] The FBI and US Drug Enforcement Agency organised and collaborated with law enforcement from around the world to shut down AlphaBay which was in 2017 the world's largest dark net. AlphaBay boasted over 40,000 vendors and nearly a quarter of a million users/customers. Authorities arrested the mastermind and administrator of the site, Canadian Alexandre Cazes, in Thailand. Additionally, hundreds of arrests were made in countries around the world of various narcotic and weapons vendors selling on AlphaBay. In June 2017, Dutch police and Europol had secretly taken over the dark net market Hansa. At that time when AlphaBay disappeared many users and

[54] Maurushat and PhD candidate Halpin are involved with the development of a cryptocurrency database matcher and tracer technology. The technology is being developed to assist with the large growing body of investigation work with cryptocurrency fraud, as well as cryptocurrency as a money-laundering tool.

[55] Andy Greenberg, 'Global Police Spring a Trap on Thousands of Dark Web Users' (*Wired*, 20 July 2017) <https://www.wired.com/story/alphabay-hansa-takedown-dark-web-trap/> accessed 7 May 2020.

vendors flocked to competitor Hansa.[56] Later in July 2017, it was publicly announced that Dutch police had been running Hansa for a month, gathering intelligence and evidence.[57] That site was also then shut down. Hundreds of arrests of vendors were made following the takedowns.

Similarly, Interpol, along with Europol and law enforcement around the world, run operations together to take down child pornography rings, as well as anti-terrorism operations. While online fraud and computer offences fall within the jurisdiction of Interpol, there is significantly less international cooperation in this field to arrest and prosecute online fraudsters.

International organisations such as Interpol provide information about online fraud scams, monitor cases, and provide intelligence and support to national police enforcement agencies, but successful international fraud investigations of online fraud organisations is few and far between. There simply aren't the resources to conduct an international fraud investigation because those resources are spent and used elsewhere.[58]

There is often a false belief among law-makers and academics that if the right legislation is enacted, and *if enough* resources are allocated to the task, that the law can rise to the challenge and overcome a myriad of obstacles to combat cybercrime. This is, however, simply not the case for online fraud, and in particular where cybercrime is enabled by AI. The existing criminal provisions for fraud in most jurisdictions would allow for a successful prosecution of a fraudster irrespective of whether a computer was used to assist with the fraud.

After attending many conferences both within Australia and Canada representing a private cybercrime investigation firm, invariably law enforcement will ask how much money was spent on an internationally coordinated investigation. This can range between USD 2,00,000 to USD 5,00,000. Time and time again law enforcement have stated that the same investigation by law enforcement would cost ten times that amount. Below we discuss why this is the case.

---

[56] Andy Greenberg, 'Operation Bayonet: Inside the Sting that Hijacked an Entire Dark Web Drug Market' (*Wired*, 8 August 2017) <https://www.wired.com/story/hansa-dutch-police-sting-operation/> accessed 7 May 2020.

[57] MIX, 'Dutch Police Secretly Ran a Huge Dark Web Drug Marketplace for a Month' (*TNW*, 20 July 2017) <https://thenextweb.com/insider/2017/07/20/police-fbi-drug-dark-web-market/> accessed 7 May 2020.

[58] At the International Cybercrime Conference in Vancouver (2018) law enforcement commented that a private investigation costing USD 2,50,000 would be closer to USD 2 million if law enforcement were to undertake the same investigation.

Cybercrime investigations involve unique challenges. The challenges involve difficulty with the harmonisation of laws, jurisdictional issues, resource implications, lack of training, ambiguity in terms of how a criminal provision will be interpreted alongside human-rights protections, and, above all, a host of technical hurdles that makes tracing back to the offender difficult. Additionally, online fraud is not seen as having health and safety repercussions like other crimes, therefore, it is not prioritised. In spite of advances in machine learning, big data techniques, and artificial intelligence, attribution remains a formidable challenge.

A. Jurisdiction

Computer crimes often involve parties located abroad. These crimes may involve people located in different jurisdictions, whether they are different states or provinces within a country or different countries altogether. Each jurisdiction may have its own laws dealing with an issue as well as its own unique set of evidence procedures in courts. Uniformity is a real problem. Successful prosecution often involves assistance and cooperation of authorities from an outside jurisdiction.[59] For a variety of reasons, some jurisdictions may or may not be willing to cooperate. Such cooperation generally must proceed through the cogs of bureaucracy in cases where time and access to good digital evidence (unaltered) is of the essence. This often means applying for warrants in multiple jurisdictions, which may translate into a loss of valuable time, and perhaps a loss of obtainable intelligence and evidence.

Private investigation firms ('**PI**'s) are less hampered with timely investigation and jurisdictional issues. If there is actionable intelligence, a PI merely picks up the phone to another PI located in that area, and contracts with them then and there to do a job immediately. This network of over 4,000 PIs world-wide operating with this type of agility makes private PIs more able to investigate online fraud. For example, the author worked on one investigation where an email tracker was sent to a spokesperson for the fraudulent company operating out of Thailand. The victim had contacted law enforcement first, but was told that they could not help her. At that point she contacted a PI who was able to act immediately on her behalf. As the victim hadn't let on that she knew that she was being defrauded, active intelligence could be gained through re-social engineering the conman. A series of email and telephone requests asking to speak to someone more senior resulted in a successful email track to a device being used in a pub in Bristol, England.

[59] For a broad in discussion of cybercrime and jurisdiction *see* Bert-Jaap Koops and Susan W. Brenner (eds), *Cybercrime and Jurisdiction: A Global Survey* (T.M.C. Asser Press, 2016).

A PI in Bristol was called to go to this pub immediately and take photos of people operating a laptop or mobile device as this is truly the only way to ascertain who the person is using a device. In this instance an identity was made by asking the pub owner a few questions. From there the case unravelled, and foreign police could be brought in for the arrests of the individuals in question. It isn't a matter of law enforcement not being involved, but a matter of when to involve them.

B. Attribution

In cybercrime and cybersecurity, figuring out who is the person or entity responsible for an attack is the greatest singular challenge. Attribution takes three forms: who are the humans behind the incident; what devices are involved with the incident; and who may be claiming responsibility of the attack (how to verify if this is false). The greatest challenge remains in identifying and determining the physical location of the computer, and then the actual individual(s) who used the computer/network to commit a crime. As seen in the above example, a PI had to go to the pub to take a photo of the individual as they were corresponding in real time with the victim.

Let us look at another example. Police in Canada, for example, cannot obtain a warrant to wiretap someone in Mongolia, and they cannot compel an ISP in Papa New Guinea to provide data logs immediately. This type of international policing requires the cooperation of law enforcement and courts in other jurisdictions. Law enforcement could contact authorities in the location of the hacker, but cooperation may not be forthcoming. First, inter-jurisdictional investigations rely on the offence being given similar priority in both jurisdictions. For truly repugnant cases, such as child pornography, jurisdictions tend to have similar strong mandates. In the case of hacking (i.e., unauthorized access) and fraud, the priorities are often disparate.

Ironically, law enforcement have much greater capabilities and can access rich communication and fraud information that PIs cannot access. For example, law enforcement can follow two trails: the communications data trail and the financial trail. Law enforcement can access stored communication such as the content of an email or the content of a text message. Law enforcement have access to capabilities such as Cellebrite forensic tools which can bypass Apple iPhones encryption. One can only license Cellebrite if one is a law enforcement agent in a designated jurisdiction. Law enforcement can also store, access, and use metadata with great facility. The same holds true for financial information. The right tools and legislative powers exist to allow for successful prosecution, however, there are only a handful

of successful international investigations of online fraud leading to arrest and prosecution. This is, again, due to lack of resources and inadequate budgets, the ability to immediately follow a lead in another jurisdiction, and the lack of law enforcement in another jurisdiction to respond to the lead with the same immediacy.

The reality is that law enforcement tend to use their resources to respond to local problems. Where there is no victim in the locale of a particular police force, priority there will not be given to an overseas investigation. Another challenge is what is known as the 'de minimus rule', whereby in order to justify valuable police resources, a certain threshold of damages must be met. The jurisdictional hurdles stem from practical considerations as well as a lack of criminalization of an act across jurisdictions.

C. Remedies

Ironically, the main reason why using a PI is more effective than the use of law enforcement is the highly practical issue of remedy. If you lose USD 2 million it is likely that recovering the money would be your first priority. A successful arrest and prosecution resulting in prison time would be a secondary benefit. The laws in most jurisdictions, however, are designed such that a successful police operation may result in arrest, prosecution, and jail time, but no money is recovered. This is due to a number of possibilities. The first, is that some jurisdictions such as Australia have a bi-furcated approach to fraud. If a victim reports the fraud to police, and there is enough evidence to prosecute, the perpetrator in question could go to prison but the victim then has to hire a lawyer to proceed in civil proceedings in order to try to recover the lost funds. In other jurisdictions such as New York, the process of asset recovery and criminal sanction in terms of sentencing are all done at once in the court.

Often the money has been laundered in safe haven jurisdictions, or increasingly is stored as a cryptocurrency – both of which are tremendously difficult to recover funds from.[60] Or if money was miraculously recovered, the enabling legislation for proceeds of crime is inherently complex, expensive and challenging as the victim must bring a case before the court. Even when there has been a successful civil claim to recover funds, it is often the case that the defendant will claim bankruptcy. The portion of assets recovered generally is merely the tip of the iceberg. The remainder of money obtained through

[60] Cryptocurrency recovery is performed by specialist technology companies such as Cryptofound Recovery, a Silicon Valley company specialising in cryptocurrency forensics (<www.cryptogound.com> accessed 6 May 2020).

fraudulent means is nearly always located in tax havens or in untouchable cryptocurrencies.

VI. How to Effectively Fight Online Fraud?

In jurisdictions such as Australia, fraud is handled by State law enforcement. This typically means that most successful fraud cases are ones where the criminal and victim are located in the same state. Online fraud is rarely based in one jurisdiction. The author has seen cases involving more than 32 jurisdictions. Organised online crime is sophisticated. Tackling this successfully requires both national and international coordination. In Australia at least, the Australian Federal Police ('**AFP**') *should* (but currently do not) take the lead on fraud cases instead of the State. For example, asking for help from overseas law enforcement must go through the designated authority under the Convention on Cybercrime. If a police officer in the State of Queensland had a lead on someone in England, a request to assist would have to go through the AFP. This process is not time-efficient whereas cybercrime leads are time sensitive.

Statistics are frightfully poor for organised fraud. Often a victim will contact law enforcement and then be told that there is nothing that they can do about it given the complexity and jurisdictional issues.[61] If an organisation lost $20,000 in a ransomware payment, this simply isn't sufficient to warrant an investigation. But the real crime is that the details of the fraud are not captured into databases allowing fraud cases to be linked within the State, Nation, and around the world. This is very problematic. On paper a victim may only have lost USD 30,000 but collectively if the data were analysed, the same ransomware or PDF fraud may have affected hundreds of victims around the world with totals loss closer to the USD 2,00,00,00,000 mark. This is simply not captured with the way in which law enforcement collects data or chooses not to record the data accurately. Indeed there are many barriers to law enforcement sharing raw data, as well as data analytics.

Bennett-Moses and Maurushat undertook a study of data sharing amongst Australian law enforcement and intelligence agencies as part of the D2D Cooperative Research Centre. A portion of the work and findings from the study was published in an online submission to the Australian government:

> Some of the challenges are definitional. For example, different legislation will use different terms (and different definitions of the same

[61] *See* Alana M. Maurushat, 'Botnet Badinage: Regulatory Approaches to Combating Botnets' (DPhil thesis, University of New South Wales, 2011).

> term) to describe the object of analysis – is it data, information, communications, records, or documents? And are these physical things or digital signals or both? There are also different terms to describe the relationship between such things and particular agencies responsible for them – data might be held, in the custody of an agency, under the control of agency, in the possession of an agency, in the care of an agency, or an agency might be responsible for it or have acquired or obtained it. Again, each of these terms often comes with conflicting definitions.
>
> In addition to definitional issues, there is an issue with the assumption of much legislation about data (or equivalent term) that it is held (or equivalent term) by one entity. The question is then whether it is given to another entity and in what circumstances this is required, encouraged, permitted, or punished. However, none of this works as well with new ways of storing data – a common data platform through which multiple agencies can access data stored on one or more public or private servers does not fit easily into the existing framework.
>
> All of these issues are discussed in the report, albeit in the specific context of law enforcement information sharing. The advantages of a single Act that resolves the current confusion, dealing with all information sharing questions in a principle-based way according to a coherent set of concepts are great. Such an Act can and should recognise distinctions based on the diversity of data and circumstances, but there is no need for hundreds of separate provisions in different legislations using inconsistent concepts and definitions. For example, only a thorough review, based on existing work of the ALRC, can derive a principles-based understanding of the circumstances in which secrecy laws are appropriate. Our report included recommendations as to how the legal framework could be reworked in order to improve information sharing for law enforcement purposes. These could be combined with this project in order to improve the current complex patchwork laws rather than being excluded from scope.[62]

While the above highlights the difficulty in information sharing within Australia, there are even greater barriers to sharing information with overseas law enforcement. There may be issues of trust, having to work within the Mutual Legal Assistance Treaty framework, and budgetary restrictions.

---

[62] Lydia Bennett-Moses and Alana Maurushat, 'D2DCRC Information Sharing Report' (2018), cited in Lydia Bennett-Moses and others, 'Response to Issues Paper on Data Sharing and Release' (2019) UNSW Law Research Paper No.19-13 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3348816> accessed 7 May 2020.

Hiring a Private Investigation firm specialising in asset recovery is a more effective way of recording funds but this is simply not an option for most victims. As discussed prior, a typical investigation will cost between USD 2,50,000 to USD 5,00,000. A victim would have to put this money up front to run the investigation with no chance of recovery. Often multiple victims will pool their money to run the investigations but more times than not a private investigation is out of reach for the victim.

The reality is that cyber-insurance is the method that most organisations turn to when they have been the victim of PDF or Ransomware. Curiously, many cyber insurance policies do not specifically cover social engineered fraud unless a company's internal network or computer has been compromised. If, for example, an employee was contacted over the phone and was tricked to give key information to a criminal, then a deceptive email was sent which did not involve breaking in to or accessing the network or system, this is not considered 'cyber'. Or when a company becomes victim to a PDF scam due to client's compromised system, this does not always meet the definition of 'cyber' or 'computer' within some insurance policies. Careful attention must be paid to the wording of cyber insurance policies.

A new market selling decryption keys for Ransomware variants has emerged. Only a few companies offer such services, and the price to decrypt is often more than the ransom but many firms are choosing to purchase the decryption key, rather than reward those criminals behind ransomware. But decryption keys are not available for all variants of ransomware, only a select few.

One concept that is yet to be fully explored in the online fraud space is to offer a bounty for information leading to the arrest behind organised cybercrime fraud. A firm would invest their own money to investigate online fraud syndicates then receive a large portion of the funds recovered. The incentive would have to be substantial but it could prove to be an effective method down the road. How such a program would look in practice would clearly present with many significant challenges. As online fraud becomes more advanced incorporating AI enabled malware, traceback to the individuals and organisations involved in fraud will become more difficult. New methods such as bounties may be required as the technologies progress.

VII. Concluding Remarks

This article has looked at socially engineered payment diversion fraud and ransomware from the perspective of real cases, and the experiences of the

authors working in the field. The authors are working on two research projects related to Socially Engineered Payment Diversion Fraud as well as Ransomware. While the empirical findings are not yet complete from these projects, initial insights have been shared in this article.

Socially engineered payment diversion fraud and ransomware have many similarities including threat vectors and information cycles. They largely differ, however, in amount and reconnaissance. Ransomware tends to request affordable payment amounts where a company can easily see the benefit of immediate payment. These amounts range between USD 10,000 and USD 50,000. For ransomware, often a criminal or algorithm has stealthily been inside a network observing and probing for an effective way to ransom the data. PDF by contrast does not necessarily have to involve system compromise, or length periods of reconnaissance. The amounts stolen, however, have a range of between USD 5,000 to more than USD 1,00,00,000.

Law enforcement has limited capability in dealing with online organised fraud due to issues of jurisdiction, attribution, resources, and the ability to follow leads in a timely fashion. Hiring a private cybercrime investigation firm, while likely more effective in dealing with frauds involving multiple jurisdictions, is simply out of reach for many organisations. Organisations in the case of ransomware either pay the ransom or purchase the decryption key. If they have cyber insurance they will attempt to make a claim post-incident. In the instance of PDF, the amount is so substantial that a firm will want to have a full audit of its systems performed, and then implement a series of operational changes to help mitigate and prevent further instances. A firm may wish to employ a cybercrime investigation firm to assist in recovering funds. Cyber insurance might also play a role for PDF.

Moving forward into the future, the emerging field of blockchain used for logistics in supply chains is promising as is the progression towards quantum encryption and quantum decryption. Both of these methods, however, will only help prevent some forms of PDF and ransomware. Criminals are smart. They evolve to ensure a continued livelihood. Even if detection, prevention, and mitigation techniques are significantly improved, targeting the weaknesses of human beings to be socially engineered will never completely disappear.

Annex: Essential Terms

Adware: Any software program in which advertising banners are displayed as a result of the software's operation. This may be in the form of a pop-up

or as advertisements displayed on the side of a website, such as on Google or Facebook.

Artificial Intelligence: An area of computer science that emphasises the creation of intelligent machines that mimic human behaviour.

Back door: A method of accessing a computer program or network that circumvents security mechanisms. Sometimes a programmer will install a back door so that the programmer can accesses the program to perform security patches, troubleshoot, or monitor use. Attackers, however, can also use backdoors that they discover (or install themselves) as part of an exploit.

Bot server and command-and-control (C&C) source: C&C refers to the communications infrastructure of a botnet. A botnet master issues commands and exercises control over the performance of bots. Bots fetch data from a pre-programmed location, and interpret that data as triggers for action and instructions on what function to perform. The pre-programmed location is known as the bot server or C&C source. C&C is achieved by means of a bot server. The term 'server' refers to any software that provide services on request by another piece of software, which is called a client. The bot requests and the server responds. Where the client is a bot, the server is reasonably enough called a bot server. Common bot servers are IRC servers, HTTP servers, the DNS (by means of TXT records), peer-to-peer nodes, cloud nodes, and increasingly devices otherwise known as the Internet of things (e.g., Xbox).

Bot: A software that is capable of being invoked from a remote location in order to provide the invoker with the capacity to cause the compromised computer to perform a function. Botnets have a modular structure whereby modules (bots) may be added or taken away from each bot to add to it new exploits and capabilities. This ensures a botnet master's ability to rapidly respond to technical measures set up to infiltrate and take down the botnet.

Botnet: A collection of compromised computers that are remotely controlled by a bot master.

Compromised computer: The term 'compromised computer' is commonly used interchangeably, and in some cases wrongly, in the literature with 'zombie', 'bot', and 'bot client', which confuses hardware with software, creates inconsistency of usage, and may be confusing to users. Herein, a 'compromised computer' is a computer that is connected to the Internet (an internet is any network of any size that uses the protocol TCP/IP, and the Internet is

the largest such internet) and on which a bot is installed. The computer is thus said to be compromised.

Crypto currency: A digital monetary currency in which encryption techniques are used to generation of units of currency which can then be verified to authorise the transfer of funds.

Dark Net: A subsection of the deep web – the portion of the Internet purposefully not open to public view through search engines or www protocol - where hidden networks such as Tor, VPN or TAILS are required to access the network. Dark nets are similar to underground markets where illicit goods are traded.

Distributed Command and Control (or super botnets): A type of botnet that draws on a small botnet comprised of fifteen to twenty bots. The botnet herders may have anywhere from 10,000 to 2,50,000 bots at their disposal but use a select few for a particular purpose. The smaller botnet is then used to issue commands to larger botnets (hence the term 'distributed command and control').

Distributed denial of service (DDoS): A DDoS attack is the most common form of online civil protest. A denial-of-service attack is distributed when multiple systems flood a channel's bandwidth and/or flood a host's capacity (eg, overflowing the buffers). This technique renders a website inaccessible. DDoS attacks are performed with a botnet, with several of these being used simultaneously. A DDoS attack may also be distributed by use of peer-to-peer nodes. A botnet is comprised of core elements. They are defined below for clarity and will be re-examined in more specific contexts in the analysis that follows this section.

DNS hijacking: DNS (domain name system) hijacking allows a person to redirect web traffic to a rogue domain name server. The rogue server runs a substitute IP address to a legitimate domain name. For example, www.alanna.com's true IP address could be 197.653.3.1, but the user would be directed to 845.843.4.1 when they look for www.alanna.com. This is another way of redirecting traffic to a political message or image.

Dynamic DNS: A service that enables the domain name entry for the relevant domain name to be updated very promptly, every time the IP address changes. A dynamic DNS provider enables a customer to either update the IP address via the provider's web page or using a tool that automatically detects the change in IP address and amends the DNS entry. To work effectively, the

time-to-live value for the DNS entry must be set very short, to prevent cached entries scattered around the Internet serving up outdated IP addresses.

Encryption: It is the conversion of plain text into 'cipher text', encrypted information. Encryption acts to conceal or prevent the meaning of the data from being known by parties without decryption codes. Botnet instructions commonly use encryption. Encrypted instruction can then not be analysed, making investigation, mitigation, and prevention much more difficult. Public-key cryptography is often used. In public-key cryptography, a twin pair of keys is created: one is private, the other public. Their fundamental property is that, although one key cannot be derived from the other, a message encrypted by one key can only be decrypted by the other key.

Exploit: It is the implementation, in software, of a vulnerability.

Fast flux: A particular, dynamic DNS technique used by botnet masters whereby DNS records are frequently changed. This could be every five minutes. Essentially, large volumes of IP addresses are rapidly rotated through the DNS records for a specific domain. This is similar to dynamic DNS tactics. The main difference between dynamic DNS and fast flux is the automation and rapidity of rotation with a fast-flux botnet. Some fast-flux botnets rotate IP addresses every five minutes, and others every hour.

Harm: Anything that has deleterious consequences, which includes injury to persons, damage to property, financial loss, loss of value of an asset, and loss of reputation and confidence. Harm arises because a threatening event impinges on a vulnerability.

Malware: A simplistic definition of malware is malicious software. Malware, for the purpose of this research, is defined as potentially harmful software or a component of software that has been installed without authorization to a third-party device.

Multihoming: It involves the configuration of a domain to have several IP addresses. If any one IP address is blocked or ceases to be available, the others essentially back it up. Blocking or removing a single IP address, therefore, is not an effective solution to removing the content. The content merely rotates to another IP address.

Organised crime: A category of transnational, national, or local groupings of highly centralized enterprises run by criminals who intend to engage in illegal activity, most commonly for profit.

Penetration/intrusion testing: A type of information-systems security testing on behalf of the system's owners. This is known in the computer-security world as ethical hacking. There is some argument, however, as to whether penetration testing must be done with permission from a system's owners or whether a benevolent intention suffices in the absence of permission.

Phishing: The dishonest attempt to obtain information through electronic means by appearing to be a trustworthy entity.

Proxy servers: A service (a computer system or an application) that acts as an intermediary for requests from clients by forwarding requests to other servers. One use of proxy servers is to get around connection blocks such as authentication challenges and Internet filters. Another is to hide the origin of a connection. Proxy servers obfuscate a communication path such that user M connects to a website through proxy server B, which again connects through proxy server Z, whereby the packets appear to come from Z not M. Traceback to Z yields information of an additional hurdle, however, as packets also appear to come from B. Other proxy servers such as Tor are anonymous.

Ransomware: A type of malicious software that prevents the user from accessing or using their data (often through encrypting the data), whereby a fee must be paid or service performed before the user's data is decrypted.

Rootkits: Software or hardware devices designed to gain administrator-level control and sustain such control over a computer system without being detected. A rootkit is used to obscure the operation of malware or a botnet from monitoring and investigation.

Safeguard: A measure intended to avoid or reduce vulnerabilities. Safeguards may or may not be effective and may be subject to countermeasures.

SQL injection: Defacing a website involves the insertion of images or text into a website. This is often done via a SQL (structured query language) injection. A SQL injection is an attack in which computer code is inserted into strings that are later passed to a database. A SQL injection can allow someone to target a database giving them access to the website.

TAILS: It is a live operation system that functions from a USB stick, DVD, or external hard-drive that, once installed onto your external device, preserves your privacy and provides anonymity for online use. Essentially it forces all connections through the Tor network, then leaves little to no trace on the computer once used.

Threat: A circumstance that could result in harm or damage and may be natural, accidental, or intentional. A party responsible for an intentional threat is referred to as an attacker.

Threatening event: An instance of a generic threat (such as malicious code) that may cause harm or damage.

Tor: It protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world. It prevents somebody from watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location. It is described as onion routing due to the use of multiple layers of proxy servers, similar to the multiple layers of an onion. It is used by users in heavily Internet-censored countries, like China and Iran, to access blocked websites, as well as by some criminals to prevent law enforcement from traceback to the source.

Virtual private network (VPN) service: A network that uses a public telecommunications infrastructure (usually the Internet) to connect remote sites or users together. This connection allows secure access to an organization's network. Instead of a dedicated, real-world connection such as a leased line, a VPN uses virtual connections 'routed through the Internet from an organization's private network to the remote site or employee'. VPN is made secure through cryptographic tunnelling protocols that provide confidentiality by blocking packet sniffing and interception software.

Virus: A block of code that inserts copies of itself into other programs. Viruses generally require a positive act by the user to activate them. Such a positive act would include opening an email or attachment containing the virus. Viruses often delay or hinder the performance of functions on a computer, and may infect other software programs. They do not, however, propagate copies of themselves over networks. Again, a positive act is required for both infection and propagation.

Vulnerability: A feature or weakness that gives rise to susceptibility to a threat. Vulnerabilities exist in software and hardware.

Worm: A program that propagates copies of itself over networks. It does not infect other programs, nor does it require a positive act by the user to activate the worm. It replicates by exploiting vulnerabilities.

Zero day: An exploit or vulnerability that is exploited against a target on the day on which public awareness of the existence of the vulnerability occurs (i.e., zero days have elapsed between the awareness and the use).

Hitting the White Ball: The Technology Neutrality Principle and Blockchain-Based Applications

Anne Veerpalu[*] *& Eduardo da Cruz Rodrigues e Silva*[**]

Abstract *This article provides a legal analysis model for legislators to employ in order to identify non-compliance with the technology neutrality principle in cases of use of blockchain technology. The principle of technology neutrality is aimed at supporting innovation and competition. The article uses the treatment of an application called CUBER in Estonia as early as in 2014 as an example for such analysis. The CUBER mobile application used blockchain technology to execute payment transactions for goods and services. The article first portrays the challenges that the technology neutrality principle poses on existing regulation. It then explores whether technology discrimination took place against CUBER and how this could have been avoided through compliance with the technology neutrality principle. Through this analysis, the article maps the challenges that all start-ups encounter when initiating the use of a new technology aiming to innovate an existing process.*

[*] Anne Veerpalu is an attorney-at-law and a PhD candidate of Law, University of Tartu, Estonia. Anne constructed the structure of the research, conducted the data search and the interviews, drafted the first version of the article and edited the final version of the article.

[**] Eduardo da Cruz Rodrigues e Silva is an associate of NJORD Law Firm and holds a Master's degree in Law and Technology from TalTech, Estonia. Eduardo researched the e-money regulation's historical perspective, the securities regulation, edited the first draft and re-edited the draft article after peer-reviews.

I. Introduction

The applications of blockchain technology can broadly be classified under financial and non-financial heads.[1] Cryptocurrencies, issuance of securities, trading, settlement, and insurance are identified as common financial areas of application, while proof of existence of documents, data storage, internet of things, internet applications, notarisation, music licensing, and anti-counterfeit solutions are popular non-financial areas of application identified. Blockchain technology is, in its essence, a data recording technology that can either be centralised or decentralised. The centralised-decentralised aspect of the blockchain relates to the existence or non-existence of a trusted centralised party administering the blockchain.

Blockchain applicabilities are represented by coins or tokens which concretise the specific rights that are attributed to the coin or token holder. As the applicabilities of blockchain are distinct and cover different areas, it is evident that different laws may apply depending on the nature of the application.

Bitcoin refers to a software which uses blockchain as is its underlying protocol to create a decentralised version of electronic cash. Payment of Bitcoin can be made directly between the parties to a transaction, without the need for a trusted centralised third party, i.e., without the supervision of a financial institution. The Bitcoin protocol establishes a network that solves the problem of double spending by time stamping transactions into a chain of hash-based proof-of-work verified blocks. The creator of any new block – called a miner – is rewarded with Bitcoins as compensation and there is no additional transaction fee from the network for the parties to the transaction. The network is called 'trustless' because there is an economic incentive for the miners (creators of new blocks) to obey the rules of the network without supervision by a centralised operator since "*it is more profitable to play by the rules than to undermine the system*".[2] Bitcoin, as a unit, is identified by Nakamoto as an electronic coin.[3]

In order to prevent discrimination against new technologies, it is important to ensure that the application of existing regulations is compliant with the principle of technology neutrality. The principle of technology neutrality

---

1 Michael Crosby and others, 'Blockchain Technology: Beyond Bitcoin' (2016) 2 Applied Innovation Review <http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf> accessed 10 February 2020.

2 Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) Bitcoin White Paper <https://bitcoin.org/bitcoin.pdf> accessed 10 February 2020.

3 Nakamoto (n 2).

is included in various legal texts in the European Union ('**EU**') and in essence means that all technologies should be treated equally, not some preferred and some discriminated against. The E-Money Directive[4] introduces the principle of technology neutrality in its Recital 7, which states:

> It is appropriate to introduce a clear definition of electronic money in order to make it technically neutral. That definition should cover all situations where the payment service provider issues a pre-paid stored value in exchange for funds, which can be used for payment purposes because it is accepted by third persons as a payment.

This means that the electronic money ('**e-money**') definition should not prefer that a specific technology be employed in allowing for the use of e-money.

Each EU member state is required to transpose EU directives into its national laws, respecting the same principles. This article is based on the e-money regulation of Estonia, and explores whether the technology neutrality principle survived the transposition of the E-Money Directive into Estonia's national law.

The case under analysis is the implementation of the Estonian e-money regulation on a mobile application called CUBER that was developed in 2014 by a local bank in Estonia – AS LHV Pank ('**LHV**'). The CUBER mobile application used blockchain technology to execute payment transactions for goods and services.

The Estonian Financial Supervisory Authority ('**the FSA**') qualified CUBER as e-money[5] under the Payment Institutions and E-money Institutions Act ('**the PIEIA**'),[6] which meant that only 1,000 - 2,500 euros of CUBER were allowed to be used per e-money device (device using the CUBER application) during a calendar year. This limitation substantially restricted the use of the CUBER application by LHV's clients. The respective limitations in the PIEIA were repealed on 13 January 2018, upon the initiative of the Ministry of Finance, which by then had realised that the limitations were linked to

---

[4] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, OJ L 267 (E-Money Directive).

[5] The FSA refused to confirm or comment on this statement. It did not consent to LHV releasing the qualification provided by the FSA to LHV or to LHV sharing the material on the case with the authors for the benefit of this research, knowing that LHV had consented to such data sharing. The relevant emails are held with the authors.

[6] *See*, Payment Institutions and E-money Institutions Act 2010 (PIEIA).

the outcome that not a single entity had applied for an e-money license in Estonia.[7]

Legal analysis of such cases is important as lessons learned could help identify non-sustainable regulation, assist in the implementation of existing regulation, and avoid discriminatory practices against innovative new business models or uses of technology. Any preferential treatment of existing technologies and the status quo of the market might qualify as protectionist, and therefore, against the principle of technology neutrality.

Since it is questionable whether the CUBER application should have been subjected, in the first place, to the PIEIA and its limitations on use, the research questions of the article are as follows:

(i) Was an old concept of e-money device disproportionally implemented on a new blockchain technology-based mobile application?

(ii) Was the implementation of the PIEIA's limitations on the use of e-money devices compliant with the principle of technology neutrality, in the context of the new innovative technology?

The case analysis is based on information publicly available and that communicated by the Head of the Legal Department of LHV.

The article is structured as follows: Section II provides an overview of the principle of technology neutrality in EU legislation and of the principle's application to the e-money regulation. Section III then discusses the circumstances of the CUBER case, the characteristics of CUBER, and its technical setup. Section IV examines the implementation of Estonia's e-money regulation on CUBER and the question of whether it should have been applied at all to the application. Finally, Section V provides a summary of the conclusions drawn in the article.

II. The Principle of Technology Neutrality in the European Union

The technology neutrality principle is included in Recital 15 of the General Data Protection Regulation[8] and Recital 16 of the EU Regulation on

---

[7] Letter by the Ministry of Finance to Mr Mihhail Stalnuhhin of the Finance Committee of the Estonian Parliament (11 October 2017) (in Estonian, held by the authors).

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119.

Electronic Identification, Authentication and Trust Services (eIDAS).[9] Those recitals respectively state that the "*protection of natural persons should be technologically neutral and should not depend on the techniques used*" and that "*it should be possible to achieve the necessary security requirements through different technologies*". This means that the use of blockchain technology for certain regulated applications should not, by itself, be reason for differential treatment.

Van der Haar introduces four rationales[10] behind the technology neutrality principle, which are as follows:

(i) The *non-discrimination* rationale requires that regulation does not favour one technology over the other, as otherwise, discriminatory rules would distort competition and the market. Achieving non-discrimination does not require major regulatory changes.

(ii) The rationale of *sustainability* indicates that the principle of technology neutrality requires regulation to be flexible and open to technological change. By not being specific to a technology, regulation becomes future-proofed as existing regulation can apply to technologies not existing at the time of its drafting. However, van der Haar highlights that application of the sustainability rationale could also lead to a decrease in legal certainty.

(iii) A slightly different rationale is that of *efficiency*, which calls for the creation of dynamic, functional rules that can evolve with technological developments. It is not sufficient to have non-discriminatory or future-proofed rules which are static, but it is essential that regulation be able to respond to changing market conditions.

(iv) The fourth rationale, which is presented from the natural persons' perspective, is *denominated consumer certainty*. As per this rationale, when services are considered by consumers as interchangeable, technology neutrality would ensure that such services are regulated in a similar manner.

These four rationales provide different perspectives on the complexity of the technology neutrality principle and how variable its application to blockchain technology can be. This also means that there are different legislative

---

[9] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257.

[10] IM van der Haar, 'The principle of technological neutrality: Connecting EC network and content regulation' (PhD thesis, Tilburg University 2008) <https://pure.uvt.nl/ws/portalfiles/portal/1063437/3240352.pdf> accessed 10 February 2020.

and regulatory paths that states may follow when applying existing laws to blockchain technology applications.

Next, we study Reed's[11] explanation of the technology neutrality principle through: (i) the different meanings of the principle; (ii) the categories of technology neutral regulation; and (iii) the example of the E-Money Directive's[12] compliance with technology neutrality.

According to Reed, one of the meanings attributed to the principle of technology neutrality is that the same fundamental rules should apply irrespective of the online or offline nature of the regulation object. This must not be confused with cases where there exists a single rule applicable irrespective of the context. The shortcoming of applying identical rules to different regulation objects is that distinctions between the objects will mean that "*the effect of the rules is different as between them*". Accordingly, Reed clarifies that "*technologically neutral rules addressing the same issue may differ in their wording and content, in order to achieve the same effects when applied to different technologies*."[13] The other meaning of the technology neutrality principle is the idea that rules should not discriminate against a particular technology.[14]

Reed considers that regulation may be classified under three heads, from the point of view of technology neutrality. These are: (i) *technology indifferent* regulation; (ii) *implementation neutral* regulation; and (iii) *potential neutral* regulation.

First, *technology indifferent* regulation requires rules to apply equally in both online and offline contexts. Regulation is indifferent to what technology is used. It instead regulates behaviour and consequent effects, and not the means used to achieve the effects.

Second, *implementation neutral* regulation means that when technology-specific regulation is introduced, it does not favour one technology over another and ensures equivalent implementation effect on different technologies. Reed gives the following example for implementation neutral regulation: "*the issuance of e-money is so fundamentally different an activity*

---

[11] Chris Reed, 'Taking Sides on Technology Neutrality' (2007) 4(3) SCRIPTed – A Journal of Law, Technology & Society 263 <https://script-ed.org/wp-content/uploads/2016/07/4-3-Reed.pdf> accessed 10 February 2020.

[12] Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, OJ L 275.

[13] Reed (n 11).

[14] Reed (n 11).

from the printing of banknotes and minting coins that it would clearly be difficult, if not impossible, to regulate both activities by means of the same legal rules."[15]

Finally, *potential neutral* regulation refers to situations where specific regulation is required to achieve an essential legal result and as a consequence, the law regulates a special technological attribute. The key factor for a law to be potentially neutral is the presence of legal requirements in the law which permit other technologies to become compliant.

For the purposes of the article, the questions are: what is considered an issuance; and whether the fact of payments made with CUBERs through a mobile application using funds in a bank account would qualify as an issuance of e-money, or whether this would merely be a payment service, since LHV was allowing the mirroring of CUBERs as money in the bank account.

In the following section, the CUBER application and its technical setup are introduced.

III. Circumstances of the CUBER Case and its Technical Setup

On 13 June 2014, a news report stated that LHV had become the first credit institution in the world to hire a cryptocurrency expert.[16] LHV was developing an innovative product called CUBER, which was an experiment to issue "*100,000 EUR worth of cryptographically protected claims against bank into Bitcoin blockchain*".[17] This meant that CUBER was built as an application on the Bitcoin blockchain.

In essence, LHV was testing a technology application which used both a centralised banking system and a new innovative technology, namely tokens,[18] when the global economy was still coming to terms with Bitcoin.

---

[15] Reed (n 11).

[16] Hans Lõugas, 'LHV palkas esimese pangana maailmas bitcoin'i-spetsialisti' (*Eesti Päevaleht*, 13 June 2014) <https://epl.delfi.ee/eesti/lhv-palkas-esimese-pangana-maailmas-bitcoin-i-spetsialisti?id=68871319> accessed 10 February 2020 (in Estonian).

[17] *See*, 'CUBER – LHV Bank started public use of blockchain technology by issuing securities' (*cuber*, 8 June 2015) <http://www.cuber.ee/en_US/news/> accessed 10 February 2020.

[18] According to the European Securities and Markets Authority (ESMA), "*Tokenisation is a method that converts rights to an asset into a digital token. It is effectively a means to represent ownership of assets on DLT. Virtually anything can be tokenised, ranging from physical goods to traditional financial instruments*". *See*, ESMA, *Advice: Initial Coin Offerings and Crypto-Assets* (ESMA50-157-1391, 9 January 2019) 7, 8 <https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf> accessed 10 February 2020.

CUBER was designed as a coloured coin,[19] which meant that "*an amount of Bitcoin [was] repurposed to express another asset*."[20] As aptly summarised by Antonopoulos:

> Colored coins are managed by specialized "wallets" that record and interpret the metadata attached to the "colored" bitcoins. Using such a wallet, the user will convert an amount of bitcoins from uncolored currency, into colored coins, by adding a label that has a special meaning. For example, a label could represent stock certificates, coupons, real property, commodities, collectible tokens, etc. To color the coins, the user defines the associated metadata, such as the type of issuance, whether it can be subdivided into smaller units, a symbol and description, and other related information. Once colored, these coins can be bought and sold, subdivided, aggregated and receive dividend payments. The colored coins can also be "uncolored" by removing the special association and redeeming them for their face-value in bitcoin.[21]

CUBER is an acronym for Cryptographic Universal Blockchain Entered Receivables, and according to its website, it is a "*technically new kind of certificate of deposit and is meant to be a building block for various innovative financial products*."[22] Nowadays, such units are called 'tokens', and these are generally categorised under three different heads, as examined further in section IV B.[23]

CUBER's product development was separated from the bank by way of a financial technology start-up, OÜ CUBER TECHNOLOGY ('**the LHV start-up**'), which was a subsidiary of the LHV Group. The LHV start-up had developed an iOS and Android CUBER application, namely CUBER Wallet, together with Swedish ChromaWay, which was meant for the use of CUBER as "*fast, free, P2P mobile fiat currency payment*".[24] In the testing phase of CUBER, the application was used for payments in the cafeteria of LHV's building.

---

[19] *See*, cuber (n 17).
[20] Andreas M Antonopoulos, *Mastering Bitcoin* (1st edn, O'Reilly 2014).
[21] Antonopoulos (n 20).
[22] *See*, cuber (n 17).
[23] Securities and Markets Stakeholder Group, *Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets* (ESMA22-106-1338, 19 October 2018) <https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf> accessed 10 February 2020.
[24] *See*, cuber (n 17).

Unfortunately, LHV's initiative was short-lived – since June 2015,[25] there have been no updates on the project website, and although no official notice of suspension of the project has been communicated to the public, according to Mr. Daniel Haab,[26] Head of the Legal Department of LHV, the project was terminated in 2015 for various reasons. Among these was the FSA's qualification of CUBER as e-money[27] under the PIEIA.[28] This qualification as such was not detrimental, however, the limitation of use under Section 6(5) of the PIEIA was. The limitation stated:

> Up to 1000 euros of e-money may be stored on an e-money device if the e-money device does not allow repeated storage of e-money (hereinafter recharging). If it is possible to recharge an e-money device, up to 2500 euros of e-money may be stored or recharged on the e-money device during a calendar year.

Accordingly, LHV could only issue 2,500 euros worth of CUBER per user per year.

While this does not mean that there were no other convincing reasons for the termination of the CUBER project, this article focuses on the regulatory obstacles faced due to the qualification of CUBER as e-money and the respective limitations of issue.

The next section explores the e-money regulation of the time and the qualification of CUBER as e-money under the regulation.

IV. E-Money Regulation

The usage of e-money surged with the advent of the Internet, and its adoption has permitted the development of new payment methods using novel technologies. E-money was not developed during this decade or century but was first recognised as a concept in 1983.[29]

---

[25] *See*, cuber (n 17).

[26] One of the authors both met with Mr Haab and has an email from Mr Haab on file confirming the same.

[27] The FSA refused to confirm or comment on this statement. It did not consent to LHV releasing the qualification provided by the FSA to LHV or to LHV sharing the material on the case with the authors for the benefit of this research, knowing that LHV had consented to such data sharing. The relevant emails are held with the authors.

[28] PIEIA, s 6(1).

[29] D Chaum, 'Blind signatures for untraceable payments' in D Chaum et al (eds), *Advances in Cryptology* (Springer 1983) 199-203.

A. The E-Money Directives and Their Transposition

In the EU, the first legislation that specifically targeted e-money was Directive 2000/46/EC on the taking up, pursuit of and prudential supervision of the business of e-money institutions, which was to be transposed by Member States by 27 April 2002. Since then, the technical evolution and growth of new mechanisms of e-money has progressed at a fast pace. Further, Directive 2000/46/EC suffered from certain limitations, due to which the second E-Money Directive (Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of e-money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC), which is presently in force, was adopted in 2009 and was required to be transposed by all Member States by 30 April 2011. The second E-Money Directive was transposed into Estonian law through the enactment of the PIEIA.

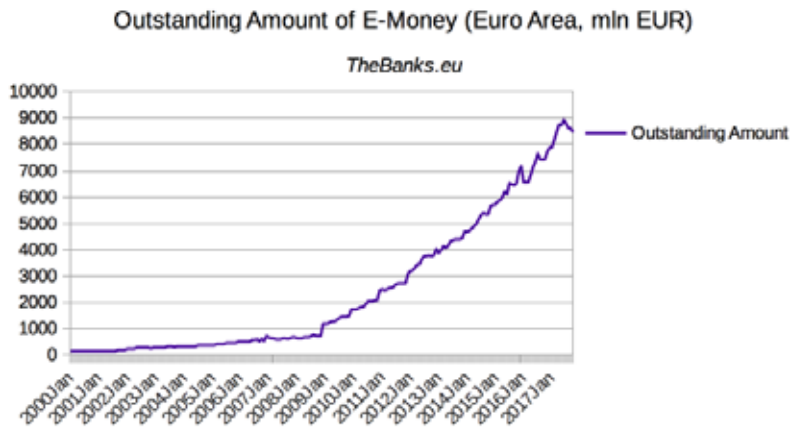

Figure 1: Outstanding Amount of E-Money[30]

In Figure 1, we see the total amount of outstanding e-money in the Eurozone from 2000 to 2017. This figure shows the amount of money that was received for the issuance of e-money, as there is a requirement for issuance of e-money at par value of euro amount received. As can be seen, there is a stagnation between the years 2000 and 2009, and a clear increase of the outstanding amount since 2009. The initial years of stagnation correspond to the period when the first E-Money Directive was in force and where e-money was almost non-existent, while the subsequent period post 2009

[30] 'Electronic Money Institutions in Europe' (*TheBanks.eu*, 2 July 2019) <https://thebanks.eu/articles/electronic-money-institutions-in-Europe> accessed 10 February 2020.

corresponds to the entry into force and transposition of the second E-Money Directive.

The first E-Money Directive prescribed a restriction on e-money institutions that forbade them from providing services not connected with the issuance and administration of e-money. The position of the United Kingdom's Financial Conduct Authority at the time, considering that the E-Money Directive regime and its licensing obligations would apply to telecommunication operators, was that telecommunication service providers could not provide telecommunication services since those were not closely related to the issuance and administration of e-money.

According to Reed, the first E-Money Directive[31] was contrary to the technology neutrality principle as it fell afoul of *implementation neutral* regulation. The reason for this conclusion is connected to the existence of three different legal regimes that could apply to the activity of transferring funds to a third party: (i) the credit institution regime; (ii) the e-money institution regime; and (iii) the payment institution regime. In comparison with the other two regimes, the first E-Money Directive contained restrictive requirements, one of which was that the activities of e-money institutions must be limited to providing only those services which were closely related to the issuance and administration of e-money. The combined effect of these requirements were, in Reed's opinion, "*to make e-money issuance only marginally profitable*".[32] This created an imbalance that led to preferential treatment of payment and credit institutions in contrast to e-money institutions, as the former could also provide additional services beyond that of issuance and administration. The payment institution regime was especially incomparable as it allowed for more freedom in the provision of services, in prescribing lower capital and liquidity requirements.[33]

Furthermore, Reed argues that "*the choice in the E-Money Directive to regulate the issuance of e-money, rather than the provision of e-payment services, was one of the reasons why this legislation was not implementation neutral.*"[34] This means that the e-money institutions were tied to the service of issuance and could not use e-money for payment services. Most

---

[31] Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, OJ L 275.

[32] Reed (n 11).

[33] Reed (n 11).

[34] Reed (n 11).

e-money issuers would – if the first E-Money Directive had allowed it – carried on payment services in addition to the issuance of e-money.

One of the main ideas underlying the principle of technology neutrality is that of online and offline equivalence. When human relations regulated by law have functional equivalence online and offline, the same/equivalent set of rules should apply. According to Reed, the drafters of the first E-Money Directive found equivalence between e-money businesses and payment systems operated by deposit-taking banks, which led to the application of equivalent laws from the latter to the former. Reed adds that the second E-Money Directive "*abandons the deposit-taking bank analogy in favour of a more generic model of payment service regulation which was developed in the light of modern, on-line payment services*."[35]

We can conclude that the second E-Money Directive had a positive effect on the usability of e-money. The sudden and consistent increase of the outstanding amount of e-money can be explained by the ability of e-money institutions to provide services not solely related to the issuance of e-money, which in turn eliminates the comparative disadvantage that existed vis-à-vis the payment institution regime.

However, the statistics in Figure 2 indicate that even the second E-Money Directive, despite its harmonising effect, failed to equalise the situation for all Member States. The figure portrays the total e-money institution licenses issued per EU Member State (since the time the respective domestic regulations entered into force).

Country	Number of E-money Institutions	Country	Number of E-money Institutions
Austria	0	Belgium	7
Bulgaria	5	Croatia	3
Cyprus	13	Czech Republic	2
Denmark	2	Estonia	1
Finland	0	France	13
Germany	8	Greece	2
Hungary	1	Ireland	8
Italy	7	Latvia	2

[35] Chris Reed, 'Online and offline equivalence: aspiration and achievement' (2010) 18 (3) International Journal of Law and Information Technology 248.

Country	Number of E-money Institutions	Country	Number of E-money Institutions
Lithuania	55	Luxembourg	8
Malta	16	Netherlands	3
Poland	0	Portugal	1
Romania	0	Slovakia	1
Slovenia	2	Spain	5
Sweden	3	United Kingdom	150

Figure 2: E-Money Institution licenses issued in the respective EU Member States[36]

As can be seen, the United Kingdom and Lithuania have been the main jurisdictions issuing e-money institution licenses, followed by Malta, Cyprus and France. The majority of EU Member States have issued a residual number of e-money institution licenses. Moreover, the number of e-money institution licenses issued per EU Member State is not proportionate to the population and economic weight of the Member State. For example, Estonia has only managed to issue a single e-money institution license, and that too, as recent as September 2019,[37] yet, its neighbouring state Lithuania has issued 55 licenses. The discrepancy in the number of licences issued may be attributed to the regulatory arbitrage of applicants who choose jurisdictions that are more appealing in terms regulatory differences, and not simply to an unwillingness of these Member States to issue licenses. For instance, a significant obstacle for applicants in Estonia was Section 6(5) of the PIEIA, which as discussed earlier, imposed a limitation of 1,000 or 2,500 euros per e-money device per year.

The next sections investigate the applicability of the PIEIA's definition of 'e-money' to CUBER, and the question of whether LHV or its start-up should have been treated as an obligated entity under the PIEIA. The origin of Section 6(5) of the PIEIA is also discussed, in order to substantiate the conclusions reached.

---

[36] Compiled from the European Banking Authority's register of payment and electronic money institutions under PSD2 (as of 23 September 2019) <https://eba.europa.eu/risk-analysis-and-data/register-payment-electronic-money-institutions-under-PSD2> accessed 10 February 2020.

[37] Estonian Financial Supervision and Resolution Authority, *in House Pay AS sai e-raha asutuse tegevusloa* (10 September 2019) <https://www.fi.ee/et/uudised/inhouse-pay-sai-e-raha-asutuse-tegevusloa> accessed 10 February 2020 (in Estonian).

B. Did CUBER Qualify as E-Money Under the PIEIA?

The E-Money Directive defines e-money in the following manner:

> "electronic money" means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions […], and which is accepted by a natural or legal person other than the electronic money issuer.

The PIEIA, in transposing the definition from the E-Money Directive, thus stated that an object must meet the following criteria to qualify as e-money:

(a) it is monetary value stored on an electronic medium;

(b) it expresses a monetary claim against the issuer;

(c) it is issued at par value of the amount of the monetary payment received;

(d) it is used as a payment instrument to execute payment transactions;

(e) it is accepted as a payment instrument by at least one person who is not the issuer of the same e-money.[38]

According to Mr. Daniel Haab of LHV, the FSA qualified CUBER as e-money under the PIEIA, which it considered to have fulfilled all the above-stated criteria. For the present analysis, the CUBER product is described on the basis of facts retrieved from the CUBER website.[39] The PIEIA valid at the time of the CUBER project has been used to analyse whether CUBER qualified as e-money under the law.

The analysis shows the following result:

(a) CUBER had monetary value because it served the function of a means of exchange and was a representation of fiat currency;

(b) CUBER was issued and stored in a blockchain technology-based application, which is an electronic medium;

(c) In purchasing CUBER from LHV, a claim was acquired against LHV who was the issuer of CUBER, and the claim amount was the amount of the value of CUBER, meaning that the CUBER expressed a monetary claim against the issuer;

---

[38] PIEIA, s 6(1).

[39] 'Conditions of use of the CUBER APP during the test period' (*cuber*, 11 May 2015) <http://www.cuber.ee/en_US/terms/> accessed 10 February 2020.

(d) CUBER represented the value of the monetary amount received and was thus issued at par value of such amount;

(e) CUBER could be used as a means of payment to third parties for acquiring goods or services. In other words, CUBER could be used as a payment instrument;

(f) CUBER was accepted by the cafeteria of the LHV building and was thus, accepted by at least one person other than the issuer.

Thus, CUBER appears to satisfy all the above-stated criteria to qualify as 'e-money' under the PIEIA. However, according to Section 6(6) of the PIEIA, deposits or other repayable funds within the meaning of Section 4 of the Credit Institutions Act shall not be deemed as e-money. Since CUBER may be considered a representation of a deposit, Section 6(6) exempts it from being classified as 'e-money'.

CUBER's website describes it as a "*technically new kind of certificate of deposit*", without any additional characteristics. In contrast, its treatment as e-money under the PIEIA presupposes that CUBER is something more than a mere use of deposited funds in the bank for payment. Such treatment, however, is flawed. CUBER was a mobile application that used Bitcoin blockchain and coloured coins technology to allow users to pay using money already deposited in their bank account. Thus, it seems redundant to qualify the mere mirroring of the same deposits into CUBERs, as falling under a different and more restrictive regime than that which would apply to credit institutions. In essence, treating CUBERs as e-money would mean that the difference in treatment was simply related to the distinct label of the deposits, i.e., CUBER, and the use of blockchain technology as infrastructure for payments. This, in turn means that the option to utilise the deposits for payment for goods and services was discriminated against once a different technology was used.

The argument that CUBER should not have been treated as e-money is reinforced by examining the example of the more recent concept of tokens and its categorisation by the European Securities and Markets Authority ('**the ESMA**').[40] The ESMA classifies tokens under three different token types: (i) payment tokens, (ii) utility tokens, and (iii) asset tokens.

(i) Payment tokens are a means of payment for acquiring goods or services. The holder has no claim on the issuer. These tokens are virtual

[40] ESMA (n 18).

currencies in the true sense of the word. The most prominent example is Bitcoin.

(ii) Utility tokens are intended to provide access to a specific application or service but are not accepted as a means of payment for other applications.

(iii) Asset tokens represent assets such as debt or equity claims on the issuer. Asset tokens promise, for example, a share in future company earnings or future capital flows. In terms of their economic function, asset tokens are thus analogous to equities, bonds or derivatives. Tokens which enable physical assets to be traded on the blockchain also fall into this category.[41]

As per the ESMA classification, CUBER was certainly not a utility token because its purpose was to be used as a general means of payment. This leaves the categories of payment token (since CUBER was used as a means of payment in the form of a deposit) and asset token (since CUBER served as a certificate of deposit). However, a payment token does not represent a claim against the user. CUBER, in contrast, represented a claim against LHV and would thus, not qualify as a payment token. Next, it would be redundant to categorise CUBER as an asset token since it represented nothing more than the par value of the fiat currency that it was issued against. The only difference is that CUBER relied on a decentralised Bitcoin blockchain-based infrastructure rather than a centralised bank infrastructure to make payments. Therefore, CUBER should not be qualified as any of the above token categories and must merely be regarded as a representation of the deposited funds in the bank account.

In summary, the authors argue that CUBER should not be qualified as e-money as this requires LHV to apply the e-money institution regime over and above the credit institution regime, and no additional legal certainty is achieved through such overlap. Furthermore, CUBER represented claims against LHV and not the LHV start-up, and LHV being a licensed credit institution was authorised to issue e-money according to Section 6(7)(3) of the PIEIA.

The fact of the matter is that CUBERs merely mirrored bank account deposits and the novel infrastructure (Bitcoin blockchain) used for paying with these deposits should not trigger additional legal norms, as this would run afoul of the technology neutrality principle. Any contrary approach would be analogous to saying that a car travelling on a private road

[41] Securities and Markets Stakeholder Group (n 23).

(centralised infrastructure) should be treated somewhat differently than the same car travelling on a public road (decentralised infrastructure).

C. Was LHV or the LHV Start-up Under the Obligation to Apply for an E-Money License?

According to Section 14(1) of the PIEIA, a company wishing to operate as an e-money institution must apply for an e-money license. Section 7(1) of the same act states that an e-money institution is a public or private limited company, the permanent activity of which is the issuance of e-money in its name. CUBER can be considered as a representation of deposits and it does not qualify as e-money, pursuant to Section 6(6) of the PIEIA. Consequently, there is no requirement to obtain an e-money license from the FSA for the CUBER application. Further, the LHV start-up was not subject to the obligation to apply for an e-money license because it was not the issuer of CUBER – which, in fact, was LHV.[42]

Even assuming that CUBER was indeed e-money and that the LHV start-up was its issuer, there was still no obligation to apply for an e-money institution license, due to the exemption in the law for a float limit of 500,000 euros. Section 12(1)(1) of the PIEIA provides that e-money service providers whose average outstanding e-money does not exceed 500,000 euros are exempt from the requirements of the act. In case of CUBER, the outstanding e-money was planned to be in the amount of 100,000 euros.

Finally, CUBER represented claims against LHV and not the LHV start-up, and the bank being a licensed credit institution was also not under any obligation to apply for a separate license for issuing CUBER because Section 6(7)(3) of the PIEIA permits the issuance of e-money by credit institutions.

D. The Origin of the Limitations Stated in Section 6(5) of the PIEIA

To the knowledge of the authors, the qualification of CUBER as e-money was not contested by LHV. According to Mr Haab,[43] the FSA interpreted each

---

[42] "*OÜ CUBER TECHNOLOGY offers an innovative solution for using CUBERs – the CUBER APP application. The CUBER APP allows to use CUBERs in payment for goods and services purchased from merchants who have joined the programme, or for transfer to other CUBER APP users. (...) A customer relationship with AS LHV Pank shall only be required if CUBERs are to be acquired from or redeemed by AS LHV Pank.*" *See*, cuber (n 39).

[43] Email of Mr Haab to the authors (19 October 2017) (held with the authors). The authors contacted the FSA to confirm this interpretation, but they have not responded to this

user's mobile device with the CUBER application to be a separate e-money device, and since the CUBER application was considered a rechargeable e-money device under Section 6(5) of PIEIA, this meant that only up to 2,500 euros of e-money per mobile device was allowed to be stored on the application during a calendar year. This was a considerable hindrance on the use of the CUBER application and as per Mr. Haab, the project proved to be unviable with such limitation.

In examining the source of this limitation, we find that it originated in the current E-Money Directive. However, these specific articles[44] were directed at transposing amendments to the 3rd Anti-Money Laundering Directive[45] and should instead have been transposed into the Money Laundering and Terrorist Financing Prevention Act of Estonia.[46] The respective Directive transposition conformity assessment[47] leaves the transposition of the respective article outside the scope of analysis because, in our understanding, its transposition can only be assessed under a conformity assessment of the 3rd Anti-Money Laundering Directive.

Instead, in Estonia, the Ministry of Finance transposed these limitations in 2011 into the PIEIA and repealed these only in 2018.[48] The repeal entered into force on 13 January 2018 and its explanatory note stated:

---

request or published the documentation on this interpretation.

44 E-Money Directive, art 19: Member States may allow the institutions and persons covered by this Directive not to apply customer due diligence in respect of:

Electronic money, as defined in point 2 of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions where, if it is not possible to recharge, the maximum amount stored electronically in the device is no more than EUR 250, or where, if it is possible to recharge, a limit of EUR 2500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1000 or more is redeemed in that same calendar year upon the electronic money holder's request in accordance with Article 11 of Directive 2009/110/EC. As regards national payment transactions, Member States or their competent authorities may increase the amount of EUR 250 referred to in this point to a ceiling of EUR 500.

45 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, now repealed by the E-Money Directive.

46 *See*, for the origin of the limitation, E-Money Directive, art 19(2).

47 Tipik Communication Agency SA, 'Conformity Assessment of Directive 2009/110/EC Estonia' (Final Report Version 2.0, 8 February 2013) <https://ec.europa.eu/info/file/69755/download_en?token=6RBYX0bl> accessed 10 February 2020.

48 With amendments transposing Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC, OJ L 337.

> It has appeared by now that these limitations may be disproportionate as until today not a single e-money institution license has been issued in Estonia.[49]

This shows that a considerable hindrance existed on e-money institutions for 7 years, without any basis in the relevant EU law and without a challenge from entrepreneurs or courts.

The following section investigates the compliance of the said limitation with the principle of technology neutrality.

V. Was the Limitation in Section 6(5) of the PIEIA Technology Neutral?

The dichotomy between regulating performance and regulating design is the cornerstone of the principle of technology neutrality. "*Technology neutrality's lodestar is intent to regulate behaviour, not technology; to worry about what occurs, not how it occurs*."[50] The e-money definition attempts to regulate performance because the conditions listed are not limited to one technology, but rather, to behaviour, i.e., it regulates the issuance of stored monetary value, its use and acceptance.

However, by applying Reed's classification of technology neutral regulation to Section 6(5) of the PIEIA, we find that this clause introducing a monetary limit for e-money devices was neither technology indifferent, implementation neutral nor potentially neutral.

Section 6(5) did not fulfil the criteria of *technology indifference*. The small monetary limits were set only for e-money devices, i.e., the Section targeted online forms of money, specific to e-money institutions. In contrast, payment accounts of payment institutions did not have any monetary limits, and even money remittance, which did not require a payment account, was not subject to monetary limitations per user.

Implementation neutrality was also not followed by Section 6(5). Reed argues that "*(the choice) to regulate the issuance of e-money, rather than the provision of e-payment services, was one of the reasons why this legislation*

---

[49] Ministry of Finance of the Republic of Estonia, *Opinion of the Ministry of Finance on the Bill on Amendments to the Payment Institutions and Electronic Money Institutions Act and Related Acts 498 SE* (nr 1.1-10/991-1, 11 October 2017) <https://www.riigikogu.ee/download/a9de2a31-3261-41b0-8626-c390d38014f3> accessed 10 February 2020 (in Estonian).

[50] Brad A Greenberg, 'Rethinking Technology Neutrality' (2015) 100 Minnesota Law Review 1495.

(e-Money Directive) was not implementation neutral." Following the same line of argumentation, only e-money devices face monetary limits due to a norm that specifically regulates e-money devices instead of regulating a wider category of e-payment wallets.

Potential neutrality was equally affected by Section 6(5) because the monetary limits were a restrictive requirement that did not have an identifiable purpose. Technologies would be unable to adapt to the monetary limits when there was a competing regime for payment institutions that did not have similar limiting requirements.

The limitation also fails to comply with van der Haar's *non-discrimination rationale* – that regulation must not favour one technology over the other, as otherwise, discriminatory rules would distort competition and the market. The simple fact of using fiat currency online (since CUBERs represented the money deposited in the bank account) caused the limitation to apply. Further, van der Haar´s rationale of *sustainability* requires regulation to be flexible and open to technological change. One may conclude that the limitation was flexible as it recognised rechargeable and non-rechargeable devices. However, the limitation failed to satisfy the sustainability rationale as it was static and non-responsive to changing market conditions. Further, Estonia's Ministry of Finance itself recognised that the limitation was disproportionate and consequently, inflexible to technological innovation.

Lastly, Section 6(5) fails the rationale of the natural persons' perspective, called the *denominated consumer certainty* rationale. As per this, when services are considered by consumers as interchangeable, technology neutrality would require that those services be regulated in a similar manner. The usage of funds on one's account through a mobile application built on Bitcoin blockchain is certainly interchangeable, from a consumers' perspective, with the usage of an Internet banking application through a centralised banking system, and consequently, these services should be regulated in a similar fashion.

VI. Conclusion

In this article, we have taken up a case study of the CUBER application and have applied the principle of technology neutrality to a specific section of the PIEIA and its implementation on CUBER. In analysing the CUBER model, we conclude that CUBER should not have been considered as e-money under the E-Money Directive and the PIEIA, as it served no purpose other than payment in fiat currency, and that therefore, it should not have been

subjected to more restrictive limitations, merely due to a difference in the infrastructure used in the cycle of payment.

Even assuming that CUBER did qualify as e-money, the LHV start-up would not require a license from the FSA as it offered an application for using CUBERs in payment for goods and services and was not the issuer of CUBERs. LHV, being a licensed credit institution, would also be exempt from the requirement of an e-money license as per Section 6(7)(3) of the PIEIA.

Finally, we conclude that Section 6(5) of the PIEIA was either erroneously transposed into national law or cautiously implemented in a very restrictive manner, which was non-compliant with the principle of technology neutrality. A monetary limitation on e-money devices, as opposed to no similar limitation on funds in bank accounts, discriminates against the medium and creates a substantial and unjustified imbalance between the e-money institutions regime and the credit institutions regime.

It's Raining Crypto: The Need for Regulatory Clarification When it Comes to Airdrops

Carol R. Goforth[*]

ABSTRACT *Worldwide regulatory restrictions have pushed crypto entrepreneurs to take creative and novel approaches in their struggle to create viable user networks for new tokens. One of the most interesting vehicles for dispersing tokens is the 'airdrop', a process by which a developer essentially 'gives away' tokens. The developers' motives in these airdrops are typically not completely altruistic. Instead, the goal is to increase the 'buzz' about new forms of crypto, and to encourage recipients to voluntarily promote the token that they now also own. The regulatory reaction to this technique has been mixed. A few nations, most notably China, have banned airdrops. Most other countries, however, have been less drastic and more ambiguous in their responses. This article lays out some of the current reactions to crypto airdrops and explains why it generally does not make sense not to treat them as involving the distribution of a security. Only where the airdrop crosses the line and requires more than a token effort (no pun intended) is regulation warranted. Where that line should be drawn is left to individual nations.*

[*] Carol R. Goforth is a University Professor and the Clayton N. Little Professor of Law at the University of Arkansas, in Fayetteville, Arkansas, USA. She has decades of experience with corporate, securities, and business law issues in the US, and has recently published a number of articles and blog posts dealing with the regulation of crypto transactions.

I. Introduction

Crypto[1] has grabbed the attention of some of the world's great entrepreneurs and financiers.[2] Billions of dollars have been (and continue to be) raised in so-called initial coin offerings ('**ICOs**') around the world.[3] Given the amount of money involved, it is not surprising that most governments have looked at how they should approach cryptoassets in general, and ICOs in particular. As should be expected, however, different jurisdictions have taken a wide variety of regulatory approaches to public distribution of these new assets.[4] All of those approaches are continuing to evolve, and most of them are quite complex. Many nations are tentatively welcoming, but several others are also overtly hostile to crypto. Considering the potentially global nature of cryptoassets, the regulatory environment for the same is

---

1 This Article assumes basic familiarity with crypto and therefore does not go into a detailed explanation of terms. If this kind of background is appropriate, see Carol Goforth, 'The Lawyer's Cryptionary: A Resource for Talking to Clients About Crypto-Transactions' (2019) 41 Campbell Law Review 47, 51.

2 For example, Vitalik Buterin is the inventor and co-founder of Ethereum. He helped create Ether when he was 19 years old and now has a personal net worth estimated to be between $100 and $200 million; Daniel Larimer founded Bitshares, Steemit, and EOS, and is probably worth between $600 to $700 million. They are both clear believers in crypto - '10 BlockchainPioneers Leading the Cryptocurrency Industry Forward' (*Medium*, 18 October 2018) <https://perma.cc/8USP-C9QQ> accessed 27 February 2019.

Nor are proponents of Bitcoin limited to tech entrepreneurs, Howard Schults, Starbucks Corp. Chairman and founder is quoted as saying that he believes '*we are heading into a new age in which blockchain technology is going to provide a significant level of a digital currency that is going to have a consumer application*.' See 'Bitcoin Bulls and Bears- Who's Hot, Who's Not on Crypto' (*Bloomberg*, 27 February 2019) <https://www.bloomberg.com/features/bitcoin-bulls-bears/> accessed 27 February 2019.

Naturally, not all of the attention has been positive. U.S. billionaire Charles Munger, vice-chairman of Berkshire Hathaway, has called Bitcoin a "*noxious poison*" - Julia Kollewe, 'Bitcoin is "noxious poison", says Warren Buffett's investment chief' (*The Guardian*, 20 February 2018) <https://perma.cc/L86E-VPL9> accessed 27 February 2019. In fact, many noted economists are highly skeptical (at best) of crypto. *See* Sead Fadilpašić, 'What Six Nobel Laurate Economists Have to Say About Crypto' (*CryptoNews*, 31 March 2018) <https://perma.cc/M9WM-LGR7> accessed 27 February 2019. Again, not all economists have been this negative. Semil Shah, 'Iterations:How Five Real Economists Think about Bitcoin's Future' (*TechCrunch*, 2013) <https://perma.cc/T993-L53B> accessed 27 February 2019.

3 The precise amount differs depending on the source. ICODATA.IO reports that there were 1257 ICOs in 2018, raising a total of $7,852,477,043 – See 'Funds raised in 2018' (*ICODATA*, 2019) <https://perma.cc/UC4Z-VYWF> accessed 27 February 2019. On the other hand, Bloomberg reported in November, 2018 that other sources suggest the total should be more than $22 billion - Justina Lee, 'How Much Have ICOs Raised in 2018? Depends on Who You Ask' (*Bloomberg*, 5 November 2018) <https://www.bloomberg.com/news/articles/2018-11-05/how-much-have-token-sales-raised-in-2018-depends-on-who-you-ask> accessed 27 February 2019.

4 For a consideration of five of the most common approaches taken by governments with regard to ICOs, see Danny Medina, 'How Governments are Reacting to ICOs' (*CoinDesk*, 3 December 2017) <https://perma.cc/89E5-U6RL> accessed 27 February 2019.

particularly challenging. What further complicates an already-bewildering array of regulatory requirements is innovation. While regulators struggle to keep up with the ICOs of yesterday, enterprising crypto-entrepreneurs are already experimenting with the next 'big thing'. Currently, it is the airdrop that has captured the imagination of the crypto-community.[5] (As will be described in more detail in Section II of this article, an airdrop is a means of disseminating cryptoassets by which the developer 'drops' the assets into qualifying crypto wallets, rather than selling them in an IPO or other alternative manners of distribution.)

Section II of this article will consider the nature of airdrops, what they do, how they work, and why entrepreneurs are increasingly using them despite regulatory uncertainty. Section III will consider the extent to which airdrops are true 'give-aways', where nothing is expected of persons acquiring the airdropped coin or token. Section IV will very briefly consider some of the concerns that have been raised with regard to airdrops. The article will then consider a limited number of the currently-existing regulatory regimes, assessing the direction in which various nations or nation-groups are progressing with their crypto regulations, as well as the current uncertainties with regard to airdrops. While only a limited number of nations have been considered, in order to make this material more accessible, national approaches have been broadly broken into three categories: nations that have some existing regulatory provisions but their treatment of airdrops is unclear (section V of this article); nations that are undecided about crypto generally and therefore have nothing on the books about airdrops (section VI of this article); and nations that are hostile towards crypto and either explicitly or presumably towards airdrops as well (section VII of this article). Finally, this article will conclude with some suggestions for how regulators in various nations might constructively approach crypto airdrops.

II. What are Airdrops?

'Airdrop' is not a regulatory term of art, but instead entered popular usage as crypto entrepreneurs turned to alternatives to public sales in order to disseminate their tokens. With regulatory authorities cracking down on unregistered coin and token distributions in the form of ICOs, and as social media sites have restricted or prohibited the advertising of ICOs, alternative distribution methods have become increasingly important. According to various

[5] *See* generally Brady Dale, 'So Long ICOs, Hello Airdrops: The Free Token Giveaway Craze Is Here' (*CoinDesk*, 17 March 2018) <https://perma.cc/H2DU-7RDN> accessed 27 February 2019.

commentators, "*[a]irdrops can be defined as the process whereby a cryptocurrency enterprise distributes cryptocurrency tokens to the wallets of some users free of charge. Airdrops are usually carried out by blockchain-based startups to bootstrap their cryptocurrency projects*."[6] The critical component of the process is that the distribution of coins or tokens is essentially free to the recipient. One source reports that Jun Hasegawa, Chief Executive Officer of Omise, claims to have pioneered the process on Ethereum in August, 2017.[7]

This article will use the term 'airdrop' to refer to a distribution of a cryptocoin or token in a manner that requires no or very little effort from the recipient and involves no exchange of tangible consideration in the form of fiat or other cryptocurrencies. Any 'contribution' from the recipient is to be evaluated based on what it costs the recipient in terms of time and effort, and not from the value to the issuer (for reasons that will be explained later). This definition is intended to be useful in both considering the question of how airdrops should be regulated, and consistent with the general understanding of airdrops in the crypto-community.

Note that not all airdrops are conducted at the beginning of a coin or token's existence. There exist precursors to the current form of airdrops on which this article focuses, in the form of distributions following hard forks where a change to the underlying programming was a adopted by some but not all participants on a given blockchain.[8] (Where a change is not adopted unanimously, the result may be a chain with two 'forks', both of which exist moving forward.) Bitcoin, for example, has forked multiple times, resulting in the creation and 'airdropping' of a number of new coins derived from the original asset.

---

[6] Katalyse.io, Mission.Org, 'What are "Airdrops" in Crypto World?' (*Medium*, 15 February 2018) <https://perma.cc/DCN8-TB8E> accessed 27 February 2019 (this same source also notes that established blockchain-based enterprises such as trading platforms or wallet services can conduct airdrops as well).

[7] Dale (n 5).

[8] A hard fork (or split among nodes on a blockchain) usually occurs after discussion and disagreement among the development team behind a virtual currency and the mining and (sometimes) investing communities. If unanimity is not possible, a hard fork will be necessary. This means there will be two non-identical but related copies of the blockchain going forward. Typically, the original asset goes on as it has before, while the new iteration adopts some different protocols and adjustments to the code. It is also possible to have a hard fork that occurs not because of a dispute between developers and miners but is instead an attempt to create a different version of a preexisting coin. For additional discussion of hard and soft forks, see Antonio Madeira, 'The DAO, The Hack, The Soft Fork and The Hard Fork' (*CryptoCompare*, 26 July 2016) <https://perma.cc/9JNT-HX9L> accessed 27 February 2019.

The first significant Bitcoin fork was likely Bitcoin XT in 2014. This development was designed to increase the number of transactions per second.[9] While it initially appeared to be successful, with more than a thousand nodes running the new software by the summer of 2015, it has now fallen out of favour. The tokens created by that fork are, however, still available.[10] In early 2016, Bitcoin Classic was launched in another effort to increase block size.[11] Early interest was strong, with about 2,000 nodes participating. Bitcoin Classic has now ceased operations.[12]

In 2015, a soft fork was implemented on the Bitcoin blockchain to allow more transactions to occur at once. In response, some users initiated a hard fork to avoid certain protocol updates that would have been required. Bitcoin Cash ('**BCH**') was issued as a result of this change and split from the main blockchain in 2017.[13] Anyone who held Bitcoin at the time of the fork became an owner of BCH as well.[14]

These kinds of transactions paved the way for the modern airdrop, as a fork is not required in order for a cryptoasset to be dropped into the wallets of crypto-users. Recognising this, one might ask why a developer or company with a new coin or token would be willing to give it away? There are, in fact, a number of valid strategies that could support such a decision.

A likely motive for token start-ups is to generate awareness of the new asset. There is more value when a token is held on as many wallets as possible, and more tokenholders create more interest, wider exposure, and an increased trading volume, particularly if there is enough interest and demand to have the interest listed on an exchange. In essence, an airdrop can be a virtually free way to conduct marketing and generate interest among members of the crypto community.

---

[9] For a further discussion of the history of Bitcoin XT, see Mike Hearn, 'An XT FAQ' (*Medium*, 27 August 2015) <https://perma.cc/6NJE-BNDX> accessed 27 February 2019. *See* also (*BXT*, 2019) <https://perma.cc/RQ4G-W6G6> accessed 27 February 2019.

[10] 'BitTokens (BXT)' (*CoinMarketCap*, 25 February 2019) <https://perma.cc/L7BW-JPYP> accessed 25 February 2019 (showing a market capitalization of $316,597 as of February 25, 2019).

[11] For a discussion of Bitcoin Classic (and the other Bitcoin hard forks), see Nathan Reiff, 'A History of Bitcoin Hard Forks' (*Investopedia*, 25 April 2018) <https://perma.cc/D6ZA-NGJW> accessed 27 February 2019.

[12] Tom Zander, 'Bitcoin Classic Closing its doors' (*Bitcoin Classic News*, 2019) <https://perma.cc/N9SL-QR5P> accessed 27 February 2019.

[13] Reiff (n 11).

[14] For a description of this airdrop, see 'Bitcoin cash (BCC)' (*Airdropalert*, 2019) <https://perma.cc/95NC-5D9R> accessed 25 February 2019. BCH is the most successful hard fork of Bitcoin, and as of the end of February, 2019, is the sixth-largest cryptocurrency by market capitalisation showing Bitcoin Cash with a market cap in excess of $2.4 billion. (*CoinMarketCap*, 2019) <https://perma.cc/9QS9-H6BZ> accessed 25 February 2019.

In addition, an airdrop can be used to more evenly distribute token supply, which is a particular benefit in a blockchain system. It can also help generate a lead database or network before a more public distribution goes live. Alternatively, depending on how it is conducted, it can also be used to reward early or loyal investors or participants in a venture. It certainly is one way to gain entrance into, and interact with the existing crypto community.

The benefits are real, because once someone holds a token they have the same motive as everyone else who owns the token or intends to invest in it — the incentive is to see that the value of the token increases. Whether by word of mouth or by virtue of the fact that people tend to value something that they own more highly than if they have no connection with it, this is a powerful way to improve token value.

However, modern economic commerce is sometimes summarised by the slogan that 'There ain't no such thing as a free lunch.' Given this reality, it is fair to look more closely at these 'free tokens.' While developers do often drop their tokens into wallets for no explicit transfer of consideration and no payment of fiat or other crypto currency, are airdrops really 'free'?

III. Are Developers and Companies really "Giving" away their Tokens?

Even sources geared at defining what constitutes an airdrop acknowledge that some distribution schemes that characterise themselves as airdrops are not completely free, at least of effort, for the recipient. For example, while noting that crypto airdrops generally refer to a distribution of 'free tokens', one source also explains that "*[t]o qualify for this free gift, one may need to perform certain tasks that include posting on social media forums, connecting with a particular member of the blockchain project, or writing a blog post.*"[15]

All airdrops require that a recipient already have a wallet that can accommodate different types of cryptocurrency. Most wallets will handle tokens that are likely to be dropped.[16] The requirements for wallet type and storage vary by project, and in some cases can be satisfied with an online soft wallet, and in some instances will need to be a wallet residing on a particular

---

[15] CoinBundle Team, 'What Are Airdrops' (*Medium*, 14 September 2018) <https://perma.cc/U5SE-TUPJ> accessed 27 February 2019.

[16] Crypto Coin Junky, 'Beginners Guide to Crypto Airdrops: Free Coins & Tokens' (*Medium*, 5 October 2018) <https://perma.cc/SB9S-CG3K> accessed 27 February 2019 (suggesting a wallet that will accommodate several different types of Ethereum Request for Comment number 20 tokens). Note that airdrops may also occur on other blockchains, such as EOS.

exchange. In addition, the wallet must be active (i.e., it must both hold a minimum level of some form of cryptocurrency before the date set by the project, and demonstrate some level of activity), to avoid the creation of multiple wallets solely to claim airdropped coins or tokens.

However, some airdrops require more than an active wallet. The project may require a recipient to do one or more of the following to participate: sign-up; retweet; refer a friend; join the project's Telegram account; join the project's discord chat; post a comment or private message about the project; or complete other social media tasks geared at spreading the word about the project.[17]

There is even terminology to distinguish between a truly 'free' airdrop and one that requires specific protocols to be followed. An 'automatic airdrop' does not require the recipient to do anything other than hold a suitable, active wallet. A 'manual' airdrop is one where specific requirements are imposed in the protocol devised by the project developers.[18] Alternative nomenclature sometimes refers to programs that require more substantial efforts from recipients as 'bounty programs', rather than airdrops. Usually these require completion of specific tasks or jobs, such as creation of new graphics, translations, marketing and promotion for the project, or writing content.[19] The line between airdrops and bounties is, however, unclear.

In a pure airdrop, however, the recipient 'pays' nothing and invests little in the way of time or effort. If it is automatic, the recipient does not even have to know that they are receiving the crypto. This would, at first glance, seem to be a situation where little is needed in terms of regulation. The recipient is not 'investing' anything, and therefore does not stand to lose any money or much, if any, time. The developer is not gaining any new currency with which to conduct illicit operations. These facts, however, do not mean that there is no reason for caution. Airdrops can still be abused.

---

[17] These potential tasks are discussed in sources such as Sudhir Khatwani, 'Airdrops In Cryptocurrencies: Everything A Beginner Needs To Know' (*CoinSutra*, 13 October 2018) <https://perma.cc/MAE9-PANZ> accessed 27 February 2019.

[18] *See* Marko Vidrih, 'Airdrops—What exactly is an Airdrop?' (*Medium*, 12 June 2018) <https://perma.cc/8WM9-7YA6> accessed 27 February 2019.

[19] *See* generally Winco, 'What is the difference between Faucets, Airdrops, and Bounties?' (*Good Audience Blog,* 10 October 2018) <https://perma.cc/V6WP-SZ68> accessed 27 February 2019. Although not directly relevant to this article, a 'faucet' is a website that offers very small increments of crypto in exchange for periodic visits or tasks over an extended period of time, usually as an incentive to help that site generate advertising income.

IV. Reasons to be Careful

There are a number of reasons for investors to be cautious and regulators to be concerned about airdrops. As is the case with any innovation, unscrupulous players have been quick to enter the field.[20] One risk is that a scammer may create a fake Twitter account that mimics an official cryptocurrency company's account. The fake account then poses as a developer for the team and requests private wallet keys,[21] ostensibly in order to airdrop coins. Alternatively, a Twitter account that resembles a legitimate company may generate a request that a target send cryptocurrency to a wallet owned by the fraudster, again in order to receive the 'free' tokens.[22] This can be done along with a promise that the transferred tokens will be returned and assurance that this is only a test to ensure that the wallet is active. There are a range of phishing, hacking, and identity theft scams that could be carried out with airdrops,[23] typically with regards to requests for information, account access, or payments that are not required in genuine airdrops.

From the perspective of the project, the lack of clarity from regulators is another reason for caution. When regulations do not clearly address the requirements applicable to airdrops, even legitimate companies acting in good faith run the risk of finding themselves in trouble with regulatory authorities down the road.

It must be noted that there are some risks often mentioned in connection with crypto that are not mentioned here. For example, one of the mostly commonly cited concerns has to do with the risk that crypto is being used for illicit purposes (either for money laundering or to finance illegal operations such as those involving terrorist activities).[24] If an airdrop does not involve the transmission of any property of value to the developer in exchange for

---

[20] For a more detailed consideration of the kinds of airdrop scams, see Alex Lielacher, 'A Guide to Airdrops Part 3: Airdrop Scams' (*BTCManager*, 26 March 2018) <https://perma.cc/U9Y9-VFFX> accessed 27 February 2019.

[21] A private key is the cryptographically protected access code that allows an owner to access his or her wallet; it is not designed to be shared with third parties. For a substantially more sophisticated explanation of public and private keys, *see* Leon Di, 'Why Do I Need a Public and Private Key on the Blockchain?' (*WeTrust*, 29 January 2017) <https://perma.cc/SE4B-MYEP> accessed 27 February 2019.

[22] Note that these kinds of things raise red flags. Private keys are never required by legitimate companies, and no airdrop requires that tokens be sent to another address first. Ideally, before taking any affirmative steps in response to an offer of airdropped coins or tokens, official sources should be checked.

[23] Crystal Stranger, 'Airdrops: the Good, the Bad, and the Scammy' (*Medium*, 7 September 2018) <https://perma.cc/T7D9-UWGX> accessed 27 February 2019.

[24] 'Regulation of Cryptocurrency Around the World' (Law Library of Congress, June 2018) 1 <https://perma.cc/T7NJ-GN3Y> accessed 27 February 2019.

crypto, neither of these would seem to be an issue with airdrops per se. This does not, of course, mean that secondary trading transactions could not cause problems, but the airdrop itself should not contribute to this particular problem.

These facts lead to the question of how nations are reacting to the new development. Not surprisingly, the development has engendered all kinds of reaction (and non-reaction). Some countries are generally welcoming to crypto, and therefore are more likely to be responding in a potentially positive or informative way to airdrops. Some nations are hostile to crypto generally, and these jurisdictions generally are not in favor of airdrops either. However, because initial regulations did not anticipate or explicitly address the airdrop phenomenon, the majority of countries have yet to indicate how they intend to reaction. For this reason, among others, it is useful to look at how countries are, in general terms, responding.

V. State of Regulation — Unclear or Ambiguous

While it is exceedingly difficult to make blanket statements about crypto because of the myriad regulatory schemes and approaches, it is generally safe to say that current regulation of airdrops is both complicated and confusing. A number of nations have some regulatory pronouncements in place, but their application is either in the process of evolving or, at best, unclear as to airdrops.

The United States ('**U.S.**') is one of the nations that have a regulatory system that it is attempting to apply to crypto, but has not decided on precise or definitive guidelines. In general terms, crypto entrepreneurs operating in the U.S. seem to be most concerned with whether airdrops will be treated as a distribution of securities and therefore within the purview of the U.S. Securities and Exchange Commission ('**SEC**'). Under the current approach taken by the SEC, crypto is generally a security if it: (1) involves the investment of money or something of value; (2) is in a common enterprise; (3) is carried out with the expectation of profits; (4) is based on the essential entrepreneurial efforts of others.[25] Airdrops could easily be found to lack the first element, meaning that they should not be treated as involving the distribution of a security.[26]

---

[25] That test is known as the Howey investment contract test ('**Howey**'), and it was first established by the U.S. Supreme Court in *Securities & Exchange Commission v W.J. Howey Co.*, 1946 SCC OnLine US SC 95 : 90 L Ed 1244 : 328 US 293 (1946).

[26] The consequences of being treated as a security are outside the scope of this Article. For a more detailed assessment of securities treatment of crypto, see Carol R. Goforth, 'Securities

However, the fear is that the SEC will treat crypto airdrops as securities in much the same way that it warned against giveaways of stock in 1999.[27] In addition, on August 14, 2018, the SEC issued a cease and desist order (the '**Tomahawk Order**') against a company and its founder for actions in connection with an ICO of 'Tomahawkcoins' or 'TOM' tokens.[28] In the Tomahawk Order,[29] the SEC found that the issuer's 'Bounty Program' constituted an offer and sale of securities because the company "*provided TOM to investors in exchange for services designed to advance Tomahawk's economic interests and foster a trading market for its securities.*"[30] The lack of cash payment did not prevent the distribution from involving securities, because the company "*received value in exchange for the bounty distributions, in the form of online marketing…*".[31] Some sources were quick to treat this as a potential condemnation of airdrops,[32] although the company called it a bounty program, and a degree of effort was required to participate.

Further complicating matters, in the spring of 2019, the SEC issued a substantially expanded framework for determining how the conventional investment contract analysis should apply to digital assets.[33] As SEC Commission Hester Peirce has noted in her commentary on the new framework "*[w]hile Howey has four factors to consider, the framework lists 38 separate considerations, many of which include several sub-points.*"[34] Included in that extensive, multi-factor framework is a very brief, and not very helpful, footnote on bounties and airdrops. With regard to airdrops in particular, the framework contends that "*the lack of monetary consideration for digital assets, such as those distributed via a so-called 'air drop,' does not mean*

Treatment of Tokenized Offerings Under US Law' (2019) 46 Pepperdine Law Review 405.

27 *See* 'SEC Brings First Actions To Halt Unregistered Online Offerings of So-Called "Free Stock"' (*US SEC*, 22 July 1999) <https://perma.cc/8TAT-7PEE> accessed 27 February 2019.

28 US SEC, Press Release, 'SEC Bars Perpetrator of Initial Coin Offering Fraud' 2018-152 (*US SEC*, 14 August 2018) <https://perma.cc/G2G2-3N2P> accessed 27 February 2019.

29 A copy of the Tomahawk Cease and Desist Order is archived at <https://perma.cc/3ZGB-BD79> accessed 27 February 2019.

30 The specific things for which 'bounties' were offered included things such as '*as making requests to list TOM on token trading platforms, promoting TOM on blogs and other online forums like Twitter or Facebook, and creating professional picture file designs, YouTube videos or other promotional materials*.' Tomahawk Order (n 29) 21.

31 Tomahawk Order (n 29) 34.

32 Robert Wernli, Jr., Robert Weber, and Osama Khan, 'Airdrop of Crypto Tokens Hits Regulatory Flak' *Sheppard Mullin* (2018).

33 SEC, 'Framework for "Investment Contract Analysis of Digital Assets"' (SEC, 3 April 2019) <https://perma.cc/J4KQ-HW52> accessed 8 April 2019.

34 Hester Peirce, 'How we Howey' (*US SEC*, 9 May 2019) <https://perma.cc/729A-CG6C> accessed 10 May 2019.

that the investment of money prong is not satisfied; therefore, an airdrop may constitute a sale or distribution of securities."[35]

This statement does not negate the first element of *Howey*, and if the matter is ever litigated, American courts may well find that an automatic airdrop lacks the requirement that an investment contract be predicated on the contribution of money or value, meaning that it will not be the sale of a security. Because this has not yet occurred, U.S. law on airdrops is unclear, especially since stock is different from crypto,[36] and the effort required of token recipients in the Tomahawk situation was substantially greater than generally expected in a true airdrop.[37]

As is the case in the U.S., the European Union ('**E.U.**') securities market regulator, the European Securities and Markets Authority, ('**ESMA**') has yet to definitely suggest to member nations whether or how airdrops should be regulated.[38] Based upon how ESMA would treat ICOs, an airdrop would have to involve the offer of a transferable security. If a true utility token is involved, there is a good argument that there is no transferable security. A truly automatic airdrop is likely to not involve an 'offer', and there may be broad exemptions if the value of any consideration is less than 100,000 Euros. To reach these conclusions, various definitions and rulings have to be made outside the context of airdrops.

'Transferable security' is defined broadly by a parliamentary directive to included "*classes of securities negotiable on the capital market*", not including instruments of payment, but including company shares, units of securitized debt, and securities "*giving the right to acquire or sell any such*

---

[35] SEC (n 33) 9.

[36] *See* Dale (n 5), citing Todd Kornfeld, counsel at the Pepper Hamilton LLP law firm, as expressing concern based on SEC actions from 1999 that targeted giveaways of free equity interests. This source reports that Stream, a blockchain-based video streaming platform, '*delayed its airdrop indefinitely because of concern that airdrops could also be in violation of securities law.*' However, stock is always treated as a security under US law while crypto must satisfy the Howey investment contract analysis, which among other things looks at whether there is an investment of money or something else of value.

[37] This is the first element of the investment contract test as set forth by the US Supreme Court in *Howey*. This is the current test utilised by the SEC to determine whether or not crypto transactions involve the sale of securities. Note that this is not the test for determining whether equity is a security. In fact, under current Supreme Court jurisprudence, equity interests in the form of stock are always a security. *Landreth Timber Co. v k. Landreth* 1985 SCC Online US SC 135 : 85 L Ed 2d 692 : 471 US 681(1985). The elements relevant to determining whether there is an investment contract do not apply in the case of stock, making the 1999 reaction by the SEC to stock giveaways largely inapplicable to crypto airdrops. See US SEC (n 27).

[38] 'Airdrops: Are free tokens free from regulation?' (*A&L Goodbody*, 4 June 2018) <https://perma.cc/Z89X-KBTA> accessed 28 February 2019.

transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures."[39] Presumably, a true utility token that has no possibility of appreciation or value other than the offered utility is not likely to meet this definition, but tokens marketed as investments would be. This should apply to airdrops as much as to ICOs.

If a token is a 'transferable security', anyone 'offering' it may be subject to various regulatory requirements, which raises the question of what constitutes an offering.[40] ESMA has previously considered the treatment of 'free' stock give-aways in a question and answer ('**Q&A**') publication intended to explain E.U. prospectus requirements that may be triggered when there is such an offer.[41] In the Q&A, ESMA indicates that "*where securities are generally allotted free of charge, no prospectus should be required.*"[42] While this appears to support the conclusion that airdrops (which are also free) do involve an offering, the ESMA position is not actually that clear-cut. The clarification from the not Commission Services was that there should be no 'offer' of securities where there is 'no element of choice', but that if the recipient 'decides' on whether to accept the security, it should be treated as an offer for no consideration.[43] However, the Q&A then suggests that there is also an exemption for offers of less than EUR 100,000.[44] Based on this reading, only truly automatic airdrops would seem to be excluded from the definition of an offering, but exemptions should apply because airdrops do not actually raise funds.

Adding complexity to this issue, however, is a recent pronouncement from ESMA. On January 9, 2019, ESMA published advice to E.U. institutions (the Commission, Council, and Parliament) that suggests that even crypto that is not a financial instrument should always be subject to anti- money laundering requirements, and similarly that all crypto should be accompanied by appropriate risk disclosures.[45] This leaves crypto entrepreneurs in the E.U.

---

[39] Directive 2014/65/Eu of the European Parliament and of the Council 2014, Tit. I, art 4 § 44.

[40] The parameters of such requirements are outside the scope of this Article, but they may include regulations under Markets in Financial Instruments Directive II, the Alternative Investment Fund Managers Directive, and the Fourth Anti-Money Laundering Directive. If there is an 'offer to the public', it would be subject to the prospectus requirements set out in the EU Prospectus Directive. See 'Airdrops: Are free tokens free from regulation?' (n 38).

[41] 'Questions and Answer- Prospectuses' (*ESMA*, January 2019) <https://perma.cc/NDJ9-RQTN> accessed 28 February 2019.

[42] ibid 13.

[43] ibid 13.

[44] ibid 13.

[45] Crypto-Assets Need Common EU-Wide Approach to Ensure Investor Protection (*ESMA*, 9 January 2019) <https://perma.cc/SQ6F-U3ZD> accessed 28 February 2019.

in much the same position as they are in the U.S. — uncertain as to law applicable to airdrops.

Of course, individual countries in the E.U. can also adopt positions on crypto. For example, in 2017, Switzerland issued guidance on the treatment of ICOs.[46] After noting that ICOs would need to be evaluated on a case-by-case basis, the Swiss Financial Market Supervisory Authority ('**FINMA**') suggested the following concerns that would impact whether particular regulations applied to ICOs:

i. The need to apply anti-money laundering requirements to token sales involving payment instruments or to regulate third parties such as crypto brokers and trading platforms carrying out secondary transactions.

ii. The need to apply banking requirements to ICO operators who accept public deposits.

iii. The need for persons acting as a securities dealer to comply with licensing requirements.

iv. The need to comply with collective investment schemes legislation if assets collected as part of the ICO are managed externally.

These concerns make it look like airdrops would not be subject to intensive regulation, given that no currency (fiat or digital) is paid to the issuer, there are no public deposits, no one is acting as a dealer, and there is no investment of assets at all. On the other hand, FINMA has also claimed that asset tokens and utility tokens that have any investment function are to be treated as securities,[47] potentially complicating matters. Only true cryptocurrencies that act purely as payment tokens, or utility tokens that provide access and have no investment potential, would be outside the definition of 'security' if this approach is taken. This leaves Swiss law in a state of uncertainty similar to that which exists in the U.S. and the rest of the E.U.

Singapore is another nation with regulations for crypto (referred to there as digital tokens) that do not specifically mention airdrops. The Monetary Authority of Singapore ('**MAS**') updated guidelines applicable to digital token offerings in 2018.[48] The current guide suggests that an offer "or issue"

---

[46] 'Regulatory Treatment of Initial Coin Offerings' (FINMA Guidance 04/2017, 29 September 2017) <https://perma.cc/BW46-C7UL> accessed 28 February 2019.

[47] 'FINMA publishes ICO guidelines' (*FINMA News*, 16 February 2018) <https://perma.cc/FW9B-EHH9> accessed 28 February 2019.

[48] 'A Guide to Digital Token Offerings' (*MAS*, November 2018) <https://perma.cc/9N-HK-QM8A> accessed 28 February 2019.

of digital tokens that are regulated as securities must comply with securities laws.[49] The Singapore Securities and Futures Act ('**SFA**') 'interprets' security to include shares representing legal or beneficial ownerships in certain businesses, or debentures, but does not include units of a collective investment scheme ('**CIS**'),[50] which is what a token-based ecosystem is likely to involve.[51] On the other hand, tokens that are true cryptocurrencies are generally not securities, at least according to Case Study 6 in the MAS Guide, which references an understanding that digital payment systems like Bitcoin are not securities or units in a CIS.[52] On the other hand, the MAS guidelines then say that if the digital token is either a security or units in a CIS, then all offers must be made in accordance with the registration requirements of the SFA. Unfortunately, neither the SFA nor the new guidance interprets or explains what constitutes an 'offer'.

The strongest authority for suggesting that airdrops should not be problematic in Singapore comes from Case Study 8 in the MAS Guide. In that example, a company intends to sell tokens to fund development of a platform. The token is designed to give holders voting rights, but nothing else. In addition, the company will distribute the token as a reward based on use and activity on the platform. In assessing whether the securities laws would apply, MAS concludes that the token in question is not a share or debenture, and not a CIS because there is no manager. The explanation also says that "*[a]s the rewards are distributed in proportionate to investor's usage and activity on the platform, it does not represent a right to claim dividends or return on capital*."[53] In this case, there is at least the potential that the tokens could appreciate in value, and nothing in the example restricted resale of tokens. This did not, however, factor into the MAS' assessment of how to treat the token distribution, leaving the appropriate treatment of airdrops unsettled since the basis for the conclusion was that there was no manager, not that there was no consideration exchanged.

Finally, consider the case of Indonesia. Indonesia is in the very early stages of developing a regulatory paradigm for crypto. Indonesia's Futures

---

[49] ibid 2.1.

[50] Singapore Securities and Futures Act 2001, ch 289, s 2.

[51] A collective investment scheme involves arrangement in respect of any property where participants do not have day-to-day management control, and (among other options) the effect of the arrangement enables participants to receive returns from the property. Singapore Securities and Futures Act 2001, ch 289, s 2. If the benefit to a token holder is appreciation of the token by virtue of the efforts of the issuer or its managers, then this definition might be met.

[52] 'A Guide to Digital Token Offerings' (n 48) 13-14.

[53] ibid 16.

Exchange Supervisory Board ('**Bappebti**') announced in June of 2018 that digital currencies were tradable commodities,[54] and at that time indicated an intent to create a system of comprehensive regulation of crypto as a commodity. More recently, Bappebti announced new regulations on the implementation of physical markets for crypto assets in futures trading.[55] Those regulations apparently focus on mechanisms for crypto asset trading, starting from the opening of accounts and including crypto asset transactions.[56] The actual regulations, however, appear to focus on traders and exchanges, which require that brokers have at least 1 trillion rupiahs (USD 70 million) in their accounts, clearing houses need paid up capital worth at least USD 107 million, and traders need to make a deposit worth USD 6,000.[57] In addition, exchanges must employ at least one security expert and retain trading information for at least five years on a server located in Indonesia.[58] As might be expected with such a nascent regulatory framework, there is nothing indicating how airdrops will be treated or how issuers of crypto will be regulated.

This group of countries is broadly representative of nations that have crypto regulations in place. Regardless of how detailed the paradigm or structure is (and in some cases, such as for the U.S., it is very detailed), airdrops tend to be outside the settled rules. This leaves the brave or fearless (some might say foolhardy) entrepreneur with room to proceed with airdrops, while more compliant or risk-averse developers may be discouraged from proceeding with this process in these nations.

VI. State of Regulation — Uncertainty in the face of Silence

A second group of countries are still deciding on how to treat crypto. Until that initial decision is made, obviously there will be little in the way of specific guidance about how airdrops should fit into the regulatory regime.

---

[54] Mandy Williams, 'Indonesian Regulatory Body sets Cryptos as a Futures Trading Commodity' (*CryptoPotato*, 4 June 2018) <https://perma.cc/4T5W-KLDV> accessed 27 February 2019.

[55] See Jeffrey GoGo, 'Indonesia's Futures Regulator Issues New Rules for Crypto Assets' (*Bitcoin.com News*, 13 February 2019) <https://perma.cc/V8XC-ARFW> accessed 27 February 2019.

[56] 'Futures Exchange Authority Issues Regulation on Cryptocurrency' (*The Jakarta Post*, 13 February 2019) <https://perma.cc/YFY5-B47P> accessed 27 February 2019.

[57] Rahul Nambiampurath, 'Indonesian Regulator Accepts Bitcoin as Tradeable Commodity' (*BeinCrypto*, 16 February 2019) <https://perma.cc/N5P5-PUPL> accessed 27 February 2019.

[58] ibid.

For example, Russia created the Russian Association of Blockchain and Cryptocurrency, now known as the Russian Association of Cryptocurrency and Blockchain, in August 2017. Its purpose was to promote the development of blockchain technology and to offer regulatory options, but it has had little success in clarifying the state of law relating to crypto in Russia. In May 2018, three crypto bills passed the first reading in the State Duma (the lower house of the Federal Assembly of Russia), including Bill No. 419059-7, 'On digital financial assets'. That bill would have made cyptocurrencies and tokens property. It would also have banned circulation of crypto as a "*legal means of payment on the territory of the Russian Federation*." In addition, it did not contemplate the exchange of crypto for fiat; only tokens issued as part of domestic ICOs could be exchanged for 'real' money. A new Draft Bill circulated in October 2018 would allow owners of private companies to create 'digital financial assets'. However, the Russian newspaper Kommersant reported on November 30 that the Bill had been sent back to first reading because of 'significant changes'.[59] Hearings on the Bill were postponed until an unspecified date in 2019, which some sources suggest will take place within the first quarter of the year.[60] The new Bill is expected to tie together regulatory initiatives on crypto, crowdfunding, and investment platforms, but its final content has yet to be decided. As of the date this article was finished, Russia was suggesting that the new regulations would be adopted (at least in part) by the end of 2019.[61] Until this project comes together, it is virtually impossible to predict how Russia will decide to treat crypto or airdrops.

India is another nation in the undecided group, although until recently it might have been more aptly characterized as being unwelcoming to crypto. For some times, reports were widely circulated that cryptocurrency was 'illegal' in India.[62] The Reserve Bank of India ('**RBI**') formally stopped Indian

---

[59] Molly Jane Zuckerman, 'Russian Crypto Bill Draft Pushed Back to First Reading for Significant Edits' (*CoinTelegraph*, 1 December 2018) <https://perma.cc/G8RB-J6L6> accessed 27 February 2019.

[60] Ana Berman, 'Russian Parliament to Discuss Crypto Bill Within Two Months, Official States' (*CoinTelegraph*, 14 January 2019) <https://perma.cc/8XEL-KDY4> accessed 27 February 2019.

[61] Daniel Palmer, 'Russia May Allow Crypto Trading in Upcoming Legislation: Official' (*CoinDesk*, 24 June 2019) <https://perma.cc/ZU4F-7HLZ> accessed 12 August 2019. This deadline (by the end of 2019) may be more likely to be met, given that the head of the Duma Financial Market Committee, Anatoly Aksakov, has acknowledged that Russia must adopt some requirements by the end of the year '*in order to comply with recommendations from international watchdog, the Financial Action Task Force (FATF).*'

[62] William Suberg, 'Cryptocurrency "Illegal" In India Says Trade Organization Head' (*CoinTelegraph*, 26 October 2018) <https://perma.cc/YLS9-E6UQ> accessed 27 February 2019.

banks from dealing in crypto in April of 2018, and the Indian Supreme Court repeatedly postponed hearing challenges to that decision.[63] By the end of 2018, however, there were suggestions that the Indian government was considering the legalization of crypto, albeit with "*tough terms and conditions attached*".[64] On January 4, 2019, the RBI issued a report concluding that "*cryptocurrencies currently pose no threat to financial stability*".[65] Nonetheless, the RBI continued to emphasize its belief that "*cryptocurrencies need 'constant monitoring,' given their rapid expansion in recent years*."[66] On the other hand, an interdisciplinary committee set up to investigate crypto is not in favor of a ban, with an anonymous senior official reporting that "*[t]here is a general consensus that cryptocurrency cannot be dismissed as completely illegal. It needs to be legalized with strong riders*."[67] The most recent pronouncement from the country, till July 2019, comes from Anurag Thakur, India's Minister of State for Finance & Corporate Affairs, who recently explained that Bitcoin will be legal while government works on crypto regulations.[68] Until this actually happens, of course, the eventual status of things like airdrops is in the air.

Another nation yet to adopt crypto regulation is Brazil. In May 2019, the Brazilian President of the Chamber of Deputies (i.e., the federal legislative body, and lower house of the country's National Congress) ordered the creation of "*a commission to consider cryptocurrency regulation in the country*".[69] Two months later, however, a federal deputy in the National Congress (and a descendant of the former royal family of Brazil) publicly opposed any crypto regulation, suggesting that it was "*merely an example of the state intervening in something which is not its business*."[70] Until this is resolved, and regulations are adopted, the fate of crypto in general, and airdrops in particular, is uncertain in Brazil.

---

[63] Ana Berman, 'India: Central Bank Report States Crypto Does Not Threaten Financial Stability' (*CoinTelegraph*, 4 January 2019) <https://perma.cc/BAW9-P2GN> accessed 27 February 2019.

[64] Yogita Khatri, 'IndiaMay Legalize Cryptos But Under 'Strong' Rules: Report' (*CoinDesk*, 26 December 2018) <https://perma.cc/EMC7-M53Q> accessed 27 February 2019.

[65] Berman (n 63), citing RBI, 'Report On Trend And Progress of Banking In India 2017-18' (*RBI*, 28 December 2018) <https://perma.cc/3QL2-S8YB> accessed 27 February 2019. The references to risk posed by cryptoassets appear at pp 29-30 of that report.

[66] Berman (n 63).

[67] Khatri (n 64).

[68] Anja Van Oosterhout, 'Bitcoin Still Legal in India; Crypto Regulation in Works' (*Bitcoinist*, 19 July 2019) <https://perma.cc/2K45-WGCS> accessed 12 August 2019.

[69] Ana Alexandre, 'Brazil Establishes Committee for Cryptocurrency Regulation' (*CoinTelegraph*, 31 May 2019) <https://perma.cc/2VUT-ZKA2> accessed 12 August 2019.

[70] Ana Alexandre, 'Brazil: Member of Former Royal Family Speaks Out Against Crypto Regulation' (*CoinTelegraph*, 15 July 2019) accessed 12 August 2019.

It should be noted that not all of the nations that have yet to enact crypto regulations appear to be hostile to crypto. The Netherlands, which apparently has "*no regulation on digital currencies*",[71] is so welcoming to crypto that the unofficial nickname for the city of Arnham has become 'Bitcoin City'.[72] In early 2019, however, the Netherlands Minister of Finance received advice that a licensing system should be introduced.[73] The emphasis on the proposed regulation was apparently on prevention of money laundering and terrorist financing, which are unlikely to be a significant issue with a 'free' token distribution such as that contemplated with airdrops. However, until regulations are actually put into place, any potential impact on crypto in general and airdrops in particular is uncertain.[74]

VII. State of Regulation — Unwelcoming

Finally, there are nations that are quite hostile to crypto, and therefore likely to be hostile to airdrops as well. China, in fact, has explicitly warned against this particularly strategy for disseminating cryptoassets.

On November 3, 2018, the People's Bank of China (the country's central bank) issued a stability report warning against the use of airdrops.[75] The report concluded that "*companies running token giveaways are evading China's blanket ban on ICOs by issuing free tokens to the investor, while keeping a large chunk of the total supply for speculation on a crypto exchange, where speculation would drive the prices up so they can profit*." This hard line approach is consistent with earlier statements from the vice governor of the People's Bank that "*[a]ny new financial product or phenomenon that is not authorized under the existing legal framework, we will crush them as soon as they dare to surface*."[76] On the other hand, it is also worth noting that reports suggest that trading in crypto continues in

---

71 *See* Nick Hubble, 'Top Crypto Friendly (and Hostile) Countries' (*Capital and Conflict*, 20 March 2018) <https://perma.cc/7ZH8-GMZF> accessed 27 February 2019.

72 ibid.

73 Adrian Zmudzinski, 'Proposed License Requirements End Anonymous Crypto Selling and Buying in the Netherlands' (*CoinTelegraph*, 20 January 2019) <https://perma.cc/D5D5-8XJT> accessed 27 February 2019.

74 In fact, reports surfaced in July, 2019, that the Netherlands was considering a more restrictive approach to crypto. 'Dutch Crypto Regulation: Ministers Becoming Anxious, Regulatory Framework to be Discussed' (*Cryptowisser*, 2 July 2019) <https://perma.cc/C4TH-XLT4> accessed 12 August 2019.

75 Jimmy Aki, 'China's Central Bank Wants to Put the Damper on Airdrops: Report,' (*Bitcoin Magazine*, 5 November 2018) <https://perma.cc/8MER-95S6> accessed 27 February 2019.

76 ibid.

China, through virtual private networks, confusing what might otherwise be a straightforward prohibition on all things crypto.[77]

Some nations that have yet to adopt any formal regulations to govern crypto have nonetheless managed to make their position fairly clear. Bulgaria is in this category, even though there are apparently no specific regulations applicable to crypto based enterprises.[78] Regardless of the lack of official regulation, in May 2017, the Bulgarian government confiscated more than 2,00,000 Bitcoins in an operation "*against organized crime*."[79] In December of the same year, Bulgarian bankers closed all accounts used by crypto exchanges, leaving thousands of investors without access to their funds.[80] Given this history, even without official regulation, it appears reasonably certain that Bulgaria is hostile to crypto and likely to airdrops as well.

Another country clearly hostile to all things crypto is Bolivia. The Bolivian government has been arresting Bitcoin miners and traders since May 2017.[81] One source describes the situation in this country as follows:

> Cryptocurrencies have never been legal in Bolivia and the government has been known to enforce its anti-Bitcoin stance rather firmly. People caught using Bitcoin and other cryptocurrencies can be fined and a number of users have even been arrested on more than one occasion for trading and mining Bitcoin.[82]

Given that all crypto appears to be illegal in the country, it is to be expected that airdrops would be similarly frowned upon although there is no regulatory structure in place that would appear to require this outcome.

VIII. Conclusion and Recommendations

While the preceding discussion picks and chooses among regulatory schemes,[83] even this abbreviated listing of regulatory approaches illustrates

---

[77] *See* William Suberg, 'Despite Ban, China Keeps Trading Cryptocurrency Thanks to Tether and VPNs, Says Report' (*CoinTelegraph*, 9 September 2018) <https://perma.cc/75YX-66K7> accessed 27 February 2019.

[78] *See* Blockpit.io, 'How are Cryptocurrencies Regulated in Bulgaria' (*Medium*, 13 December 2018) <https://perma.cc/874F-G2DB> accessed 27 February 2019.

[79] Hubble (n 71).

[80] Hubble (n 71); see also 'Bulgaria News' (*CoinTelegraph*, 2019) <https://perma.cc/M2DT-D7TH> accessed 27 February 2019.

[81] Hubble (n 71).

[82] Brad Stephenson, '5 Countries Where Bitcoin Is Illegal' (*Lifewire*, 24 June 2018) <https://perma.cc/6HB9-LTSD> accessed 27 February 2019.

[83] For a more complete consideration of the international regulation of cryptocurrencies generally, see Law Library of Congress, 'Regulation of Cryptocurrency Around the World'

some of the differing reactions to crypto. It also provides fairly strong evidence that most nations have yet to address airdrops, as they continue to struggle with how to deal with the new technology.

Countries with more open and developed economies have tended to approach crypto from a relatively pragmatic position, recognising that bans are not only likely to be ineffective as against persons who insist on participating in the crypto world,[84] but also that there are potential advantages that might stem from innovation in this arena.[85] An outright ban essentially limits a nation's ability to take advantage of the potential economic benefits associated with such innovation, and therefore there would have to be a particular national perspective or interest at play in order to justify (or even really explain) this approach. It also prevents the country from having a more nuanced approach to regulation, meaning that countries with a ban might have larger problems with issues such as money laundering and the financing of terrorist and other criminal enterprises.[86]

Given the intangible nature of crypto, a more realistic approach might be to regulate the business based on national interests. For example, most countries are likely to want to avoid problems associated with money laundering and the financing of illegal activities such as terrorism. Similarly, most

---

(June 2018) <https://perma.cc/T7NJ-GN3Y> accessed 27 February 2019. This source specifically notes the wide range of approaches that various nations have taken towards cryptoassets, as well as the fact that these approaches are changing dramatically over time. The most commonly noticed actions involve warnings about the risks of investing in crypto markets, and the concern over illegal activities such as money laundering and terrorism. ibid at p 1. Regulatory reactions included in the report range from outright bans on cryptoassets and ICOs to state sponsored cryptocurrencies. ibid at p 2. A list of countries with explicit and implicit bans on crypto appears at p 4.

[84] Consider this statement, issued while India was apparently still contemplating a ban on virtual currencies:

'*Plans are afoot in India to ban cryptocurrencies. While it is as yet unclear what exactly the government's move against cryptocurrencies will be, what is clear is the fact that implementing it is going to be incredibly difficult. ….[C]ryptocurrencies are not bound by national jurisdictions but are powered by blockchain technology—a decentralized, distributed, public online ledger that is used to record transactions. A global network of computers manages the database that records all deals.*'

Nupur Anand, 'Why it Won't be Easy to Ban Cryptocurrencies in India' (*Quartz India*, 14 November 2018) <https://perma.cc/9EJ5-BVZ4> accessed 28 February 2019. See also Nick Spanos, 'Stifling Innovation With Regulation: Why Countries Shouldn't Ban Cryptocurrency Trading' (*Blockchain-Expo blog*, 2 February 2018) <https://perma.cc/UC54-VGGK> accessed 28 February 2019 (suggesting that a ban is like trying to stop a flood).

[85] A discussion of the potential value of crypto is outside the scope of this limited Article. For a brief introduction to this topic, focusing on crypto following the major declines in value during 2018, see Lawrence Wintermeyer, 'The Role of Cryptocurrencies In Future Society' (*Forbes*, 26 October 2018) <https://perma.cc/84EY-7W2Z> accessed 28 February 2019.

[86] *See* Anand (n 84), making this point.

nations are reasonably concerned about the potential for fraudulent initiatives designed to bilk citizens of hard-earned wealth. Countries may also set a priority of minimising tax avoidance, either out of concern that an underground barter economy could develop, or because traders might take advantage of comparative anonymity offered in various crypto markets and fail to report economic gains that would ordinarily be taxed. Once regulatory goals are set, airdrops can be evaluated to determine how much of a risk they pose.

Consider first the problem of money laundering and the risk that either proceeds from the sale of cryptoassets could be used to fund illegal activities or the crypto itself might fund criminal enterprises. The reality is that an airdrop does not involve the exchange of any property of value for the coin or token being dropped. Since the recipient is not contributing anything that can substitute for 'money',[87] there appears to be no risk that a criminal's money will be somehow laundered as a result of the airdrop itself. If the concern is somehow with secondary trading in the asset, then it is the secondary trading market that should be regulated rather than the airdrop itself.

Similarly, the absence of any contributions in fiat or other property readily convertible into fiat similarly limits the usefulness of airdrops as a vehicle for financing criminal activities. Since no money (or property with monetary value) is being contributed, there is nothing with which to finance the illicit behavior. Further, as has previously been stated, if there is a risk associated with subsequent appreciation of the coins or tokens and later trading of those assets, regulation should focus on that behavior which is where the risk occurs.

The same analysis applies when considering the extent to which airdrops provide problems for taxing authorities. Since nothing of value is exchanged for an airdropped token, there is unlikely to be a taxable event at that point. If a recipient realises gain later, through secondary trading of the airdropped asset, that should be the point at which tax may be due. Regulation of trading platforms would seem to be a more appropriate response than limiting airdrops. Even so-called privacy coins (which make actual ownership hard to trace) become problematic only when the coins are traded for value or used as payment.

Another frequently identified problem associated with crypto involves thefts, scams, and outright fraud. Regulators have identified a number of

---

[87] At most, a few services may be requested in order to have the coin or token dropped into a recipient's wallet. Part 3 of this Article includes a discussion of the kind of effort or actions that may be required.

common schemes associated with crypto that fit in this category, including the risk of being hacked,[88] Ponzi schemes,[89] pump-and dump operations,[90] and bait-and-switch.[91]

Hacks belong in a category of their own because the wrongdoer is not the issuer of the crypto, who also stands to lose. The market already provides incentives for reasonable cybersecurity initiatives, and the party who really needs to be monitored is the hacker rather than the creator of a new interest. For regulators convinced that legal protections are needed to minimise the risk of hacking, it is probably worth asking whether the victims of hacking are protected by other legal rights. Perhaps they have the right to utilise the country's bankruptcy laws to obtain redressal, as was the case in Japan following the Mt. Gox hack.[92] Alternatively, the victims of a hack might be able to bring a claim, individually or collectively, against the issuer of the tokens if it failed to use appropriate care in protecting the rights of the tokenholders from security risks. Tightening regulation of crypto entrepreneurs who are interested in airdrops in order to limit the impact of hackers seems like an overreaction. It might prevent hacking, but it also has the potential to stifle legitimate business and innovation as legitimate coins and tokens will also be affected.

---

[88] The biggest theft of Bitcoin via a hack so far was Mt. Gox, which involved a loss of around 800,000 Bitcoins. The largest Ethereum hack was the DAO incident which involved the loss of 3.6 million Ether. See 'Scams Include Deceptive Investment Opportunities, Bait-And-Switch Schemes and Deceptive Mining Tools' (*Finder*) <https://perma.cc/WXW9-8UMQ> accessed 28 February 2019. Not that it is not the blockchain itself that is being hacked, but rather an exchange (as in the case of Mt. Gox), a wallet service, or a smart contract with an exploitable vulnerability (as in the case of The DAO).

[89] For an explanation of this kind of pyramid scam, see US SEC, *Investor Alert, Ponzi Schemes Using Virtual Currencies*, US SEC Pub. No. 153 <https://perma.cc/7QXE-3ZNU> accessed 28 February 2019.

[90] As explained by the SEC:

> 'Pump-and-dump schemes often occur on the Internet where it is common to see messages posted that urge readers to buy a stock quickly or to sell before the price goes down, or a telemarketer will call using the same sort of pitch. Often the promoters will claim to have "inside" information about an impending development or to use an "infallible" combination of economic and stock market data to pick stocks. In reality, they may be company insiders or paid promoters who stand to gain by selling their shares after the stock price is "pumped" up by the buying frenzy they create. Once these fraudsters "dump" their shares and stop hyping the stock, the price typically falls, and investors lose their money.'
>
> US SEC, 'Fast Answers, "Pump-and-Dumps" and Market Manipulations' <https://perma.cc/X8U2-JH3Y> accessed 29 January 2019.

[91] *See* generally Dan Cummings, 'Cryptocurrency Fraud And The Anatomy of The Scam' (*ETHNews*, 10 June 2017) <https://perma.cc/6UDD-CCKZ> accessed 28 February 2019. This source also considers Ponzi schemes, pump and dump, and phishing.

[92] This is not to suggest that bankruptcy provides complete protection for those who lose investments to hackers. For a description of the Mt. Gox hack and bankruptcy proceedings, see Adrienne Jeffries, 'Inside The Bizarre Upside-Down Bankruptcy of Mt. Gox' (*The Verge*, 22 March 2018) <https://perma.cc/C9RB-5HAZ> accessed 28 February 2019.

With regard to other common scams associated with crypto generally, Ponzi schemes, pump-and-dump, and bait-and-switch all have the same general objective — the issuer or promoter essentially aims to steal victim's investments and leave them with nothing of value. While it is absolutely true that an airdropped coin or token may have little of value, it is equally true that the recipients have invested nothing (with the exception of time, in some cases). Thus, they don't stand to 'lose' anything. The risks of these kinds of fraudulent schemes therefore do not seem to provide a substantial reason to regulate airdrops.

This is not to say that there are no scams associated with airdrops. Phishing expeditions,[93] for example, may be particularly common. Here, however, the question is whether legitimate enterprises need to pay the price for protecting those who fall for dubious offers. A prohibition on offers that ask for private keys or a ban on requiring trust trades in order to establish that a wallet is active is not likely to be effective against individuals willing to engage in these kinds of transactions. They generally know that what they are doing is fraudulent. Broader regulation on or restriction of airdrops might limit the number of opportunities for scam artists, but again, it also limits potentially legitimate distributions. In addition, there may be less restrictive ways to combat the problem. For example, many regulators provide the public with information in the form of press releases, informational documents, investor alerts, and public warnings.

Of course, the call of where to draw the line is up to the regulatory authorities, based on whether a particular nation is more in favor of a highly regulated and therefore more protective regime, or an economy where market forces are allowed to influence outcomes. The real question for regulators, and the hardest one, is where to draw the line as to what is a true airdrop. Automatic drops that require nothing more than the possession of an active wallet do not, to this author at least, seem to require much in the way of regulation. Where more is required from the recipient in terms of effort and time, the greater the risk of abuse. An airdrop that requires significant amounts of time does implicate the risk of loss where effort may not be rewarded by a promised asset or the cryptoasset fails to do whatever it was supposed to do.

---

[93] As explained by one source:

'*Phishing is one of the biggest and most common cryptocurrency scams worldwide. It is an attempt to obtain sensitive information from a user such as usernames, passwords, card details, etc. In the cryptocurrency world, phishing scams attack cryptocurrency exchange passwords, digital wallets, private keys, etc. This process is usually done through a fake website which looks like an authorized one.*'

Habib Azam, 'How to avoid the most common crypto scams' (*CryptoDigest*, 12 August 2018) <https://perma.cc/K8UB-C4TT> accessed 28 February 2019.

And because most goals focus on avoiding loss to the recipient, it is the cost of the effort to the recipient that should be used to determine whether there has been a significant or 'material' contribution.

In addition, if the recipients are expected to post positive comments and lack a sufficient basis for those observations, particularly if the terms of the airdrop are not mentioned, the greater the possibility of misrepresentations being disseminated to defraud others. Positive comments can easily contribute to an unrealistic picture of a particular coin or token, especially where a reader might be unaware that the positive review was made only in fulfillment of an airdrop requirement. This may be relevant in secondary market trading and when the issuer makes subsequent distributions. In either case, however, it is not the airdrop itself that is problematic but later activities, which themselves could be regulated.

Deciding where to draw the line as to what constitutes a genuine airdrop and what is a bounty program or offering of securities that should be regulated requires a consideration of the facts and circumstances, which may not offer the certainty that the crypto community desires outside the scope of automatic airdrops. The difficulty in drawing lines is not, however, a reason to simply ban legitimate crypto-based companies from continuing to innovate in this emerging and evolving area. A more nuanced approach is required.

Regulators Nurturing Fintech Innovation: Global Evolution of the Regulatory Sandbox as Opportunity-Based Regulation

Deirdre Ahern[*]

Abstract *The regulatory sandbox is a real-world alternative to regulatory lag. Its emergence as a novel regulatory development responds to challenges faced by FinTech innovators in navigating an unwieldy regulatory landscape not designed with FinTech in mind. Regulatory sandboxes are in operation in developed countries including Australia, Canada, Denmark, Hong Kong, Singapore, Switzerland, the Netherlands, the United Arab Emirates, the United Kingdom, and the United States. Within the European Union they are seen in Denmark, Hungary, Lithuania, Poland and the Netherlands. The concept has also gained traction with regulators in developing countries such as India, Indonesia, Malaysia, Mauritius and Thailand. Not only is the regulatory sandbox an experimental space for firms testing innovative FinTech products and services, it is also a novel regulatory experiment for regulators. This article advances the available literature through focusing on the contradictions inherent in the role of the regulator in administering a regulatory sandbox. It characterises the regulatory sandbox as a form of agile, opportunity-based regulation, distinguished by a regulatory approach that is concerned with actively supporting innovators in nurturing cutting-edge innovation to benefit innovators, consumers, investors, and the wider economy. This is path-breaking regulatory territory. In its provision and design, a regulatory sandbox performs a crucial signalling function in relation to a given financial system's receptivity to FinTech business. An economic, pro-innovation agenda is at work. Distinct policy questions are therefore raised regarding the*

[*] Dr Deirdre Ahern, Associate Professor, Director of Law, Technologies and Society Research Group, Trinity College Dublin, Dublin, Ireland. Email: dahern@tcd.ie. The author is a member of the European Commission's Informal Company Law Expert Group (ICLEG); this paper does not form part of the work of ICLEG, nor do the views expressed in it purport to reflect the position of the European Commission. An earlier version of this paper was presented at the Addressing the Global Challenge of Responsive FinTech Regulation Symposium, Trinity College Dublin, 8 March 2019. The author thanks the symposium participants and the anonymous referees for their comments.

legitimate role of public gatekeeper financial services regulators operating regulatory sandboxes. The role of a regulatory sandbox in nurturing and expanding competition suggests a public interest role in the interests of consumer choice, price and efficiency rather than simply on risk minimisation. However, pressure on regulators to produce sandbox successes and to compete with other sandboxes may influence the exercise of regulatory discretion and produce regulatory distortions that affect competition in FinTech markets.

"*The balance between allowing innovation to thrive and protecting customers is tough to achieve but it is critical. Too much regulation and the industry becomes sclerotic, … bogging consumers down with antiquated systems and products. Too little, and fraud abounds. As a concept, financial innovation does not have the best of reputations.*"[1]

I. Introduction

The Fourth Industrial Revolution is an exhilarating period of experimentation. Path-breaking, disruptive innovation is radically changing the structure of financial services markets and processes. Bricks and mortar banking and face to face advice are being upended by disintermediated access to financial services. The advances being worked upon span a vast sphere including money transmission, smart contracts, digital identification tools, robo-advising, distributed ledger technology ('**DLT**'), big data analytics, initial coin offerings ('**ICOs**'), crowdfunding and peer to peer lending. It is axiomatic that law often trails in the wake of societal change. This truism is exemplified by the explosion of financial technology ('**FinTech**'). The speed of FinTech adaptations has left rule-makers and regulators at sea as they seek to

[1] O Ralph, 'FCA Does Big Number to Prove it is the Font of Financial Wisdom' *Financial Times* (London, 6 April 2016) <https://www-ft-com.eur.idm.oclc.org/content/50b6fb98-fb3b-11e5-b3f6-11d5706b613b> accessed 2 November 2019.

understand the innovations that are being developed, define their mandate in relation to such innovations, and make important policy choices with respect to the application of regulation to these innovators as compared with more traditional financial services. Certainly, responsive regulation is a tall order as an expanding array of distinct and interchangeable products and services emerge under the FinTech umbrella. But it is more complex than that. Governments fear that if their regulators do not come to the aid of FinTech innovators to assist them to navigate the regulatory framework, entrepreneurs may be discouraged from bringing their product to market in that jurisdiction. Thus, with FinTech, not only is the classic regulatory dilemma between a facilitatory approach and a regulatory approach at play, but an economic agenda is also a significant undercurrent at work. The emergence and spread of the regulatory sandbox as a novel regulatory development speaks to that agenda and responds constructively to the challenges faced by FinTech innovators in navigating an unwieldy regulatory landscape not designed with FinTech in mind. The genius of the regulatory sandbox lies in how it provides a sheltered environment to assist FinTech innovators to negotiate the impasse of an unclear regulatory environment while testing the viability of their imaginative products on a scaled-down basis. This is complex and path breaking regulatory territory that pushes regulators and regulatory actors beyond tried and trusted roles.

Dissecting the regulatory sandbox phenomenon as a form of market intervention falling short of conventional hard regulation, this article presents the regulatory sandbox as agile, opportunity-based regulation, characterised by an original regulatory approach that is concerned with actively supporting innovators in nurturing cutting-edge innovation with a view to delivering benefits to innovators, consumers, investors, and ultimately the wider economy. In its provision and design, the regulatory sandbox phenomenon performs a crucial positioning function, broadcasting a given financial system's receptivity to FinTech business and the perceived constructiveness of its regulatory approach. The existence, design and differentiation of individual regulators' sandbox offerings prompt important questions about the role of regulators in FinTech markets. As the regulatory sandbox concept gains traction and matures, legitimate questions need to be asked in relation to its situation within the regulatory landscape and the role of regulators in playing midwife to selected FinTech entrepreneurs' creations. To begin with, the regulatory sandbox's role in nurturing and expanding competition within FinTech product and service markets suggests a public interest role for regulators in improving consumer choice, price and efficiency. This is a completely different driver than a regulatory model predicated on risk-reduction.

An unavoidable question for scholars and policy-makers concerns how these two mandates can be appropriately reconciled.[2] It is argued here that a regulator's competition promotion agenda should not come at the expense of appropriate consumer and investor protection.

Section II tracks the origination of the regulatory sandbox, positioning it at the apex of regulatory supports for FinTech innovation within a financial ecosystem, and charts its global spread. A characterisation of the regulatory sandbox as opportunity-based regulation follows in Section III. This terrain unpacks the role that financial services regulators are taking as promoters of FinTech innovation within their jurisdiction and the possible implications for competition and regulatory sentiment. Section IV considers the potential for the regulatory environment provided by the regulatory sandbox to compromise appropriate regulation. Flowing from this, Section V presents a hierarchy of models of regulatory relief observed in available sandboxes and their regulatory consequences.

II. The Origination of the Regulatory Sandbox Phenomenon

Financial regulation is typically concerned with risks to the public interest including market conduct and consumer protection, market integrity, soundness of financial institutions and financial stability. Classically, financial services regulators are concerned with two ends of a ruler – devising and enforcing rules with a focus on risk-based regulation. However, command and control regulatory behaviour is less fashionable as regulators become more dynamic; responsive regulation is flexible.[3] Challenges for financial market regulation and legal controls have been heightened by technological advances such as the advent of algorithmic trading, predictive advisory services, automated credit scoring applications and Digital IDs, to name but a

---

[2] On this, *see*, E Avgouleas, 'Regulating Financial Innovation' in N Moloney, E Ferran and J Payne (eds), *The Oxford Handbook of Financial Regulation* (OUP 2015); C Brummer and Y Yadev, 'Fintech and the Innovation Trilemma' (2019) 107 Georgetown Law Journal 235 (exploring the difficulty of regulators successfully encouraging financial innovation while also achieving rules simplicity and market integrity); Iris H-Y Chiu, 'The disruptive implications of fintech - policy themes for financial regulators' (2017) 21(1) Journal of Technology Law & Policy.

[3] On responsive regulation, *see generally*, R Baldwin and J Black, 'Really Responsive Regulation' (2008) 71 Modern Law Review 59; J Braithwaite, 'The Essence of Responsive Regulation' (2010) 44 UBC Law Review 475. For a good discussion in a technology context, *see*, M Fenwick, Wulf Kaal and EP Vermeulen, 'Regulation tomorrow: what happens when technology is faster than the law' (2016) 6 American University Business Law Review 561.

few. As Brummer observes, "*regulatory and market disruptions overlap*".[4] Many regulators believe in the wisdom of standing back and adopting a 'wait and see' approach, watching these innovations manifest while probing their costs and benefits. In the European Union ('**the EU**'), rather than rushing to regulate in the FinTech space, the EU institutions have undertaken careful information-gathering and monitoring of business and regulatory developments at the national level.[5] Other regulators may be tempted to apply the full rigour of rules not designed for FinTech even where the fit is not good, with the result that beneficial innovation meets with unsuitable regulatory barriers and as such, may risk being stifled prematurely. This could occur, for example, when the full rigour of capital adequacy rules designed for banks are applied to crowdlending operations, making market entry difficult. At the other end of the regulatory continuum lie concerns that amid competition to carve up the FinTech pie, some regulators are opting for a race to the bottom in a bid to attract start-ups and investors.

Globally, we are some way off fashioning a suitable regulatory path to meet the brave new world that FinTech brings. Thus far, much of the extant international policy discussion concerning FinTech remains preliminary and generic – descriptive and largely confined to mapping developments, while extolling the virtues of continuing regulatory debate and dialogue. Progress is slow and no match for the speed of technological invention.[6] In the regula-

---

[4] C Brummer, 'Disruptive Technology and Securities Regulation' (2015) 84 Fordham Law Review 977, 980.

[5] *See further*, European Commission, *FinTech Action Plan: For a More Competitive and Innovative European Financial Sector* (COM(2018) 109/2) <https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf> accessed 2 November 2019.

[6] Scholars are beginning to tackle thorny questions of regulatory approach for FinTech. *See*, for example, Brummer (n 4); Fenwick, Kaal and Vermeulen (n 3); E Biber and others, 'Regulating Business Innovation as Policy Disruption: From the Model T to Airbnb' (2017) 70 Vanderbilt Law Review 1561; DW Arner, JN Barberis and RP Buckley, 'FinTech, RegTech and the Reconceptualization of Financial Regulation' (2017) 3 Northwestern Journal of International Law and Business 371; W Magnusson, 'Regulating FinTech' (2018) 71 Vanderbilt Law Review 1167; D Ahern, 'Regulatory Arbitrage in a FinTech World: Devising an Optimal EU Regulatory Response to Crowdlending' (2018) 3 Journal of Business Law 193; J Armour and L Enriques, 'The Promise and Perils of Crowdfunding: Between Corporate Finance and Consumer Contracts' (2018) Modern Law Review 51; J Armour and L Enriques, 'Individual Investors' Access to Crowdinvesting: Two Regulatory Models' in D Cumming and L Hornuf (eds), *The Economics of Crowdfunding* (Palgrave 2018); Iris H-Y Chiu, 'Pathways to European Policy and Regulation in the Crypto-economy' (2019) 10 European Journal of Risk Regulation 738; RH Weber and R Baisch, 'FinTech – Eligible Safeguards to Foster the Regulatory Framework' (2018) 33 Journal of International Banking Law & Regulation 335; V Burilov, 'Regulation of Crypto Tokens and Initial Coin Offerings in the EU' (2019) 6 European Journal of Comparative Law and Governance 146; M Lehmann, 'Global Rules for a Global Market Place? – The Regulation and Supervision of Fintech Providers' (2019) European Banking Institute Working Paper No. 45 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3421963> accessed 2 November 2019.

tory vacuum, the distinctive fluidity of the regulatory sandbox phenomenon is born of regulatory adaptability to the complexity of FinTech. Not surprisingly, in working towards formulating appropriate regulatory approaches to FinTech, a stakeholder-based approach has assumed prominence internationally. This is a space for reflexive governance, fitting within the core of decentred regulation, involving both state and non-state actors operating within a responsive regulatory agenda.[7]

While regulatory solutions for FinTech prove elusive, what is not in doubt is the economic promise of FinTech.[8] An ill-fitting regulatory framework of uncertain application to FinTech applications causes frustration when juxtaposed alongside FinTech's potential, not just for consumers, but also the wider economic benefits for countries where FinTech is nurtured and scaling up is facilitated.[9] Thus, in the regulatory vacuum, governments and regulators are acutely aware of the importance of providing an ecosystem of spaces that will support financial technology – incubators, accelerator hubs and innovation hubs as well as regulatory sandboxes.[10] While incubators generally involve mentoring and hothousing, accelerator hubs[11] provide physical space for experimentation and collaboration. Innovation facilitators, often styled as innovation hubs or labs, are generally designed to provide engagement, support and advice on how to negotiate the regulatory framework. Innovation hubs thus provide informal points of contact with regulators which, at an early stage, proves both less intimidating and more convenient for start-ups and small firms than more formal contacts with regulators. Queries generally addressed by hubs include issues in relation to whether authorisation is needed, how regulatory and supervisory requirements may be applied in practice, anti-money laundering regime issues and the

---

7 For a good discussion of this style of approach to regulation, *see*, A Wardrop, 'Co-Regulation, Responsive Regulation and the Reform of Australia's Retail Electronic Payment Systems' (2014) 30 Law in Context: A Socio-Legal Journal 197; Fenwick, Kaal and Vermeulen (n 3).

8 The global FinTech market is projected to reach US $124.3 billion by 2025. *See*, 'Global FinTech Market Report' (*QYResearch*, 21 February 2020) <https://www.qyresearch.com/index/detail/1527695/global-fintech-market> accessed 4 March 2020.

9 This of course also depends on the availability of access to venture capital in a given financial system. *See*, M Arnold, 'UK Fintech Sector in Buoyant Mood as Valuations Soar' *Financial Times* (London, 27 September 2018) <https://www.ft.com/content/3bcad1be-b1d7-11e8-8d14-6f049d06439c> accessed 2 November 2019 (reflecting on the effects of open banking in the UK).

10 Terms such as 'innovation hub' and 'accelerator' have not assumed a unified understanding or become a recognised term of art and are being used interchangeably with a variety of other terms such as 'innovation lab' and 'FinTech lab'. On this taxonomical dissonance, *see*, Basel Committee on Banking Supervision, *Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors* (Bank for International Settlements, 2018) 39 <https://www.bis.org/bcbs/publ/d431.pdf> accessed 2 November 2019.

11 The term 'hub' is often added to refer to the provision of a co-working space.

applicability of consumer protection measures.[12] First, benefits flow to the innovator. Vitally, this informal contact allows non-regulated entities to informally engage with FinTech regulators concerning the regulatory perimeter.[13] This may also help to map the need to engage with other regulators and supervisors concerning the regulatory perimeter on issues such as data privacy. Second, and equally crucially, the benefits flowing are two way – regulators who facilitate such contact and informal support gain enormously from the associated ability to keep abreast of and understand FinTech trends in market innovation. This enables the lessening of a regulator's regulatory blind spot in relation to what is happening outside those firms that are authorised and within its direct regulatory line of sight. These discussions are thus hugely beneficial to regulators and help to ensure that regulatory policy discussions, risk-assessment and decision-making are based on a solid knowledge foundation. In short, innovation supports provide an invaluable and costless mutual learning opportunity.

Building on the mindset of these initiatives to encourage FinTech, the unique hybrid business advisory and regulatory initiative known as the regulatory sandbox germinated. A regulatory sandbox gives permission to try and fail, and to do so in a controlled fashion that is less costly than would be the case on the open market as well as without systemic risk implications. The trailblazing concept originated in the United Kingdom ('**the UK**') and helped to establish the global reputation of the Financial Conduct Authority ('**the FCA**') as a regulatory leader. The history of the regulatory sandbox can be traced back to a deceptively simple act of reasoning by analogy. In 2015, Sir Mark Walport, then Britain's chief scientific adviser, floated the idea that the financial services sector could benefit from having the equivalent of clinical trials available to the pharmaceutical industry.[14] This appealed to the

---

[12] European Supervisory Authorities, *FinTech: Regulatory Sandboxes and Innovation Hubs* (JC 2018 74, 2019) para 28 <https://esas-joint-committee.europa.eu/Publications/Press%20Releases/JC%202018%2074%20Joint%20Report%20on%20Regulatory%20Sandboxes%20and%20Innovation%20Hubs.pdf> accessed 2 November 2019. Queries on issues such as data protection and cybersecurity usually fall within the mandate of other sectoral regulators.

[13] There is a credible argument that a regulatory sandbox should be a bolt-on to an effective innovation hub rather than operating on a stand-alone basis. On this, *see*, RP Buckley and others, 'Building FinTech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond' (2019) European Banking Institute Working Paper No. 53 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3455872> accessed 2 November 2019.

[14] United Kingdom Government Chief Scientific Adviser, *FinTech Futures: The UK as a World Leader in Financial Technologies* (Government Office for Science, 2015) 10-11, 52 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf> accessed 2 November 2019.

Project Innovate division of the FCA[15] and the FCA's regulatory sandbox regime for FinTech was unveiled a year later in 2016. The FCA's prototype aimed "*to promote more effective competition in the interests of consumers by allowing firms to test innovative products, services and business models in a live market environment, while ensuring that appropriate safeguards are in place*."[16] Firms applying to the FCA sandbox apply on a cohort basis (there are two six-month test periods each year). Applicants must set out in their application how they meet the eligibility criteria for testing. This requires having a financial services business in the UK which is 'genuinely innovative' and meets an 'identifiable consumer benefit'.[17] Applicants must also show a demonstrable need and readiness for sandbox testing.[18] The FCA's dedicated sandbox unit assesses regulatory sandbox applications[19] and decides which, if any, of the applicable regulations can be relaxed in any given case. This allows an agile, tailored approach to be taken which adapts to the needs of individual FinTech companies while also ensuring that appropriate consumer protection is in place. Controlled roll-out to consumers within a regulatory sandbox allows modifications to be made to the business model to respond to consumer and regulatory feedback. The FCA regards the sandbox as having been effective in helping firms to understand and potentially accelerate their route to market, and reduce costs on external regulatory consultants.[20] The FCA also concludes that the sandbox has successfully allowed it to identify and control risks.[21]

The economic imperative of realising FinTech's potential, coupled with the difficulty of navigating regulatory landscape, has played a part in rapidly propelling the success of the regulatory sandbox solution beyond national borders. Following in the footsteps of the UK, regulatory sandboxes have emerged in financial centres across the globe.[22] Regulatory sandboxes are in operation in developed countries including Australia, Brunei, Canada,

---

[15] Project Innovate began in 2014 with the aim of providing innovative firms with support to navigate the regulatory system and of promoting competition to benefit consumers.

[16] Financial Conduct Authority, *Regulatory Sandbox Lessons Learned Report* (2017) para 2.1 <www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf> accessed 2 November 2019.

[17] ibid 4.

[18] Financial Conduct Authority (n 16) 4.

[19] Distributed ledger technology was the most common type of technology being utilised in the first two cohorts of firms in the FCA sandbox.

[20] Financial Conduct Authority (n 16) para 2.8.

[21] Financial Conduct Authority (n 16).

[22] DA Zetzsche and others, 'Regulating a Revolution from Regulatory Sandboxes to Smart Regulation' (2017) 23 Fordham Journal of Corporate & Financial Law 31; M Weschler, L Perlman and N Gurung, 'The State of Regulatory Sandboxes in Developing Countries' (2018) Columbia Digital Financial Services Observatory Working Paper <https://dfsobservatory.com/sites/default/files/DFSO%20-%20The%20State%20of%20Regulatory%20

Denmark, Hong Kong, Singapore, Switzerland, the Netherlands, the United Arab Emirates (Abu Dhabi) and the United States (in the States of Arizona, Kentucky, Utah and Wyoming). Within the EU, they are seen in Denmark, Hungary, Lithuania, Poland and the Netherlands. Meanwhile, Austria, Estonia, Italy and Spain have committed to launching a regulatory sandbox. The EU is presently contemplating whether it should intervene to ensure some uniformity of approach.[23] Sandboxes are of most relevance in jurisdictions where there are reasonably developed authorisation regimes for financial services, and particularly, FinTech. While the regulatory sandbox has gathered most headway in developed and emerging economies, it also reveals potential in developing countries. For example, regulatory sandboxes are in evidence in Bahrain, Indonesia, Jordan, Kazakhstan, Malaysia, Mauritius, Mozambique, Nigeria, Rwanda, Sierra Leone and Thailand.[24] Some developing countries such as the Philippines have deployed a 'test and learn' model that bears similarities to the sandbox concept. The main differential is that a regulatory sandbox is generally subject to a more formalised process with standard application and assessment criteria.[25] In other emerging and developing economies such as Kenya, Mexico and Sri Lanka, regulatory sandboxes remain under active policy consideration. In the context of developing countries, a regulatory sandbox has obvious potential to facilitate FinTech solutions that assist with a financial inclusion objective within the relevant financial ecosystem.[26] That said, developing countries can present unique challenges for FinTech innovation in terms of market, resources, infrastructure, distance from innovation hubs and other supports.[27]

Among the developing countries, India has made an active effort to improve its receptivity to FinTech innovation. A regulatory sandbox framework was

---

Sandboxes%20in%20Developing%20Countries%20-%20PUBLIC.pdf> accessed 2 November 2019; Buckley and others (n 13).

[23] European Supervisory Authorities (n 12); European Commission, *Final report of the Expert Group on Regulatory Obstacles to Financial Innovation* (2018) 70 <https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf> accessed 2 November 2019.

[24] Weschler, Perlman and Gurung (n 22).

[25] Weschler, Perlman and Gurung (n 22) para 2.2, Exhibit 1.

[26] On financial inclusion, *see*, I Jenik and K Lauer, 'Regulatory Sandboxes and Financial Inclusion' (2017) Consultative Group to Assist the Poor Working Paper <www.cgap.org/sites/default/files/researches/documents/Working-Paper-Regulatory-Sandboxes-Oct-2017.pdf> accessed 2 November 2019; T Aveni and I Jenik, 'Crowdfunding in China: the Financial Inclusion Dimension' (*Consultative Group to Assist the Poor*, July 2017) <www.cgap.org/sites/default/files/researches/documents/Brief-Crowdfunding-in-China-Jul-2017_0.pdf> accessed 2 November 2019.

[27] Weschler, Perlman and Gurung (n 22) para 4.2.3.

finalised by the Reserve Bank of India ('**the RBI**') in 2019.[28] In 2016, the RBI established an inter-regulator working group to examine the regulatory landscape for enabling the delivery of low-cost financial products and services in the context of the FinTech evolution. Its observations floodlit the importance of establishing a regulatory sandbox for FinTech. The origination of the RBI's sandbox proposal can be traced to the 2017 Household Finance Report[29] where the creation of a regulatory sandbox was proposed that would allow small-scale testing and temporary waivers of certain regulations in a carefully controlled environment.[30] The subsequent deliberations of the Working Group on FinTech and Digital Banking[31] led in turn to the publication of a Draft Framework in April 2019 for public consultation and of the 'Enabling Framework for Regulatory Sandbox' in August 2019.[32] The potential to improve retailer and consumer access to banking and payments mechanisms and other financial services in India was well-captured in the following terms:

> The [regulatory sandbox] can go a long way in not only improving the pace of innovation and technology absorption but also in financial inclusion and in improving financial reach [such as through enabling] microfinance, innovative small savings and micro-insurance products, remittances, mobile banking and other digital payments.[33]

---

[28] The final framework was released in August 2019: *see*, Reserve Bank of India (Department of Banking Regulation, Banking Policy Division), *Enabling Framework for Regulatory Sandbox* (2019) <https://rbidocs.rbi.org.in/rdocs//PublicationReport/Pdfs/ENABLING79D8EBD31FED47A0BE21158C337123BF.PDF> accessed 2 November 2019.

[29] Reserve Bank of India, *Report of the Household Finance Committee on Indian Household Finance* (2017) para 7 <https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/HFCRA28D0415E2144A009112DD314ECF5C07.PDF> accessed 2 November 2019.

[30] ibid para 7. This would enable the collection of "*empirical evidence which can ultimately lead to better policy solutions, whilst simultaneously evaluating the risk of any new product or technology.*"

[31] Reserve Bank of India, *Report of the Working Group on FinTech and Digital Banking* (2018) <https://rbi.org.in/scripts/PublicationReportDetails.aspx?ID=892#4> accessed 2 November 2019.

[32] Reserve Bank of India (Department of Banking Regulation, Banking Policy Division), *Draft Enabling Framework for Regulatory Sandbox* (2019) <https://rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=920> accessed 2 November 2019; Reserve Bank of India, 'RBI releases draft Enabling Framework for Regulatory Sandbox' (Press Release, 2019) <https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=46843> accessed 2 November 2019. The RBI indicated that feedback was received from 69 stakeholders, including FinTech firms, banks, multilateral agencies, industry associations, payment aggregators, audit and legal firms, government departments and individuals.

[33] Reserve Bank of India (n 28) para 3.3.

The RBI regulatory sandbox framework for FinTech companies includes an indicative list of innovative products and technologies which may be eligible,[34] and also indicates what is ineligible including cryptocurrencies, ICOs and credit registries. The framework is designed to be open to entities including banks and financial institutions for products that are ready for testing, meet a gap in the financial ecosystem and have clear benefits for consumers or the FinTech industry. The RBI framework also sets out a series of conditions to be met including minimum net worth requirements, fit and proper criteria for directors and promoters, satisfactory credit score, robust IT infrastructure and adequate managerial resources. Notably, insurance cover is a requirement for participation.[35] The RBI's sandbox will operate on the basis of a series of thematic cohorts such as financial inclusion, payments and lending, and digital know your customer ('**KYC**'). The application process for the first themed sandbox on digital retail payments products opened in late 2019 with a view to testing commencing in 2020.[36] This will enable FinTech innovation in the sphere of digital payments, digital KYC and wealth management. This is in line the RBI's drive to facilitate FinTech innovation, improve financial inclusion and move India towards a cashless economy. The Indian example illustrates the significant potential for FinTech to provide digital payment solutions in developing countries where access to brick and mortar financial institutions is a challenge.

III. Opportunity-Based Regulation and Regulators as Promoters of Competition in FinTech Markets

The regulatory sandbox effectively showcases how regulators themselves have proved agile and inventive in recognising and working around the deadening effect of regulatory lag.[37] The regulatory sandbox also represents a 'reasonable compromise'[38] where rushing to regulate may be a mistake.

---

[34] Mobile technology applications, data analytics, application program interface (API) services, blockchain technology applications, artificial intelligence and machine learning applications are listed. *See*, Reserve Bank of India (n 28) paras 6.1.1-6.1.2.

[35] Reserve Bank of India (n 28) para 6.8.3.

[36] No maximum number of participants has been set for each cohort. Participation will be for a maximum of 27 weeks.

[37] On agile governance, *see*, World Economic Forum, 'Agile Governance: Reimagining Policy-making in the Fourth Industrial Revolution' (2018) <http://www3.weforum.org/docs/WEF_Agile_Governance_Reimagining_Policy-making_4IR_report.pdf> accessed 2 November 2019.

[38] WG Ringe and C Ruof, 'A Regulatory Sandbox for Robo Advice' (2018) European Banking Institute Working Paper No. 26, 52 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3188828> accessed 2 November 2019.

Within the framework of FinTech innovation supports, the regulatory sandbox lies at the apex in terms of its characteristic regulatory interface because it moves beyond being purely an advisory conduit associated with other supports such as innovation hubs. Although regulatory sandboxes for FinTech differ across jurisdictions in terms of entry requirements and nature of the environment, a shared characteristic is that firms admitted to the sandbox are restricted in relation to the nature and scale of the activities they may carry out during testing in the sandbox environment. Monitoring of testing is a more resource-intensive activity for regulators than the general compliance monitoring they typically undertake, given the innovative nature of the FinTech products being tested and the likelihood of unknowable risks, all the while navigating a regulatory framework not designed with the product in mind. This explains the importance of managing a contained roll-out within the test bed. A scaled-down test reduces the total risk and may be designed to concentrate the risk on consumers considered best equipped to handle such risk. As far as sandbox users are concerned, contained roll-out provides invaluable early-stage feedback allowing product modifications and tweaks to the business model. Provision of advice by regulators on regulatory compliance assists with product roll-out and increases the chance of being able to harness the opportunity successfully. In short, the sandbox is of benefit in terms of saving time and financial resources as well as easing the regulatory journey of a user. If viability is thrown into doubt, the associated expense for failure will be far less in a sandbox launch to a small client base followed by a managed exit than would be the case with a full-scale launch on the open market.

Incontestably, the adoption of a regulatory sandbox qualifies, on its face, as a pro-innovation regulatory stance – an adaptive regulatory move away from Baldwin and Black's dialectic of risk-based regulation or problem-based regulation[39] to a new type of regulation which this article terms 'opportunity-based regulation'. Within the lens of opportunity-based regulation, financial services regulators play a critical part in actively nurturing and promoting competition in emerging and nascent FinTech markets, in addition to operating in the traditional regulatory space. Quintessentially, the sandbox concept comprises a *realpolitik* alternative to regulators sitting on their hands while maintaining a passive 'wait and see' stance to regulatory lag.[40] Through the prism of a regulatory sandbox, opportunity-based regula-

[39] R Baldwin and J Black, 'Driving Priorities in Risk-Based Regulation: What's the Problem?' (2016) 43(4) Journal of Law and Society 565.

[40] For a discussion of a 'wait and see' approach as a justifiable regulatory strategy in the context of crowdfunding, *see*, Armour and Enriques (n 6). In the context of crowdlending, *see*, Ahern (n 6).

tion provides a 'third way' featuring a more active stance involving support, mutual dialogue and learning in order to realise the potential of FinTech innovation.[41] This is regulatory agility at its peak. The regulatory sandbox concept actively supports cutting-edge innovation with a view to delivering opportunities for innovators, but also benefits for consumers, investors, and ultimately the wider economy. The active support and mentoring provided within the sandbox environment marks out opportunity-based regulation in this context as travelling quite some distance beyond mere facilitative regulation.

Opportunity-based regulation for sandbox participants is responsive and dialogic, but also time-limited. This serves to dynamically propel FinTech innovation to market in spite of the unwieldiness of a regulatory framework not made with these business models in mind. This agenda is consistent with Ringe and Ruof's contention that "*[g]ood regulation … should not only focus on addressing potential risks, but should also strive to identify market developments that are desirable for the system, and moreover promote those*."[42]

In big picture terms, it is entirely legitimate to regard the regulatory sandbox as part proxy for governmental desire to boost the economy by attracting and enabling FinTech innovation. This forces the consideration of competition promotion as part of the regulatory agenda of the regulatory sandbox. Internationally, there is a bifurcation between countries adopting the dual mandate model, whereby regulators are charged with encouraging business innovation as well as having a traditional regulatory role, and those where market development is hived off to specialist trade bodies. The UK's FCA provides the quintessential example of the formal dual mandate model, having the role of promoting effective competition in regulated financial services in the interests of consumers as well as of performing traditional regulatory functions. The Financial Services Act 2012 acknowledges a triptych of consumer protection, market integrity and competition objectives.[43] The FCA's effective competition mandate is further elucidated by the statutory specification that regard may be had by the FCA to considerations such as

---

[41] In the United States, there is a history of the Securities and Exchange Commission using pilot schemes to trial regulation. On this, *see*, Brummer (n 4) 1046-1047.

[42] Ringe and Ruof (n 38) 7.

[43] Financial Services and Markets Act 2000, s 1B(3) (as substituted by s 6 of the Financial Services Act 2012). On the background to the competition promotion mandate, *see*, Independent Commission on Banking, *Final Report: Recommendations* (2011) paras 8.75-8.87 <https://webarchive.nationalarchives.gov.uk/20120827143059/http://banking-commission.independent.gov.uk/> accessed 2 November 2019.

ease of market entry and encouragement of innovation.[44] That said, even where a competition promotion role is not formally assigned to a regulatory agency in establishment legislation, a pro-FinTech agenda may nonetheless arise on a de facto basis based on the adaptive manner in which a regulatory agency exercises its operational powers. This has particular resonance in relation to the operational application of regulatory sandbox models by regulators in practice.

Why does this matter? A role in promoting innovation and effective competition in financial services assigned to a sectoral regulator is clearly distinct from the role of competition law, more generally, in preventing abusive behaviour which distorts the market. Nonetheless, arguments can be summoned against a quasi-market-making role being assigned to regulators. Most obviously, the argument can be advanced that in the case of the regulatory sandbox, regulators are artificially interfering with natural selection in the market. The operation of a regulatory sandbox regime has direct and indirect impacts on the structure of competition and shapes market responses of both incumbents and potential entrants to FinTech markets. Both the existence of a regulatory sandbox regime and its design features matter and have effects on the choices and behaviour of regulatory actors. The contours of the regulatory perimeter of a regulatory sandbox have an impact on how FinTech actors, particularly start-ups, plan and execute their route to market. Buckley et al contend that any 'copy-cat sandbox' based on the FCA model does not send such a strong pro-innovation signal as the original.[45] However, as the regulatory sandbox proliferates globally, many other regulators are carving out their own identity through innovating in their own right on sandbox characteristics, for instance, by providing a guaranteed time to a decision on applications, and in Singapore and India, through the provision of a dedicated Insurtech sandbox.

The regulatory sandbox is unique in terms of the manner in which the regulator is making ex ante business judgments on the commerciality of what is proposed and is placing itself in the position of an arbiter on innovation. Representing the heart of what the regulatory sandbox is about, innovation is understandably the overriding entry threshold. However, the strictures of how that is understood vary from jurisdiction to jurisdiction. Under the UK FCA model, the overriding criterion for admission to the sandbox is essentially that what is proposed to be tested must involve bringing sufficiently new or ground-breaking innovation to the market that makes a real addition

---

[44] Financial Services and Markets Act 2000, s 1E(2) (as substituted by s 6 of the Financial Services Act 2012).

[45] Buckley and others (n 13) 17-18.

to the available consumer offering.[46] This innovation threshold has gone on to become a fairly universal requirement in other jurisdictions inspired by the UK's initiative.[47] This generally requires demonstration that the financial services product or service is genuinely innovative and benefits consumers by either meeting an untapped need or serving an existing need better than current market players. A well-measured approach is seen in the definition of 'innovation' in Arizona, a state which has led the way in the United States in terms of being the first to provide a framework for FinTech. Innovation is defined as:

> the use or incorporation of new or emerging technology or the re-imagination of uses for existing technology to address a problem, provide a benefit or otherwise offer a product, service, business model or delivery mechanism that is not known by the Attorney General to have a comparable widespread offering in this state.[48]

The knock-on effects of threshold determinations on innovativeness are considerable given the practical and goodwill advantages that accompany the cachet of selection for a given sandbox. This points up the prospect of regulators as deciders of what qualifies as innovative, rather than as simply interpreters and enforcers of rules. This is a major role shift.

In judging novelty, given the rapidly emerging nature of the FinTech industry, there are likely to be amplified knowledge and information gaps relevant on the part of the FinTech regulator.[49] Regulatory personnel assessing sandbox applications are likely doing their very best to be on top of FinTech in terms of both business models and technological innovation, yet they may be heavily reliant on observation-based learning, often from regulatory actors with whom they are engaged in regulatory dialogue, rather than having the benefit of direct experiential learning. The challenge of threshold decisions on admission to the sandbox being made on the basis of imperfect information is particularly acute in emerging markets with innovative new products. Information asymmetries are likely to be greater again for sandbox regulators who prioritise guaranteed expedited decision-making as a feature of the

---

[46] Financial Conduct Authority, 'Applying to the regulatory sandbox' (2017) <https://www.fca.org.uk/firms/regulatory-sandbox/prepare-application> accessed 2 November 2019.

[47] *See*, for example, Monetary Authority of Singapore, *FinTech Regulatory Sandbox Guidelines* (2016) paras 6.2(a), 6.2(b) and 7.4 <www.mas.gov.sg/~/media/Smart%20Financial%20Centre/Sandbox/FinTech%20Regulatory%20Sandbox%20Guidelines%2019Feb2018.pdf> accessed 2 November 2019.

[48] Arizona Revised Statutes 2018, § 41-5601, para 4 <https://law.justia.com/codes/arizona/2018/title-41/section-41-5601> accessed 2 November 2019.

[49] F Scott Morton, 'Are a Competition Authority and an Industry Regulator Equivalent?' (2015) 14 Colorado Technology Law Journal 9, 13.

sandbox offering, thus making decisions based on a truncated assessment process.

The assessment of innovation as the touchstone entry criterion for admission to regulatory sandboxes means that regulator determinations indirectly influence market viability propositions and thus, market outcomes. Accordingly, whether or not a competition promotion role is formally assigned to a relevant regulator administering a FinTech sandbox, assessment invariably requires financial services regulators to gauge and compare applications based on existing competition, product comparators and substitutability and potential market demand.[50] Anna Wallace, Head of Innovate at the UK's FCA has reflected on the contribution of regulators to determining market innovation as follows:

> As regulators we're under constant pressure to be more 'pro-innovative'. [A regulatory sandbox allows you] to do that in a way that gives you comfort that you're creating an environment that you control. Up until now regulators have never had the power to do that — the regulators have either decided whether something is outside or inside regulation. The regulatory sandbox provides a third way, where you can allow it in a small way into regulation, so you can observe what the risks and issues of that business model are. You control that environment before allowing it into the market.[51]

In terms of market outcomes, opportunity-based regulation is selectively applied – there are winners and losers. The competitive selection process for the sandbox creates a small in-group cohort of participants[52] and a larger out-group of non-participants. The sandbox gives those admitted a considerable competitive advantage compared to their peers in terms of testing, negotiating route to market and navigating regulatory compliance. Sandbox participation can help to reduce initial regulatory uncertainty, thereby enabling greater focus by participants on crystallising the technical performance of the innovative product or service and its business model. Sandboxes participants benefit from cost-free compliance advice, potential regulatory

---

[50] On the question of whether sectoral regulators are appropriately equipped to define markets and engage in market analysis, *see*, MM Dabbah, 'The Relationship Between Competition Authorities and Sectoral Regulators' (2011) 70 Cambridge Law Journal 113, 128.

[51] J Kelly, 'Arizona Sandbox Gives Start-Ups a Regulatory Path to US' *Financial Times* (London, 12 November 2018) <https://www.ft.com/content/aac62a22-c196-11e8-84cd-9e601db069b8> accessed 2 November 2019.

[52] Responding to criticism of an earlier proposal to limit participation to 10-12 entities at once, the Reserve Bank of India's final framework for its regulatory sandbox released in August 2019 (n 28) did not limit the number of entities that could be admitted to the sandbox at once.

waivers, and the goodwill value of a level of official endorsement which is marketable to financiers and potential clients. The type of tools and support provided by regulators vary but advice on regulatory compliance that assists with product roll-out is standard. Thus, special treatment afforded to sandbox participants dissolves the level playing field for market entry, and participation in the sandbox potentially reduces both the barriers to and the costs of market entry significantly.

A sandbox regime based on selective admission and centred around innovation differs fundamentally from an authorisation regime that is potentially open to all. The riposte to this is that the trade-off of the sandbox's selectivity is a stopgap measure to address regulatory complexity and that individual nurturing in small cohorts helps some FinTech innovators succeed who otherwise would not. Nonetheless, in the rush to facilitate FinTech innovation, countries need to be conscious of fairness in designing, integrating and applying a regulatory sandbox within a financial system. Equality of access is a consideration. The RBI's Working Group on FinTech and Digital Banking highlighted the regulatory pitfall of choosing "*to unduly favour newcomers by regulating them less stringently than incumbents, in the name of fostering competition*."[53] Reflecting that objection, not every jurisdiction has thrown its hat in the regulatory sandbox ring, and for some regulators, this is a conscious decision based on principled objection rather than a passive regulatory stance. Anecdotal evidence suggests that some sectoral regulators, including those in France, Germany and Ireland remain cautious and sceptical about the role of regulatory sandboxes and their part in driving competition outcomes in this post-financial crisis era. The preference of these regulators is to confine themselves to a more general advisory role, often in the form of a FinTech regulatory advisory desk open to all.

A further consideration concerns the manner in which the traditional role of the regulator is rewritten in the context of the regulatory sandbox. Provision of a regulatory sandbox sees a regulator moving from the role of gatekeeper to quasi-compliance consultant and ally. Valuable product advice is dispensed. For example, in the UK, the FCA provides secondary review of robo-advice by a qualified financial advisor.[54] Relatedly, there is an inherent

---

[53] Reserve Bank of India (n 31). However, that objection did not permeate the subsequent Draft Enabling Framework for Regulatory Sandbox: Reserve Bank of India (n 32). *See also*, United States Department of the Treasury, *A Financial System that Creates Economic Opportunities: Nonbank Financials, Fintech and Innovation* (2018) 171 <https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf> accessed 2 November 2019.

[54] Financial Conduct Authority (n 16) para 2.6. For an exploration of the potential of a dedicated regulatory sandbox for robo-advice, *see*, Ringe and Ruof (n 38). On regulation of

risk of herding behaviour by both investors and retail customers based on a positive bias surrounding mere selection for admission to testing in the regulatory sandbox. Rightly or wrongly, a firm's admission to a regulatory sandbox and the associated regulatory oversight has prestige value and can lead to a public perception of increased regulatory certainty. Although in actuality a preliminary testing phase, admission to the sandbox is frequently perceived on the ground and in the media as providing a coveted regulatory stamp of approval and de facto endorsement of the underlying product or service, which helps to attract customers and venture capital.[55] In the UK, the FCA specifically flags as a success indicator that testing in the regulatory sandbox has been instrumental in helping firms access finance.[56] Indeed, reflecting this, anecdotal evidence suggests that some firms primarily use the sandbox process not for product testing, but rather to obtain free compliance advice or alternatively, as a means to attract the interest of venture capitalists so that they can pivot and scale up. To conclude, both direct and indirect competitive impacts accrue from regulatory sandbox participation.

Turning to the regulator's perspective, there is pressure on regulators administering sandboxes to produce tangible results and for regulators to compare their respective outcomes. Pressure on regulators to produce sandbox successes may influence the exercise of regulatory discretion and produce regulatory distortions. Particularly in cases where a tailored regulatory environment is created, an element of regulatory capture may be at play given the desire of regulators to see successful testing and market entry of sandbox participants. For the FCA sandbox, the first cohort of 24 accepted firms was announced in late 2016.[57] 75 percent of firms in the first cohort successfully completed testing with 90 percent of these proceeding towards a wider market launch.[58] On the back of these figures, the FCA sandbox is regarded as top of the leader board by competition promotion standards. However, in many other jurisdictions, sandbox outcomes have been far more muted.[59] In some cases, a less than expected initial take-up of the regulatory

---

robo-advice, *see*, Iris H-Y Chiu, 'Transforming the Financial Advice Market - The Roles of Robo-advice, Financial Regulation and Public Governance in the UK' (2019) Banking and Finance Law Review (forthcoming).

55 J Kelly, 'A 'Fintech Sandbox' might sound like a Harmless Idea. It's Not' *Financial Times* (London, 5 December 2018) <https://ftalphaville.ft.com/2018/12/05/1543986004000/A--fintech-sandbox--might-sound-like-a-harmless-idea--It-s-not/> accessed 2 November 2019.

56 Financial Conduct Authority (n 16) paras 1.1, 2.10-2.12.

57 A further four cohorts were accepted based on competitive applications in 2017, 2018 and 2019.

58 Financial Conduct Authority (n 16) para 2.9.

59 For example, in Australia, as of May 2019, there was only one current user and six past users of the regulatory sandbox licence exemption: *See*, Australian Securities and Investments

sandbox offering is likely to be due in part to inherent restrictions within the national design of a particular sandbox.[60] Public discussion around bottom line results underscores how conscious FinTech regulators are about calibrating their sandboxes to signal their attractiveness to the FinTech market. As a consequence, some regulators have been coy in relation to fully transparent disclosure of outcomes.

This brings the discussion to the competition between jurisdictions (and thus, sandbox regulators) for FinTech business. A regulatory sandbox needs to be contextualised as but one element of a regulatory environment. However, all else being equal, each regulator competes with substitute sandbox regimes to attract the market for sandboxes: start-ups and other innovators across the FinTech spectrum. In an open market, prices perform an economic signalling role in relation to the state of supply and demand. The regulatory sandbox performs a similar function, providing an indicator that a regulator offering the regulatory sandbox as a lifeline to FinTech actors is pro-innovation or 'FinTech-friendly'. Innovation is the overriding entry threshold and this, combined with favourable regulatory treatment and support provides the foundation of the signalling function. The signal emitted is nuanced, going beyond the black or white of the existence of a sandbox offering or its absence. Signalling comes not only from the primary signal provided by the availability of the sandbox, but also from the more nuanced secondary signalling deriving from a sandbox's constituent parameters (comprising matters such as eligibility criteria, duration, supports, regulatory relief and reporting requirements). Thus, the FinTech-friendly signal being broadcast to FinTech innovators may be stronger in some jurisdictions and dimmer or absent in others.

In examining secondary signalling, overall consideration of the design choices made by the sandbox regulator should enable a view to be formed in relation to the general regulatory approach being adopted, including whether it is well-defined, objective and transparent and whether the overall approach is facilitatory or even lax, having regard to the protections available

---

Commission, 'Regulatory sandbox: Licence exemption users' (2019) <https://asic.gov.au/for-business/innovation-hub/fintech-regulatory-sandbox/regulatory-sandbox-licence-exemption-users/> accessed 2 November 2019.

[60] In Australia, for example, when poor levels of industry interest became evident, there was a strong backlash against the restrictive design of the regulatory sandbox and (as referred to earlier), root and branch legislative reform is consequently underway to make the exemption framework accessible to a greater range of financial products and services. *See*, 'FinTech Australia Supports Proposed Sandbox Expansion and Calls for Further Improvements' (*FinTech Australia*, 15 March 2018) <https://fintechaustralia.org.au/fintech-australia-supports-proposed-sandbox-expansion-and-calls-for-further-improvements/> accessed 2 November 2019.

to consumers and the equivalent treatment of competitors outside the sandbox. Furthermore, by the same means, inter-country comparisons of regulatory sandboxes (and overall regulatory structures) should be capable of being formed by the business and legal community and scholars. However, at this point in the evolution of the regulatory sandbox, a few short years after the UK led the field in establishing the first sandbox in 2016, it is challenging to comprehensively compare different sandbox regimes.[61] In the absence of a supranational guiding framework for regulatory sandboxes, use of terminology, wider legal frameworks and regulatory approaches and design vary considerably. National regulators have adapted and innovated in devising their own brand of regulatory sandbox. This restricts observational generalisations when discussing the regulatory sandbox concept.[62] In design, FinTech regulatory sandboxes cover a wide range of activities, traversing banking, investment activities and services as well as insurance and compliance products. In some countries, a selective or restricted approach to eligible candidates and types of projects admitted has been employed. For example, in India, the RBI's sandbox was initially designed to be specifically confined to start-ups but in response to feedback this was broadened out in the final version. Hong Kong's sandbox is restricted to incumbent banks (and partnering technology firms). Its FinTech Supervisory Sandbox launched in 2016 is specifically intended to enable banks to engage in pilot tests of FinTech initiatives such as biometric authentication.[63] Reflecting its heritage in banking, Switzerland has a regulatory sandbox solely for projects involved in banking.[64]

IV. Does the Regulatory Sandbox Compromise Appropriate Regulation?

In defining eligibility controls to restrict access to regulatory sandboxes, jurisdictions are learning through trial and error what fits best in their regulatory and commercial landscape. As such, regulators are finding their regulatory comfort zone and broadcasting it to the market in the form of agreed parameters for regulatory sandboxes. Not all opportunities are regarded equally.

---

[61] Ringe and Ruof (n 38) 44 (noting the difficulty of comparing the efficacy of different regulatory sandbox models while they are in their infancy).

[62] Given the different models of sandbox that have evolved, the term 'regulatory sandbox' as employed in this paper, is neutral as to whether the firms admitted are regulated or unregulated and whether any regulatory relief applies to them.

[63] Hong Kong Monetary Authority, *Fintech Supervisory Sandbox 2.0* (2020) <https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech-supervisory-sandbox.shtml> accessed 2 November 2019.

[64] In 2018, proposals were made that would extend the Swiss sandbox to include the development of products based on blockchain.

The State of Arizona, motivated by risk minimisation, specifically excludes securities trading, insurance products, or services that provide solely deposit-taking functions from eligibility to enter the FinTech Sandbox.[65] There is a concern that some finance centres with light touch regulatory environments that are keen to position themselves as FinTech-friendly may prioritise innovation over putting adequate safeguards in place to protect the public interest.[66] Cryptocurrencies are a case in point. For some observers, the willingness of certain regulators to allow cryptocurrency actors to experiment in the sandbox has raised alarm bells. Many jurisdictions have steered clear no doubt due in part to concerns about the insufficiency of investor protection as well as the uncertainty of regulatory approach.[67] For example, the RBI's indicative black list shows caution in excluding cryptocurrency/crypto asset services and ICOs from sandbox participation.[68] Such judgment calls are particularly complex in relation to emerging technologies and dovetail to a wider frame of how the relevant sandbox operates. As such, it would be facile to label such regulatory choices as inherently right or wrong in their own right. There is nonetheless a concern that facilitating market access via the establishment of a regulatory sandbox could cut across well-established objectives of financial regulation and in doing so, permit harm to investors and consumers.[69] Problematically, there is a dearth of publicly available information, both as to the exercise of regulatory discretion, and in relation to sandbox outcomes in practice.

In Singapore, a recognised regional financial centre with a light-touch regulatory environment, the Central Bank has been focused on trialling ICOs and facilitating ownership of cryptocurrencies using a regulatory sandbox rather than banning them outright as some countries have done amid investor protection fears.[70] In the UK, a number of cryptocurrency companies have been admitted to the FCA sandbox. Within a controlled environment, it hopes to be able to distinguish good ICOs and cryptocurrencies from poor

---

[65] Arizona Attorney General, 'FinTech – FAQs' (2018) <https://www.azag.gov/fintech/faq> accessed 2 November 2019.

[66] *See generally*, Iris H-Y Chiu, 'A Rational Regulatory Strategy for Governing Financial Innovation' (2017) 8 European Journal of Risk Regulation 743 (arguing that there has been insufficient regulatory focus on governing financial innovation).

[67] For a good discussion of the issues, *see*, Iris H-Y Chiu, 'Decoupling Tokens from Trading: Reaching Beyond Investment Regulation for Regulatory Policy in Initial Coin Offerings' (2018) 3 International Business Law Journal 265; Chiu (n 6).

[68] Reserve Bank of India (n 28) para 6.3.

[69] Weber and Baisch (n 6).

[70] HE Benedetti and L Kostovetsky, 'Digital Tulips? Returns to Investors in Initial Coin Offerings' (2018) <https://ssrn.com/abstract=3182169> accessed 2 November 2019; DA Zetzsche and others, 'The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators' (2019) 63(2) Harvard International Law Journal 267.

ones. However, a crucial observation is that participation in an ICO that has come about via a sandbox may lack appropriate regulatory protection for disgruntled investors. There are valid concerns to be ironed out given that crypto-assets such as Bitcoin are frequently used to facilitate criminal activity and also expose inexperienced retail investors to considerable risk.[71] This illustrates the regulatory dilemmas that exist surrounding satisfactory reconciliation of a pro-innovation stance with a risk protection imperative when administering a regulatory sandbox.

A further issue arises in relation to how thoroughly sandbox applications are vetted for fitness and probity. Notably, competitive rivalry between sandboxes within a broader FinTech competition agenda is driving a trend towards both the type of information assessed at the application stage being watered down, and decisions being made and communicated in a relatively short pre-determined time, rather than based on an objective, substantive assessment by the regulator which leaves it suitably informed and ready to make its decision. As competition for a slice of the FinTech pie has heated up, a number of jurisdictions have sought to give their sandbox an enhanced competitive edge by introducing expedited decision-making with a view to enabling innovative products to come to market more quickly. An expedited application process reduces the burden on firms in relation to the time and financial resources committed to the application process. Malaysia and Singapore have come to the fore in this respect. The Central Bank of Malaysia is expected to reach a decision on applications within a remarkably quick time of 15 working days.[72] Singapore's Sandbox Express provides a 21 day model for insurance broking, recognised market operators and remittance businesses.[73] Applications for the Sandbox Express are truncated and considered based on an evaluation of the technological innovativeness of the relevant product or service and on a fitness and propriety assessment with a view to fast-tracking decisions. In India, a four week time to decision is on the table.[74] It is too early to say whether these developments will have a deleterious effect in individual cases, but with truncated decision-making, there

---

[71] A fuller consideration of investor protection issues is outside the scope of this paper.

[72] Bank Negara Malaysia, *Financial Technology Regulatory Sandbox Framework* (2016) <www.bnm.gov.my/index.php?ch=57&pg=137&ac=533&bb=file> accessed 2 November 2019.

[73] Monetary Authority of Singapore, 'MAS Launches Sandbox Express for Faster Market Testing of Innovative Financial Services' (Media Release, 2019) <https://www.mas.gov.sg/news/media-releases/2019/mas-launches-sandbox-express-for-faster-market-testing-of-innovative-financial-services> accessed 2 November 2019.

[74] Reserve Bank of India (n 28) para 7.2.1. This, however, relates to preliminary screening. A further three-week assessment period is provided for, following a four-week test design phase.

certainly seems to be potential for inadequate risk-assessment with consequent adverse implications for the public good during testing and beyond.[75]

A. Disclosures

Disclosures perform an important function in drawing consumers' attention to risk. Most sandboxes have specific rules in relation to informing potential consumers in relation to the restricted nature of the sandbox. Customers of sandbox participants are notified of the potential risks of participating in the testing and are obliged to give their informed consent indicating that they understand and accept the risks.[76] There may also be a requirement to make consumers aware of available redress mechanisms. In jurisdictions where consumer protection is restricted during the sandbox period, as compared to on the open market, consumers must be duly notified of such restriction.[77] Until the regulatory sandbox, as a regulatory innovation, matures and is subject to empirical study, it is difficult to fathom the effectiveness of disclosures in influencing the market behaviour of prospective sandbox consumers and investors. The potential cautionary effects of such disclosures may be counteracted by press releases from regulators trumpeting the admission of the latest participants to their sandbox, thus lending an air of credibility to proceedings that may cause market actors to unduly relax their guard. This shows the delicate tightrope that FinTech regulators must walk as they negotiate promoting innovation with micro-prudential and macro-prudential objectives.

B. Risk Mitigation

Small-scale testing over a defined period of time within a sandbox helps to minimise consumer risk. Nonetheless, one of the most important design aspects of the testing environment provided by any regulatory sandbox is the nature of the controls provided concerning how risk is mapped and contained. It is common for a bespoke framework of protections to be agreed upon by regulators with each sandbox participant, tailored to the nature of the testing activity. Regulators face a multi-faceted challenge in designing

---

[75] In Singapore, for applications that are complex and require more time to assess, the MAS may decide not to consider the application under the Sandbox Express and instead assess it under the customised sandbox approach.

[76] *See*, for example, Reserve Bank of India (n 28) para 6.8.2.

[77] In some regulatory sandboxes, consumers can expect to enjoy the same consumer protection and enforcement rights as consumers outside the sandbox in that jurisdiction. Thus, in the UK, consumers in appropriate cases may have recourse to the Financial Ombudsman Services and the Financial Services Compensation Scheme. In other schemes such as the Australian FinTech Licensing Exemption, the protection available to sandbox consumers is truncated.

appropriate investor, consumer and systemic protections, based on anticipating a range of actor responses to a given stimulus.[78] This challenge is multiplied several-fold in the case of FinTech innovation as it involves wading through relatively uncharted waters. The point has been reinforced by the Consultative Group to Assist the Poor:

> New products and services that are tested in a sandbox may present additional risks that may be hard to assess before the service/product is fully launched in the market. These risks may include those stemming from features of the innovation and/or limited regulatory and supervisory capacity (e.g., poorly designed regulatory requirements, whether too light or too burdensome; inadequate supervisory tools necessary for collecting and analyzing the data generated).[79]

In the UK, assignment of a dedicated case officer to sandbox participants helps to support the successful design and operation of the test as well as the navigation of the regulatory framework. Close contact with an FCA case officer is designed to ensure that the business model fits within the regulatory framework and that necessary safeguards are built in.[80] Such mode of continuing discussion, and where appropriate, recalibration, is useful. This model is also on the cards for the RBI's sandbox which counts on the oversight of its FinTech Unit under the guidance of an Inter Departmental Group, benefiting from domain experts.[81] By contrast, stock protections can be built into a FinTech block exemption model that does not require an individual application and approval process. In Australia, a number of safeguards are built in by the Australian Securities and Investments Commission ('**ASIC**') to the FinTech licensing exemption through the imposition of pre-conditions such as consumer protection measures, client and exposure limits, dispute resolution and compensation arrangements. In relation to testing robo-advice products, consumer detriment can be mitigated against by ensuring that the advice generated is audited by appropriately qualified staff provided by the regulator.[82] This solution is of clear benefit to both the sandbox participant and clients. This approach was taken in the UK by the FCA for firms using its sandbox to test robo-advice products.[83] Such safeguards can thus

---

[78] *See further*, N Moloney, 'Regulating the Retail Markets' in Moloney, Ferran and Payne (n 2).

[79] Jenik and Lauer (n 26) 6.

[80] Financial Conduct Authority (n 16) para 2.14.

[81] Reserve Bank of India (n 28) para 7.1.

[82] This is done through qualified financial advisers checking the automated advice provided based on programmed algorithms.

[83] Financial Conduct Authority (n 16) para 4.42.

mitigate the risk of unsuitable or incorrect advice being provided both while live testing is occurring and thereafter.

It bears mentioning that since the global financial crisis, policy-makers have moved from a conception of the financial citizen as empowered to a more protective stance in relation to consumers as in need of fair treatment.[84] In the domain of new FinTech products and services, investors of varying hues are at risk of falling for hype and not being suitably informed as to what could go wrong and the consequences therein. Appropriate types of consumer protection measures for sandbox testing will vary depending on factors such as the business model and the nature of technology employed. Restrictions of scale are likely to be imposed in order to contain risk, both for individual consumers and to avoid risks that would impact on financial stability more generally. Along with capital limits, restrictions may be imposed on the number of consumers[85] and on the frequency of transactions. Where relevant, it is common to impose quantifiable restrictions in the form of maximum transaction values and cash holding limits. In some cases, customers may be restricted to a certain profile or market segment better placed to absorb the potential risk. Furthermore, measures to shore up data privacy and cybersecurity are key matters of concern.[86]

A consumer redress mechanism may be tailored, including specification of the availability of financial compensation to customers in the testing period in specified circumstances. Sandbox participants must generally demonstrate that they have the resources to be able to compensate customers in the event of any loss suffered during testing. Reflecting this, for sandbox participants trialling the use of digital currencies in money remittance underpinned by DLT, a safeguard built in by the UK's FCA requires participants to guarantee any funds lost in the transmission process.[87] This underpins the importance of reliable and efficient payment mechanisms. The Indian RBI sandbox framework opts instead for an insurance requirement to cover losses.[88]

The biggest issue in judging whether a regulatory sandbox compromises appropriate regulation relates to the matter of regulatory reliefs being afforded to participants, and it is to this question that we now turn.

---

[84] D Kingsford Smith and O Dixon, 'The Consumer Interest and the Financial Markets' in Moloney, Ferran and Payne (n 2).

[85] In Arizona, a cap of 10,000 Arizona-resident consumers is imposed.

[86] RP Buckley and others, 'The Dark Side of Digital Financial Transformation: The New Risks of FinTech and the Rise of TechRisk' (2019) European Banking Institute Working Paper No. 54 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3478640> accessed 2 November 2019.

[87] Financial Conduct Authority (n 16) para 4.9.

[88] Reserve Bank of India (n 28) para 6.8.3.

V. A Hierarchy of Models of Regulatory Relief in Sandboxes

Responsive regulation needs to be responsible. Public gatekeeper functions and regulatory controls should not take a back seat in the race to attract FinTech start-ups. This dilemma has parallels with the debate on the market for corporate incorporations, with the race for pre-eminence in the United States being won hands down by Delaware for its pro-management corporate law framework.[89] Like the market for incorporations, regulatory fragmentation enables competition among regulatory sandbox regimes. Jurisdictions vary in terms of the sectoral regulator's power to relax or waive regulatory requirements for sandbox users. Weber and Baisch caution that "*watering down and softening proven regulatory concepts should not be done recklessly.*"[90] Indeed, some jurisdictions have come out firmly against regulatory sandboxes in so far as they embody regulatory dilution. The role of expanding competition suggests a public interest mandate in promoting consumer choice, price and efficiency. This is a completely different driver than a risk-reduction regulatory model which typically stems from a regulatory focus on mitigating the potential for systemic harm and harm to the consumer. In the zeal to embrace FinTech, a legitimate and unavoidable question concerns how easily these two mandates can be reconciled. These divergent drivers create the potential for regulatory friction. Clearly, a competition promotion mandate should not come at the expense of appropriate investor protection and concern for market stability.[91] It has been contended that while a race to the bottom is a concern, this is outweighed by the "*dire need of more competition*" in financial services markets.[92] Within oppor-

---

[89] K Greenfield, 'Democracy and the Dominance of Delaware in Corporate Law' (2004) 67(4) Law and Contemporary Problems 105; F Stevelman, 'Regulatory Competition, Choice of Forum, and Delaware's Stake in Corporate Law' (2009) 34(1) Delaware Journal of Corporate Law 57. In a European context, *see*, C Kirchner, RW Painter and Wulf Kaal, 'Regulatory Competition in EU Corporate Law after *Inspire Art*: Unbundling Delaware's Product for Europe' (2005) 2 European Company and Financial Law Review 159; D Ahern, 'The Societas Unius Personae: Using the Single-Member Company as a Vehicle for EU Private Company Law Reform, Some Critical Reflections on Regulatory Approach' in AJ Viera Gonzalez and C Teichmann (eds), *Private Companies in Europe: the Societas Personae (SUP) and the Recent Developments in the EU Member States* (Thomson Reuters Aranzadi 2016) 55.

[90] Weber and Baisch (n 6) 337.

[91] Competition and potentially, financial stability challenges are posed by TechFins (large technology companies (the acronym 'GAFA' is used to refer to Google, Apple, Facebook, and Amazon) entering the FinTech space. For a discussion of the issues and the case for a potential monitoring role for RegTech, *see*, DW Arner, J Barberis and RP Buckley, 'FinTech, RegTech and the Reconceptualization of Financial Regulation' (2017) 33 Northwestern Journal of International Law and Business 371; RP Buckley and others (n 86).

[92] Buckley and others (n 13) 21.

tunity-based regulation, a robust regulatory approach should, however, dictate that where such a dilemma presents itself, risk minimisation must be prioritised. In the UK, a statutory cue is provided that in the event of a clash, consumer protection and market integrity trump promoting effective competition.[93]

Within the EU, both Germany and France have exhibited robust anti-sandbox sentiment and are not in favour of providing regulatory sandboxes, with BaFin, the German regulator, said to be against providing 'little buckets and spades'.[94] These regulators are sending a distinct message – that FinTech should not be afforded special treatment and that risk protection is the paramount concern of the regulator. Within the regulatory culture that prevails in Germany, the FinTech industry itself is also keen to avoid the reputational damage which admission to a special regulatory environment might yield.[95] Notably, no dual competition mandate exists in Germany. The solution here for inexperienced firms is to find a licensed co-operation partner to provide a stepping stone before going it alone to seek regulatory authorisation. There has also been strong opposition in the United States to the possibility that legislative reforms might involve regulatory requirements being waived for FinTech.[96]

Jurisdictions vary in terms of the latitude afforded to the regulator to relax or waive regulatory requirements for sandbox participants. While providing regulatory relief to participants divides opinions, it is in essence an agile regulatory adaptation to harsh or unwieldy regulatory topography. As the United States Treasury Department puts it, "*[a] regulatory environment with largely binary outcomes — either approval or disapproval — may lack appropriate flexibility for dealing with innovations.*"[97] A hierarchy or sliding scale of models of regulatory relief observed in different regulatory sandbox systems that have emerged to date is presented below. Four primary models characterising an observed continuum of national regulatory

---

[93] Financial Services and Markets Act 2000, s 1B(4) (as substituted by s 6 of the Financial Services Act 2012).

[94] Attributed to Felix Hufeid, President of the German Federal Financial Services Supervisory Authority (BaFin): C Kociok, 'No Regulatory Sandbox in Germany' (*GreenbergTraurog*, 27 April 2017) <www.gtlaw-financialservicesobserver.com/2017/04/no-sandbox-in-germany/> accessed 2 November 2019.

[95] ibid.

[96] *See*, the opposition engendered by the Financial Services Innovation Bill introduced in the House of Representatives in 2016 (The Financial Services Innovation Act of 2016, HR 6118, 114th Cong 2016). *See further*, LG Thomas, 'The Case for a Federal Regulatory Sandbox for Fintech Companies' (2018) 22 North Carolina Banking Institute 257, 268-269.

[97] United States Department of the Treasury (n 53) 167.

approaches to sandboxes are evident, each sending different signals to would-be participants.

A. No Relaxation of Applicable Rules

The first category of regulatory sandbox predicates that no relaxation of rules is available to sandbox users. It evinces a strict letter of the law approach. Participants are subject to applicable legislation at all times. This has the consequence that participants in the sandbox do not receive more favourable treatment than those outside it in relation to the applicability of relevant rules. The Danish Financial Supervisory Authority's regulatory sandbox, FTLab, which opened in 2018, provides an example of this approach. Not permitting a relaxation of the rules during the sandbox test period helps to meet concerns in relation to equality of access. What marks this type of sandbox out from forms of informal FinTech supports such as innovation hubs is that the assistance provided to chosen participants is more formalised and concentrated.

B. Relaxation of Applicable Rules Permitted Only Within the Discretionary Scope of Existing Rules

The second category is a variant on the first and occurs where there is an inbuilt discretion in the relevant regulatory rules to relax their application, with the sandbox operating within this framework. This model has particular potential within the EU where national regulatory authorities are required to apply relevant EU financial services legislation but are permitted to work within any in-built flexibility in these instruments in relation to their application to FinTech. EU financial services law enshrines a principle of proportionality whereby regulatory and supervisory requirements are to be applied having regard to matters such as the size and risk profile of the firm concerned as well as the nature and complexity of the risks inherent in the business model.[98] The EU's FinTech Action Plan expressly tips off Member States in relation to this possibility:

> National competent authorities must apply relevant EU financial services legislation. However, these rules include a margin of discretion with regard to the application of the proportionality and flexibility principles embedded in these rules. This can be particularly useful in the context of technological innovation.[99]

---

[98] *See further*, European Supervisory Authorities (n 12) para 30.
[99] European Commission (n 5).

To date, the UK's FCA has followed this approach in applying the EU financial services rulebook.[100] For the FCA sandbox, most firms are required to have a restricted authorisation in order to enter the test environment. This ensures that the firm has the requisite competence and financial wherewithal needed to carry on the relevant business with an appropriate degree of consumer and investor protection. However, sandbox tools provided by the FCA potentially include rule waivers and no-enforcement action letters (comfort letters). That said, despite signalling the potential for rule waivers in individual cases, anecdotal evidence suggests that to date, the FCA has not relaxed actual regulatory requirements for any sandbox user. The Norwegian regulatory sandbox for the FinTech industry, created by the Financial Supervisory Authority of Norway meets this model, with the supervisory authority having the power to suspend certain requirements based on the principle of proportionality to the extent permitted by the regulatory regime.[101]

C. Block Exemption Licence

While application to a general regulatory sandbox may result in the creation of a customised sandbox, a block exemption licence model would not. A block exemption approach is intended to provide a pre-defined sandbox with pre-determined parameters including in relation to available regulatory reliefs. Using a block exemption approach signals to FinTech innovators that they can opt-in based on an autonomous determination of eligibility by the regulatory actor.

This model is evident in Australia, Switzerland and Singapore. In Australia, ASIC has exercised its statutory relief powers to provide a FinTech licensing exemption for a period of up to 12 months, free from the need to have an Australian financial services or credit licence.[102] ASIC uses a white list approach such that firms can satisfy themselves that they come within criteria for validation testing and notify ASIC of intention to test without

---

[100] A post-EU withdrawal approach remains to be seen but is likely to remain consistent.

[101] The Norwegian Ministry of Finance asked the Financial Supervisory Authority of Norway to establish a FinTech regulatory sandbox in 2019. It was established in December 2019. *See further*, M Wilhelm, 'Regulatory Sandbox for the Fintech Industry Coming to Norway in 2019' (*Simonsen Vogt Wiig*, 14 November 2018) <https://svw.no/aktuelt/aktuelt/20182/november/regulatory-sandbox-for-the-fintech-industry-coming-to-norway-in-2019/> accessed 2 November 2019.

[102] ASIC Corporations (Concept Validation Licensing Exemption) Instrument 2016/1175 and ASIC Credit (Concept Validation Licensing Exemption) Instrument 2016/1176. *See further*, ASIC, *Testing FinTech Products and Services without Holding an AFS or Credit Licence* (Regulatory Guide 257, 2016) <https://download.asic.gov.au/media/4420907/rg257-published-23-august-2017.pdf> accessed 2 November 2019.

any requirement that ASIC issue an approval.[103] A number of safeguards are built in through the imposition of pre-conditions such as consumer protection measures, client and exposure limits, dispute resolution and compensation arrangements. There is no exemption from other laws such as anti-money laundering or tax laws. Switzerland's regulatory sandbox, introduced in 2017 for projects in banking, involves a licence-free innovation area or sandbox by means of an amendment to the Banking Ordinance.[104] Crucially, this means that FinTech companies carrying out relevant activities can test without a banking licence. In 2019, Singapore introduced a fast-track sandbox (to complement its pre-existing general regulatory sandbox) named the Sandbox Express, built on a block exemption approach.[105] The objective is to enable certain lower risk and well-understood activities to enter the experimentation phase and test more quickly by providing pre-defined sandboxes to cover insurance broking, recognised market operators and remittance businesses.[106]

D. Tailor-Made Sandbox Based on Relaxation of Specific Rules

The most radical category of sandbox is the tailor-made sandbox whereby discretionary relaxation of rules for individual sandbox users is permitted and no such flexibility is provided to entities outside the sandbox. The tailor-made sandbox model permits relaxation of rules on a case by case basis to create an individualised sandbox for FinTech entrepreneurs. This is a regulatory trump card for countries positioning themselves as key FinTech centres and signalling their willingness to facilitate new business models. Opportunity-based regulation involving relaxation of the regulatory framework is clearly considered justifiable by these regulators in helping to get nascent FinTech innovation out of the traps. However, care needs to be taken that due attention is paid to risks as well as opportunities in making that compromise.

In contemplating a relaxation of otherwise applicable rules, this model of regulatory sandbox goes counter-clockwise to the trend of post-global

---

[103] This dispensation from the need for an Australian Financial Services Licence or credit licence applies, for example, to stored value card products and the provision of certain foreign exchange services.

[104] Relevant operators are not regarded as accepting deposits from the public on a commercial basis if the sums deposited do not exceed CHF 1 million and certain other criteria are met.

[105] Monetary Authority of Singapore (n 73).

[106] Monetary Authority of Singapore, *Sandbox Express* (Consultation Paper P015, 2018) <www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Consultation%20Papers/2018%20Nov%20Sandbox%20Express/Consultation%20Paper%20on%20Sandbox%20Express.pdf> accessed 2 November 2019.

financial crisis regulation where the regulatory landscape for financial services has seen accretions of more regulation rather than less. In a sandbox design allowing regulatory requirements to be relaxed for participants, there is an obvious concern that this may compromise consumer protection. That said, such relief is generally ring-fenced – where regulatory requirements are relaxed for entities admitted to the sandbox, this is usually confined to the sandbox testing period. Unless the jurisdiction allows for a tailored regulatory regime to be negotiated upon sandbox exit, entities will need to obtain the requisite regulatory approvals generally applicable outside of the sandbox. Although it is early days and regulators are still dipping their toes in the waters of regulatory flexibility, it bears pointing out that a lack of transparency in relation to how far rules may be bent is problematic. For instance, Malaysia's National Regulatory Sandbox Initiative somewhat opaquely contemplates 'regulatory flexibilities' being afforded.[107]

Jurisdictions where tailored regulatory relaxation is permitted include the State of Arizona (United States), Brunei, Canada, Hong Kong, Indonesia, Malaysia and Singapore. The approach taken by Malaysia as a competitive regulatory strategy was elaborated upon by a policy insider as follows:

> With the Sandbox, we are willing to "flex" rules and regulations to enable testing where we deem that the solution contains strong value proposition and the risks can be appropriately contained. This will also allow us to reduce time to market for new innovative products, which under normal process, might get stifled by regulatory hurdles. It enables us to ensure that our regulatory framework is relevant and responsive to innovations that can bring game changing outcomes to our financial services sector.[108]

Rather than a consensus approach emerging, each regulator has approached regulatory relaxation in its own way. The Hong Kong Monetary Authority has the power to relax supervisory requirements for incumbent banks admitted to its FinTech Supervisory Sandbox launched in 2016 to enable banks to engage in pilot tests of FinTech initiatives such as biometric authentication.[109] In Singapore, the Monetary Authority of Singapore's regu-

---

[107] Bank Negara Malaysia, *Financial Technology Regulatory Sandbox Framework* (2016) para 1.5 <www.bnm.gov.my/index.php?ch=57&pg=137&ac=533&bb=file> accessed 2 November 2019.

[108] Encik Aznan bin Abdul Aziz, 'Financial Technology Enabler Group (FTEG) Chairman's Opening Remarks at Finnovasia KL' (Finnovasia, Kuala Lumpur, Malaysia, 20 March 2017) <http://www.bnm.gov.my/index.php?ch=en_speech&pg=en_speech&ac=721&lang=en> accessed 2 November 2019.

[109] Norman TL Chan, 'Speech by Mr Norman T L Chan, Chief Executive of the Hong Kong Monetary Authority' (HKMA Fintech Day, Hong Kong, 11 November 2016) <www.bis.

latory sandbox permits the creation of a customised sandbox for participants whereby certain legal and regulatory requirements may be relaxed for an entity for the duration of the sandbox.[110] Examples of these are provided in the relevant sandbox guidelines and include financial requirements such as capital adequacy requirements, as well as matters relating to management experience and existing track record.[111] In India, the RBI Sandbox contemplates relaxation of regulatory requirements on a case by case basis for the duration of the sandbox[112] and the framework provides examples in the form of matters including track record, liquidity requirements and financial soundness.[113] Such flexibility does not extend to KYC requirements, anti-money laundering requirements, counter-financing of terrorism measures and other statutory restrictions.

The Canadian Securities Administrators ('**the CSA**') also plays a role in tailoring bespoke exceptions to securities laws.[114] In Canada, discussion may first occur with the local securities regulator on a case by case basis in relation to the relevant business model and the application of securities laws before submission of an application to the CSA. The CSA will determine the tailored terms and conditions for individual sandbox participation. For example, in 2017, Token Funder Inc. was admitted to the CSA Regulatory Sandbox with a view to launching an initial token offering by means of a private placement and was granted relief from the dealer registration requirement while in the sandbox. However, conditions including KYC requirements were imposed.[115] Somewhat controversially, Québec's financial regulator, Autorité des Marches Financiérs ('**AMF**'), provided Impak Finance, an ICO platform for investing in socially responsible enterprises, with relief from securities regulation requirements concerning not only registration as a securities dealer, but also the provision of a prospectus to investors.[116] These are usually considered standard investor protection measures.

---

org/review/r161111c.pdf> accessed 2 November 2019.

[110] Monetary Authority of Singapore (n 47) Appendix A.

[111] Monetary Authority of Singapore (n 47) Appendix A.

[112] Reserve Bank of India (n 28). Some interpretative confusion is created by the juxtaposition of para 8.1, which states "*the RBI will provide the appropriate regulatory support by relaxing specific regulatory requirements*" where necessary, for the duration of the sandbox, with para 4.3, which states "*the RBI or its RS [regulatory sandbox] cannot provide any legal waivers.*"

[113] Reserve Bank of India (n 28) para 6.2.

[114] Canadian Securities Administrators, *CSA Regulatory Sandbox* (2017) <https://www.securities-administrators.ca/industry_resources.aspx?id=1588> accessed 2 November 2019.

[115] *See*, Canadian Securities Administrators, *Decision in the Matter of Token Funder Inc.* (2017) <https://www.securities-administrators.ca/uploadedFiles/Industry_Resources/DE_TokenFunderInc.pdf> accessed 2 November 2019.

[116] A Stanley, 'ICO Ban? Canada's Regulators are Giving One Token Sale a Big Break' (*CoinDesk*, 6 September 2017) <https://www.coindesk.com/ico-ban-canadas-

Patrick Theoret of AMF reasoned that "*[i]t's in the spirit of the sandbox that we are willing to alleviate some of the requirements on … a test case basis. It's a test run to see whether there are investor protection [issues] with the relief that we grant*."[117] This highlights the role of the sandbox as a contained mutual learning experience.

Open-ended regulatory flexibility permits adaptability and regulatory dialogue. However, any associated lack of certainty in relation to determining the baseline of the regulatory perimeter is absolutely undesirable, not just as a matter of commercial certainty, but more fundamentally, in terms of the need for a core policy determination of where the regulatory bar should be set. Therefore, although the flexibility of the regulatory sandbox is its strength in relation to promoting competition, it may also prove to be its Achilles' heel. While promoting innovation and competition in Fintech markets, regulators need to remember that they are public gatekeepers. Regulatory dialogue is one thing. There needs, however, to be firm limits as to the extent of regulatory flexibility. All market participants ought to be treated equally and fundamental sound principles of financial regulation should not be watered down on a whim even for a time-limited period. Reflecting such concerns, for some, the regulatory sandbox is simply wrong-headed and a tailor-made sandbox, a *non sequitur*. Perhaps the real work can be just as well done by the unsung hero – the innovation hub.[118] It would be wrong to assume that the relatively small number of regulatory sandbox schemes in existence across the globe to date is simply attributable to many regulators lagging behind early adopters. In some countries, regulators are privately unconvinced that a regulatory sandbox is an appropriate part of the toolbox of a regulator in their distinct regulatory landscape and regulatory culture. These concerns ought to be weighed in the balance in inter-regulator and stakeholder dialogue on the regulatory sandbox, and the future of FinTech regulation and innovation facilitation.

VI. Conclusion

Transformative technological change is ongoing and regulators are keenly aware of their contribution to facilitating FinTech competition and innovation. Market innovation is forcing regulatory innovation; iterative, agile experimentation and new regulatory strategies. The regulatory sandbox construct, characterised here as opportunity-based regulation, is best understood

---

regulators-giving-one-token-sale-big-break> accessed 2 November 2019.

[117] Stanley (n 116).

[118] Buckley and others (n 13).

contextually within, if not a regulatory vacuum, a slowly evolving regulatory topography that does not yet meet the specific needs of FinTech markets. A compromise blend of 'softly, softly' and 'wait and see' regulatory stances is accordingly evident in the roll-out of the regulatory sandbox as a two-way learning tool for the regulator and the regulatory actor. Significantly, not only is the regulatory sandbox an experimental phase for firms testing innovative products and services, it is also a novel regulatory experiment as far as regulators are concerned as they use the sandbox to actively learn about new technologies and products and how regulation needs to adapt and respond.

While sandboxes perform a valuable gap-filling role, they are not a regulatory panacea for FinTech. Financial innovation is complex, involving technological innovation and disruptive new business models, and presents both benefits and risks. Proportionate regulation is the answer but understanding and devising what is needed will take a considered response. As one regulatory insider astutely puts it, "*Regulation must not front-run innovation. Introducing regulation prematurely may stifle innovation and potentially derail the adoption of useful technology.*"[119] The proliferation of the regulatory sandbox phenomenon is indicative of a willingness among regulators to boost the FinTech economic bounce with an adaptive regulatory stopgap for the brightest FinTech innovators. The broader coherence and competition challenges for FinTech, posed by global regulatory fragmentation, will continue. In the meantime, there is considerable potential for calculated forum shopping by mobile FinTech entrepreneurs as they work out what opportunities are offered by available regulatory sandboxes.

In forging ahead with a competition promotion agenda, regulators need to be sensitive to the ripple effects of a regulatory sandbox on barriers to entry and natural selection in the market. The tailor-made regulatory sandbox model evident in some jurisdictions heralds bespoke regulation for a sandbox in-group, thus creating a multi-tiered regulatory framework. This is a remarkable development. As we tread a careful path from the global financial crisis, care must be taken not to compromise appropriate regulation. A fundamental regulatory issue for each jurisdiction to confront concerns the justifiability of granting full or partial waiver of core regulatory requirements to sandbox participants, even for a time-limited period.

---

[119] R Menon, 'Remarks of R Menon, Managing Director, Monetary Authority of Singapore' (Singapore Forum, Singapore, 2 April 2016) <https://www.finews.asia/finance/23415-ravi-menon-monetary-authority-of-singapore-fintech-innovation-blockchain-lattice-80> accessed 2 November 2019.

The Case for Regulating Crypto-Assets: A Constitutional Perspective

Jaideep Reddy[*]

Abstract *In July 2019, the Ministry of Finance, Government of India announced that an Inter-Ministerial Committee (the '***Committee***') had submitted its report (the '***Committee Report***') recommending that possessing or dealing with cryptocurrency be banned and made a criminal offence. This article examines whether such a ban is justified under our constitutional scheme. The article finds that the right to carry on various kinds of crypto-asset activities can be traced to various enumerated fundamental rights under the Constitution of India. Analyzing the Committee Report, the article finds that its recommendation of an outright ban is unlikely to be a reasonable restriction on these rights, as such a ban is likely arbitrary and excessive. Since crypto-assets are a value-neutral platform technology - akin in many ways to the Internet - the article recommends that an empirical approach be adopted towards studying any risks associated with crypto-assets, and that a regulatory approach be adopted to mitigate these risks rather than an outright prohibition. This would comport with the interests of liberty, innovation, and consumer protection.*

[*] Leader, Technology Law, Nishith Desai Associates. The views expressed in this article are personal. The author would like to acknowledge the discussions had with various colleagues while developing the views in this article. As a note of disclosure, the author was part of the team representing the Internet and Mobile Association of India and another petitioner in their writ petition in the Supreme Court against the Reserve Bank of India circular on 'virtual currencies'. The Court in that case held that the circular was a disproportionate restriction on fundamental rights. Since the judgment was pronounced when the article was in the final stages of editing, and since this article is primarily focused on the Inter-Ministerial Committee's report, references to the case are made only to the extent necessary to comment on the report.

I. Nature of Crypto-Assets

Traditionally, reliable transfers of value on the Internet required central intermediaries, eg, banks and clearing houses. This was in order to ensure that bad actors did not use the same units of value more than once (a phenomenon known as 'double-spending'; the physical world analogy is counterfeiting).

Cryptocurrencies, or 'crypto-assets',[1] generally aim to enable the reliable transfer of value over the Internet without central intermediaries, while still not allowing double-spending.[2] In other words, they seek to provide a secure and decentralized means of transferring value online.

The first crypto-asset was Bitcoin, introduced by a seminal white paper in 2008.[3] Other cryptographic systems had tried and failed to achieve a similar end.[4] For this reason, among others, the Bitcoin system has been globally recognized as a breakthrough in computer science and cryptography.[5] The Institute for Development and Research in Banking Technology (IDRBT), established by the Reserve Bank of India (RBI), has called Bitcoin a "*groundbreaking application*".[6]

---

1 This article uses the term 'crypto-assets' in line with the international legal trend, because crypto-assets have so far not shown wide adoption as a currency.

2 Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' <https://bitcoin.org/bitcoin.pdf> accessed 4 June 2020.

3 ibid.

4 Arvind Narayanan and Jeremy Clark, 'Bitcoin's Academic Pedigree' (2017) 15(4) ACM Queue <https://queue.acm.org/detail.cfm?id=3136559> accessed 4 June 2020.

5 ibid 15 which states that '*Understanding all these predecessors that contain pieces of bitcoin's design leads to an appreciation of the true genius of Nakamoto's innovation*'; See Yossi Gilad and others, 'Algorand: Scaling Byzantine Agreements for Cryptocurrencies' (2017) Proceedings of the 26th Symposium on Operating Systems Principles 51, 51 <https://people.csail.mit.edu/nickolai/papers/gilad-algorand-eprint.pdf> accessed 4 June 2020 which states '*Cryptographic currencies such as Bitcoin can enable new applications, such as smart contracts and fair protocols, can simplify currency conversions, and can avoid trusted centralized authorities that regulate transactions*'; Luke W. Vrotsos and Cindy H. Zhang, 'Harvard Invests Millions in New Cryptocurrency' *The Harvard Crimson* (12 April 2019) <https://www.thecrimson.com/article/2019/4/12/hmc-crypto-investment/> accessed 4 June 2020; Digital Currency Initiative <https://dci.mit.edu/> accessed 4 June 2020.

6 Institute for Development and Research in Banking Technology, *Applications of Blockchain Technology to Banking and Financial Sectors in India* (IDRBT, White Paper, 2017) chs 1, 3 <https://www.idrbt.ac.in/assets/publications/Best%20Practices/BCT.pdf> accessed 4 June 2020.

II. Crypto-assets are a Value-Neutral, Platform Technology

Bitcoin was introduced to reduce transactions costs of financial intermediaries and mitigate a certain type of credit card fraud known as chargeback fraud.[7] Its benign goal was to increase efficiencies in e-commerce transactions.[8] It also appears to have sought to preserve privacy to the extent that stock exchanges and banks already did.[9] This is not to run away from the fact that crypto-assets have also proven to be a vehicle for crime in many cases, and present new challenges to law enforcement.[10] Rather, it is meant to show that the system is not designed with any negative values embedded, but rather was intended to create a new technology to facilitate existing commerce.

For reasons beyond the scope of this article (but most notably, price volatility), crypto-assets like Bitcoin have not made a compelling case to be used as a means to purchase and sell everyday goods and services. However, crypto-assets still present some tangible benefits, some of which have materialized and some of which are emerging. Some examples are discussed below:

- Software applications: Most notably, after the creation of Bitcoin, crypto-asset networks like Ethereum emerged, which allow computer programmers to run their software applications on a decentralised network, as opposed to a central server or a set of servers.[11] This aims to decentralise the risk associated with running a software application on a single server maintained by a single entity, in case that server suffers from downtime or is compromised, or the entity is

---

7 Nakamoto (n 2).

8 Nakamoto (n 2).

9 Nakamoto (n 2) states, '*The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. ... The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.*' One notes that stock exchanges and banks are generally regulated by Know Your Customer (KYC) obligations. However, this is a matter of regulation and not the design of the system. As discussed subsequently, jurisdictions like the E.U. and Canada have begun to impose KYC obligations on crypto-asset intermediaries. Further, there is still generally no KYC system globally for physical cash.

10 Eg, Water Pavlo, 'Crime and Punishment in the Cryptocurrency World' <https://www.forbes.com/sites/walterpavlo/2020/02/25/crime-and-punishment-in-the-cryptocurrency-world/#5ac7ede748fe> accessed 4 June 2020.

11 *A Next-Generation Smart Contract and Decentralized Application Platform* (An introductory paper to Ethereum, introduced before launch, which is maintained) (White Paper, Ethereum Foundation, 2013-19) <https://github.com/ethereum/wiki/wiki/White-Paper> accessed 4 June 2020.

untrustworthy. Programmers run their software applications on the network by paying fees to the network in crypto-assets (in Ethereum, the crypto-asset is known as 'Ether').[12] The network in turn allocates these fees to the participants per a pre-determined logic. Instead of fees accumulating to a single entity, fees are distributed to a greater network of participants, in small chunks. This system of compensation may not be feasible through the traditional financial system due to the number of participants, the small size of transactions, and the automated exchange of value through 'smart contracts'. As institutional endorsement of this technology, over 500 firms globally (including Accenture, AMD, BBVA, BP, Credit Suisse, Deloitte, Government of Andhra Pradesh, HP, Infosys, ING, Intel, JP Morgan, Microsoft, Pfizer, Thomson Reuters, Samsung, and Santander) chose to form the 'Enterprise Ethereum Alliance', a non-profit corporation, to collaborate to develop enterprise blockchain solutions based on the Ethereum network (there are other platforms like Ethereum such as EOS and Stellar, and each – being at a relatively early stage – is finding its feet technologically). With these innovations, the wider software development community in India and abroad is now looking to acquire skills in developing decentralized software applications using crypto-assets.[13]

- Remittance: India was found by the World Bank to be the largest receiver of inward migrant remittances globally in 2018, receiving USD 79 billion.[14] The same report of the World Bank also noted that the average cost of receiving remittances in South Asia was 5.2% in the first quarter of 2018, which would translate to a cost of approximately USD 4.1 billion, or approximately INR 28,914 crore, annually for India. By contrast, some crypto-asset networks promise cost-savings of up to 60% on cross-border remittances.[15] This would translate to cost-savings of approximately INR 17,348 crore a year for the

---

[12] ibid.

[13] Eg, Khwaja Shaik, 'The Top 10 Blockchain Skills you Need to Develop' (*IBM*, 1 March 2018) <https://www.ibm.com/blogs/blockchain/2018/03/the-top-10-blockchain-skills-you-need-to-develop/> accessed 4 June 2020.

[14] World Bank Group and Knomad, *Migration and Remittances, Recent Developments and Outlook* (Migration and Development Brief, April 2019) <https://www.knomad.org/sites/default/files/2019-04/Migrationanddevelopmentbrief31.pdf> accessed 4 June 2020; World Bank Group, *Record High Remittances Sent Globally in 2018* (Washington, Press Release No. 2019/1488, April 2019) <https://www.worldbank.org/en/news/press-release/2019/04/08/record-high-remittances-sent-globally-in-2018> accessed 4 June 2020.

[15] Monica Long, 'Ripple and XRP Can Cut Banks' Global Settlement Costs Up to 60 Percent' (*Ripple: Insights*, 23 February 2016) <https://ripple.com/insights/ripple-and-xrp-can-cut-banks-global-settlement-costs-up-to-60-percent/> accessed 4 June 2020.

country; for perspective, this amounts to the expenditure of India's nationwide Mid Day Meals scheme for close to 2 years.[16]

- Store of value: Individuals today choose a variety of investment avenues including bank deposits, company shares, real estate, foreign currency, and commodities. Crypto-assets present an additional investment avenue for those who see promise in the future of the technology, based on the above or other use-cases.

The above illustrations are not intended to comment on whether crypto-assets and blockchain technology will ultimately prove to be effective or successful. Of that, time may be the best judge, and the technology is still finding its feet. However, the above illustrations are meant to show that crypto-assets are not inherently good or bad, but are a platform technology holding significant promise. They can only be normatively or legally assessed based on the use to which they are put. In that aspect, they can be likened to platform technologies of yore, each of which did not emerge without societal fears of severe harm: electricity, railways, telecommunications, motor vehicles, aircrafts, mobile phones, and the Internet.[17] In fact, in its early years, even the company business structure was criticized by well-known thinkers of the time.[18] These technologies and innovations are different in nature to phenomena which are considered by Indian law to be inherently pernicious, such as gambling, immoral trafficking, alcohol, or narcotic substances (activities known as *res extra commercium*).[19] Crypto-asset systems should hence be treated by the law on the same plane as platform technologies like the Internet (which are regulated), rather than as vices or socially harmful activities (which are banned outright).

---

[16] Ministry of Finance-Government of India, *Expenditure Profile 2017-2018* (2018) 25 <https://www.indiabudget.gov.in/budget2017-2018/ub2017-18/eb/stat4a.pdf> accessed 4 June 2020.

[17] Nishith Desai and others, *Building a Successful Blockchain Ecosystem for India: Regulatory Approaches to Crypto-Assets* (Research Paper, December 2018) 2 <http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research_Papers/Building-a-Successful-Blockchain-Ecosystem-for-India.pdf> accessed 4 June 2020; See Nathaniel Whittemore, 'PODCAST: Josh Brown on Why Bitcoin is like the 1800s Railroad Boom' (*Coindesk: Bitcoin Macro*, 8 November 2019) <https://www.coindesk.com/podcast-josh-brown-on-why-bitcoin-is-like-the-1800s-railroad-boom> accessed 4 June 2020.

[18] Adam Smith, *An Inquiry into the Wealth of the Nations* (Book V, 1776) 374 <http://media.bloomsbury.com/rep/files/primary-source-93-adam-smith-the-wealth-of-nations-on-joint-stock-companies.pdf> accessed 4 June 2020.

[19] *Khoday Distilleries Ltd. v State of Karnataka*, (1995) 1 SCC 574, para 60 (*Khoday case*).

III. Constitutional Freedoms Associated with Crypto-Assets

In our constitutional scheme, it is well-settled that fundamental rights are to be construed liberally with rights-holders being at center stage and the State being highly accountable.[20] Ten Judges of the Supreme Court of India in *Rustom Cavasjee Cooper* v. *Union of India*[21] (known as the Bank Nationalisation case) held:

> Impairment of the right of the individual and not the object of the State in taking the impugned action, is the measure of protection. To concentrate merely on power of the State and the object of the State action in exercising that power is therefore to ignore the true intent of the Constitution. ... Protection of the right to property or personal freedom is most needed when there is an actual threat. To argue that State action which deprives a person permanently or temporarily of his right to property, or personal freedom, operates to extinguish the right or the remedy is to reduce the guarantee to an empty platitude. Again to hold that the extent of, and the circumstances in which, the guarantee of protection is available depends upon the object of the State action, is to seriously erode its effectiveness. (emphasis added)

With that in mind, various constitutional and fundamental rights dealing with crypto-assets are discussed below. It goes without saying that these rights are subject to reasonable restrictions contemplated by the Constitution.

1. The right to trade and do business under Articles 19(1)(g) and 301: Persons carrying out commercial activities such as mining crypto-assets, buying and selling crypto-assets, or bartering crypto-assets would be doing so in exercise of their fundamental right under Article 19(1)(g) and constitutional right under Article 301. The Supreme Court has interpreted the aforesaid Articles to include the right to carry on any trade which is not *res extra commercium* i.e., ("*inherently vicious and pernicious, and is condemned by all civilised societies*", "*immoral and criminal*", and "*articles or goods which are obnoxious and injurious to health, safety and welfare of the general public*").[22] Prominent examples of activities held to be *res extra commercium* in India are alcohol, gambling, and human trafficking.[23] For reasons

---

[20] Eg, *PUCL v Union of India*, (2005) 2 SCC 436.
[21] *Rustom Cavasjee Cooper v Union of India*, (1970) 1 SCC 248.
[22] *Khoday case*.
[23] *Khoday case*; *State of Bombay v R.M.D. Chamarbaugwala*, AIR 1957 SC 699 : 1957 SCR 874; *Cooverjee B. Bharucha v Excise Commr., Ajmer* AIR 1954 SC 220 : 1954 SCR 873.

stated above, crypto-assets are a platform technology with benefits and risks, and dealing with them does not have an immoral or inherently pernicious element. Countries around the world, including the Indian government in various reports as described in this article, have recognized its benefits (while also acknowledging risks). As discussed subsequently, no developed and democratic country has chosen to prohibit crypto-asset activity.

The Supreme Court in *Internet and Mobile Assn. of India* v. *RBI* (the '**IAMAI**' case) has recognized that all those who carry out crypto-asset business activity (other than those who do so as a hobby without any expectation of profit) are entitled to the right under Article 19(1)(g) in respect of such activity.[24]

2. The right to life, liberty and privacy under Article 21: In *K.S. Puttaswamy* v. *Union of India* (the now famous '**Right to Privacy**' case) decided by a Nine Judge Bench of the Supreme Court, various opinions of the learned Judges referred to the autonomy and dignity of the individual as being fundamental to the freedoms guaranteed under the Constitution.[25] The learned Judges upheld the right of individuals to make decisions autonomously as a fundamental right. For instance, Chandrachud, J. (for four learned Judges) held:

"Life is precious in itself. But life is worth living because of the freedoms which enable each individual to live life as it should be lived. The best decisions on how life should be lived are entrusted to the individual. They are continuously shaped by the social milieu in which individuals exist. The duty of the state is to safeguard the ability to take decisions – the autonomy of the individual – and not to dictate those decisions." (emphasis added)

Similarly, Nariman, J. held that the fundamental right of privacy would include the "*privacy of choice, which protects an individual's autonomy over fundamental personal choices. … The dignity of the individual encompasses the right of the individual to develop to the full extent of his potential. And this development can only be if an individual has autonomy over fundamental personal choices*." (emphasis added)

---

[24] *Internet and Mobile Assn. of India v RBI*, 2020 SCC OnLine SC 275.

[25] *K.S. Puttaswamy v Union of India*, (2017) 10 SCC 1. (*Right to Privacy* case)

Observations to a similar effect were made by all the remaining learned Judges who authored opinions viz. Chelameswar, Bobde, Sapre, and Kaul, JJ.

The decision of an individual to participate in a technological and mathematical breakthrough acknowledged by leading institutions worldwide, like crypto-assets, is a fundamental personal choice. Individuals exercise their fundamental personal choice to participate in crypto-assets, whether by writing software programs which use crypto-assets, buying and selling crypto-assets based on the promise of the underlying technology, or 'mining' crypto-assets which contributes to the maintenance of the global network. They do so in exercise of their autonomy to take decisions regarding their own lives. Therefore, it is submitted that the right to participate in a legitimate technological innovation such as crypto-assets would be a part of individuals' right to liberty and privacy under Article 21 of the Constitution.

3. The right to property under Article 300A: In *K.T. Plantation (P) Ltd.* v. *State of Karnataka*, a Constitution Bench of the Supreme Court held that the term 'property' under Article 300A includes intangibles like copyrights and other intellectual property and embraces every possible interest recognised by law.[26] Similarly, according to Black's Law Dictionary, 'property' includes the rights in an intangible, and the said dictionary states that these rights include the right to possess and use, the right to exclude, and the right to transfer.[27] It alternatively defines property as "*any external thing over which the rights of possession, use, and enjoyment are exercised*".[28]

   A crypto-asset is a unit on an Internet-based ledger which can be transacted using a unique 'private key', which is a cryptographic series of characters. Only those who know the private key possess and may transfer the crypto-asset. Crypto-assets are generated or 'mined' by the exertion of computer power to solve non-obvious cryptographic problems, and are thereafter transacted on the basis of the value ascribed by market forces. The holder of the private key excludes

---

[26] *K.T. Plantation (P) Ltd. v State of Karnataka*, (2011) 9 SCC 1 (*K.T. Plantation case*).

[27] *Black's Law Dictionary* (11th ed 2019) states that '***property*** *(14c)* ***1.*** *Collectively, the rights in a valued resource such as land, chattel, or an intangible. It is common to describe property as a "bundle of rights." These rights include the right to possess and use, the right to exclude, and the right to transfer. — Also termed bundle of rights.* ***2.*** *Any external thing over which the rights of possession, use, and enjoyment are exercised <the airport is city property>*'.

[28] ibid.

others from possession and the ability to transfer. Since crypto-assets can be possessed, used, and transferred, and their holder can exclude others from doing these actions, it is submitted that they have the legal characteristics of 'property'.[29]

Since the *K.T. Plantation* case expressly recognizes intangibles, it is difficult to argue that crypto-assets, as a representation of value on the Internet, are not 'property' under Article 300A merely because they are intangible. Importantly, in the *IAMAI* case, the Court recognized that virtual currencies / crypto-assets are a form of 'intangible property'.[30] Its finding that virtual currencies can act under certain circumstances as money does not hamper the argument that crypto-assets are 'property' under Article 300A, since money has been treated as a form of property under the Constitution and under Indian statutes.[31]

Holders of crypto-assets should hence not be deprived of their crypto-assets except in accordance with the principles laid down under Article 300A, i.e., for a public purpose and with payment of compensation in a just, fair, and reasonable manner.[32]

4. Right to free speech and expression under Article 19(1)(a): While the argument is novel and untested globally, it is worth considering whether crypto-asset activity may be protected under Article 19(1)(a) of the Constitution. It is well settled that the freedom of speech and expression under Article 19(1)(a) includes the freedom of propagation

---

[29] Under the General Clauses Act 1897, s 2(36) 'movable property' means 'property of every description, except immovable property'. See also infra n. 31. Crypto-assets would hence be movable property and holders of them would have the rights of holders of any other movable property, such as civil and criminal remedies against theft.

[30] *IAMAI case*, para 6.87.

[31] Eg, *Dwarkadas Shrinivas v Sholapur Spg. & Wvg. Co. Ltd.*, AIR 1954 SC 119 : 1954 SCR 674 para 33 in which while holding a measure to infringe the right to property under (then) Article 31 of the Constitution, Mahajan, J observed, '*[t]he plaintiff and the other preference shareholders therefore are in imminent danger of losing the shares themselves or losing valuable property in the nature of money which they will have to pay out in order to meet the call*.' (emphasis added); Sale of Goods Act 1930, s 2(7) provides that 'goods' means 'every kind of moveable property other than actionable claims and money', thereby demonstrating that the term 'moveable property' includes 'money'. In addition, as mentioned above, a Constitution Bench in the *KT Plantation* case held that 'property' under art 300A embraces 'every possible interest recognized by law.' Further, the Court in the *IAMAI* case recognized that virtual currencies can have characteristics of *both* goods and money, holding at para 6.86, "*[t]herefore, it is not possible to accept the contention of the petitioners that VCs are just goods/commodities and can never be regarded as real money*" (emphasis added).

[32] *K.T. Plantation case*.

of ideas.[33] This freedom has been held to extend to the Internet medium which provides a market place of ideas to persons of all kinds.[34] To the author's knowledge, no Indian court has considered the application of Article 19(1)(a) to computer software programmes or cryptography. However, the U.S. Court of Appeals (Ninth Circuit) has held, in the context of the First Amendment of the U.S. Constitution (providing the right to free speech), that encryption software, in its source code form and as employed by those in the field of cryptography, was protected by the First Amendment.[35] It was held that cryptographers use source code to express their scientific ideas in much the same way that mathematicians use equations or economists use graphs. Separately, the U.S. Supreme Court has also held certain types of election-related corporate expenditure to be protected by the First Amendment, hence showing that free speech can extend to economic elements of expression.[36] In the context of crypto-assets, possibilities of expressive activity include: writing and publishing of the underlying software code; running the code on a computer system; writing, publishing, and running software code for decentralised applications such as 'smart contracts'; expressing the value of things in terms of crypto-assets; and using crypto-assets in contexts intended to be expressive of ideas, such as decentralisation.[37] Due to the lack of judicial precedents on

---

[33] *Romesh Thappar v State of Madras,* AIR 1950 SC 124 : 1950 SCR 594.

[34] *Shreya Singhal v Union of India,* (2015) 5 SCC 1.

[35] *Daniel J Bernstein v US Department of Justice* (9th Cir) No. 97-16686 (May 6, 1999) ("*encryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes… Cryptographers use source code to express their scientific ideas in much the same way that mathematicians use equations or economists use graphs. Of course, both mathematical equations and graphs are used in other fields for many purposes, not all of which are expressive. But mathematicians and economists have adopted these modes of expression in order to facilitate the precise and rigorous expression of complex scientific ideas. Similarly, the undisputed record here makes it clear that cryptographers utilize source code in the same fashion*").

[36] *Citizens United v Federal Election Commission,* 2010 SCC OnLine US SC 10 : 558 US 310 (2010).

[37] Crypto-assets operate only by way of cryptography-based software programmes, written by software programmers in the field of crypto-assets and blockchain technology. Underlying each such software programme is the source code. Further, every crypto-asset transaction is nothing more than a software message propagated to the participants of the network. Every software programmer creating a crypto-asset network and every participant transacting in crypto-assets can therefore be said to be expressing, through source code or software messages, their participation in the new technological innovation. In addition, many blockchain software programs, such as those written on the popular Ethereum network, use a crypto-asset (in Ethereum, 'Ether') as the 'fuel' to enable the operation of the software program. They cannot execute their software programs on these networks without using crypto-assets like Ether. Further, crypto-asset technology has created a new form of transactions which can be enabled over the Internet. Such transactions earlier were not possible

the subject in India, whether Indian courts will recognize crypto-asset activity to be protected by Article 19(1)(a) is uncertain and may depend on the context of the activity over which the right is being asserted.[38] Broadly speaking, any expressive activity which is directly affected[39] by a prohibition on crypto-asset activity may be held to be covered by Article 19(1)(a). Importantly, if a right under Article 19(1)(a) is recognized in the context of crypto-asset activity, the main consequence is that any restriction on the same must necessarily be traced to the itemised grounds under Article 19(2), rather than the more sweeping ground for a restriction under Article 19(6) ("*in the interests of the general public*") vis-à-vis Article 19(1)(g).

5. Rights under Article 14: All persons in India have the right under Article 14 to be free from arbitrary or discriminatory State action. As far as arbitrariness is concerned, a legislation would be invalidated under Article 14 when it is done capriciously, irrationally, without adequate determining principle, and/or is excessive and disproportionate.[40] It must be supported by a relevant consideration of material facts.[41] As far as non-discrimination is concerned, Article 14 essentially requires that among equals the law should be equal and equally administered, and that likes should be treated alike.[42] Any distinction made by the law between persons (i.e., any classification of persons) must be based on intelligible differentia, and the intelligible differentia must have a rational relation to the object sought to be achieved by the Act.[43]

   These principles are applicable to legislative actions and not just administrative actions.[44] For instance, the Supreme Court in the 2013 case of *State of Maharashtra* v. *Indian Hotel & Restaurants Assn.* struck down a Maharashtra Act prohibiting dance performances in eating houses and bars as there was little or no material on the basis of which the State concluded that dancing in the prohibited establishments was likely to deprave, corrupt, or injure public morals.[45]

---

without central intermediaries. By participating in the technology, individuals may express their endorsement and belief in the new ideas introduced by this technology.

38 *Maneka Gandhi v Union of India,* (1978) 1 SCC 248.

39 *Bennett Coleman and Co. v Union of India*, (1972) 2 SCC 788.

40 *Shayara Bano v Union of India,* (2017) 9 SCC 1.

41 *Shri Sitaram Sugar Co. Ltd. v Union of India,* (1990) 3 SCC 223 (*Sitaram case*).

42 *K.R. Lakshman v Karnataka Electricity Board,* (2001) 1 SCC 442.

43 *Special Courts Bill, 1978 , In re*, (1979) 1 SCC 380.

44 *Sitaram case.*

45 *State of Maharashtra v Indian Hotel and Restaurants Assn.,* (2013) 8 SCC 519 as discussed by *Indian Hotel and Restaurant Assn. v State of Maharashtra,* (2019) 3 SCC 429.

The Court also held that it was not a permissible classification to distinguish between exempted establishments (gymkhanas and 3-star or higher hotels) and prohibited establishments (all other establishments) as the class of a person could not speak for a person's morality or decency. This case was specifically applied in the *IAMAI* case in the context of the RBI circular on virtual currencies. Persons carrying out crypto-asset activity therefore would have the fundamental right to be free from arbitrary or discriminatory restrictions by the State on this activity.

IV. Reasonable Restrictions

The above rights are not absolute and are subject to reasonable restrictions in accordance with the Constitution. These restrictions are of slightly varying nature depending on the corresponding right. The rights under Article 19 are subject to "*reasonable restrictions*",[46] the right under Article 21 can only be taken away by "*fair, just and reasonable*" procedure established by law,[47] the right under Article 14 can only be taken away on the basis of a reasonable classification as described above, and the right under Article 300A can only be taken away if the State action was for a public purpose and with compensation to the affected persons.[48]

Broadly speaking, fundamental rights can only be impinged upon if the measure is not arbitrary or disproportionate.[49] While non-arbitrariness is a multi-faceted concept, its elements which are relevant to this article are (as held by several cases): (i) a measure is taken with due application of mind and consideration of relevant facts,[50] and (ii) a measure is founded on intelligible differentia (i.e., does not treat equals unequally) which have a rational relation to the objects sought to be achieved.[51]

The test of proportionality requires that: (i) the restrictive measure is designated for a proper purpose; (ii) the measure is rationally connected to the fulfilment of the purpose; (iii) there are no alternative less invasive measures; and (iv) there is a proper relation between the importance of achieving the aim and the importance of limiting the right.[52]

---

[46] *Papnasam Labour Union v Madura Coats Ltd.*, (1995) 1 SCC 501.
[47] *Right to Privacy case.*
[48] *K.T. Plantation case.*
[49] *K.S. Puttaswamy v Union of India,* (2019) 1 SCC 1. (*Aadhaar case*)
[50] *Sitaram case.*
[51] *Special Courts Bill, 1978 ,In re,* (1979) 1 SCC 380.
[52] *Aadhaar case.*

Two recent examples of cases where the Supreme Court has held State action to be arbitrary and disproportionate are *K.S. Puttaswamy* v. *Union of India*.[53] (the '**Aadhaar**' case) and the *Indian Hotel and Restaurant Assn.* v. *State of Maharashtra* (the '**dance performances**' case).[54] In the Aadhaar case, decided by a Constitution Bench, the majority struck down subordinate legislations requiring Indian residents to compulsorily link their mobile numbers and bank accounts with their Aadhaar numbers, finding the linkage requirements to be disproportionate. It found that, in the context of bank account-Aadhaar linkage, though the State claimed that such linkage was in order to tackle money laundering, the State had not explained how such linkage would in fact reduce money laundering. It also found that the State had not discharged its burden of why Aadhaar linking was imperative when banks were already carrying out alternative Know Your Customer (KYC) methods. It held that the presumption of criminality is treated as disproportionate, and that "*[u]nder the garb of prevention of money laundering or black money, there cannot be such a sweeping provision which targets every resident of the country as a suspicious person*." It found that the State should have carried out a proper study about the methods adopted by persons who indulge in money laundering and the kinds of bank accounts which such persons maintain, and targeted those bank accounts for the purpose of Aadhaar linking. Similarly, it held that the circular requiring persons to link their mobile numbers with Aadhaar was "*disproportionate and unreasonable State compulsion*". It held that there could be less intrusive alternatives to this mandatory linkage, and that "*for the misuse of such SIM cards by a handful of persons, the entire population cannot be subjected to intrusion into their private lives*."

In the dance performances case, the Court struck down various provisions of a Maharashtra Act restricting dance performances in certain kinds of commercial establishments. An example of a provision it found arbitrary and disproportionate was a provision proscribing the serving of alcohol in rooms where dance was performed. It found that the State was influenced by moralistic overtones, and that even if there are isolated incidents of misbehaviour with dancers, alternative measures – and not a complete prohibition – would have to be adopted.

However, the *locus classicus* on the reasonableness of a restriction on fundamental rights is (arguably) the early case of *Chintaman Rao* v. *State of M.P.,* decided by a Constitution Bench of the Supreme Court in 1950.[55]

---

[53] *Aadhaar case.*
[54] *Indian Hotel and Restaurant Assn. v State of Maharashtra,* (2019) 3 SCC 429.
[55] *Chintaman Rao v State of M.P.,* AIR 1951 SC 118 : 1950 SCR 759.

In *Chintaman Rao*, the Court struck down a restriction on the manufacture of *bidis* during the agricultural season, holding that alternative, less invasive measures were available (such as a regulation of the hours of work) and that the impugned measure went much in excess of its object (adequate supply of agricultural labour in *bidi* manufacturing areas). It also found that the effect of the measure was that a manufacturer of *bidis* could not employ persons even from places not covered by the notification. It held that such a prohibition was of an arbitrary nature as it had no relation to the object of the legislation.

The right to property under Article 300A too, though not a fundamental right, cannot be restricted in a disproportionate or excessive manner. This has been held by a Constitution Bench in the *K.T. Plantation* case.[56] The Court held that before depriving persons of their right under Article 300A, there has to be a 'public purpose' and the right to claim compensation. The Court held further that the measure (including the compensation) must always be "*just, fair and reasonable*" as understood in terms of Articles 14, 19(1)(g), and other Articles.

This article analyzes whether these criteria of reasonableness and proportionality are met by the Committee's recommendation of an outright ban on crypto-asset activity.

V. Analyzing Each Reason in the Committee Report

The Committee Report was completed in February 2019 and released publicly in July 2019.[57] The Committee consisted of the following members:

a) Secretary, Department of Economic Affairs, Ministry of Finance, who was the Chairman;

b) Secretary, Ministry of Electronics and Information Technology (MeitY);

c) Chairman, Securities and Exchange Board of India (SEBI); and

---

[56] *K.T. Plantation case.*

[57] Department of Economic Affairs, *Report of the Committee to Propose Specific Actions to be Taken in Relation to Virtual Currencies* (Ministry of Finance-Government of India, 28 February 2019) <https://dea.gov.in/sites/default/files/Approved%20and%20Signed%20Report%20and%20Bill%20of%20IMC%20on%20VCs%2028%20Feb%202019.pdf> accessed 4 June 2020; Press Information Bureau, Government of India, Inter-Ministerial Committee on Virtual Currencies submits its Report along with Draft Bill 'Banning of Cryptocurrency & Regulation of Official Digital Currency Bill, 2019' (Press Release, 22 July 2019) <https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579759> accessed 4 June 2020.

d) Deputy Governor, RBI.

The minutes of the Committee's meetings suggest that it also closely consulted the Chairman of the Central Board of Direct Taxes.[58]

The Committee Report recommends the introduction of a Draft Banning of Cryptocurrency and Regulation of Official Digital Currency Bill, 2019 (the '**Draft Bill**') which provides for an outright ban on the use of 'cryptocurrency' (as defined in the Draft Bill) for any purpose, including buying, selling, and storing. The Draft Bill in fact criminalizes activities relating to 'cryptocurrency' with a fine or imprisonment of up to ten years.

In light of the constitutional principles discussed above, this is on its face an extreme step since it criminalizes all uses of a value-neutral technology. As stated above, crypto-assets are a platform technology which can be used for beneficial or harmful purposes, like the Internet. The Draft Bill would prevent all useful applications of the technology which, as described above, include applications which can bring significant cost-savings in cross-border inward migrant remittances, and innovations in decentralized software applications by India's software community. Importantly, it would, in one fell swoop, bring 50 lakh persons in India under the threat of criminal prosecution, facing a potential ten-year jail term, forcing them to dispose of a legitimate and valuable asset. Because of these severe repercussions, the Draft Bill needs close scrutiny on whether it is a reasonable restriction on the fundamental freedoms discussed above with respect to crypto-assets.

Below, each reason given by the Committee Report in support of the Draft Bill is set out along with responses setting out why – it is submitted – the reason is specious and/or can be effectively addressed with a less invasive measure.

Committee Report's Reason: Crypto-assets do not have any of the benefits of fiat currency and cannot replace fiat currency.[59]

Response: The mere fact that the technology has a value-transfer or value-storage role does not mean that it has to be fiat currency or legal tender. There are many systems of value transfer or stores of value which work in tandem with fiat currency, including gold and loyalty points systems. In fact, the largest multi-brand loyalty points system in India consists of over 100

[58] Committee Report (n 57) 84-85.
[59] Committee Report (n 57) 27.

million customers and over 100 leading, mainstream commercial enterprises.[60] Customers earn 'points' by making purchases and the points can in turn be redeemed for value at a large network of merchants.[61] These points are not legal tender or fiat currency in India and are purely contractual. Similarly, gold, which is used as a store of value and investment asset by many persons (including the RBI) is not legal tender or fiat currency in India.

Therefore, the use of crypto-assets cannot be prohibited merely because it is not fiat currency or does not have its characteristics. Rather, an empirical economic assessment of the financial stability or monetary policy implications of the use of crypto-assets should be carried out, and its usage regulated accordingly. No such empirical assessment appears to have been carried out by the Committee or any other authority in India.

Committee Report's Reason: Crypto-assets have no inherent value beyond the utility their underlying technologies represent.[62]

Response: In economic theory, value is widely acknowledged to be determined by individuals' subjective preferences, which dictate demand and supply for a particular item.[63] This is clearly borne out by the high values often paid for antiques, artwork, and other collectors' items, which go far beyond the cost of labour and materials associated with such items. For instance, a gold coin – one of the last gold coins to be minted in the United States – was sold for 7.6 million USD in 2002.[64] The most valuable work of art ever sold at an auction was Pablo Picasso's 1955 painting, Les femmes d'Alger, which was sold for 179.3 million USD in 2015.[65] It is difficult to say that the Committee Report would have ascribed such a high 'inherent value' to these items. Yet, it could be nobody's case that transactions in collectors' items should be banned. It would be difficult to justify a restriction on a constitutional freedom merely because the State is of the view that the activity lacks

---

[60] *See Payback* <https://payback.in.> accessed 4 June 2020; also InterMiles <intermiles.com> accessed 4 June 2020.

[61] ibid.

[62] Committee Report (n 57) 27.

[63] Edward P. Stringham, 'Economic Value and Costs are Subjective' in Peter J. Boettke (ed), *Handbook on Contemporary Austrian Economics* (Edward Elgar Publishing 2010) ch 4 <https://ssrn.com/abstract=1676261> accessed 4 June 2020 states, '*With a few exceptions, almost all modern economists believe that goods are valued based on how they satisfy individuals' subjective preferences*.'

[64] 'The Most Expensive Items Ever Auctioned: Double Eagle Coin' (*CNN Business*, 2 March 2016) <https://money.cnn.com/gallery/luxury/2016/03/02/most-expensive-auction-items/7.html> accessed 4 June 2020.

[65] 'The Most Expensive Items Ever Auctioned: Pablo Picasso's Les Femmes d'Alger' (*CNN Business*, 2 March 2016) <https://money.cnn.com/gallery/luxury/2016/03/02/most-expensive-auction-items/index.html> accessed 4 June 2020.

value. As Chandrachud, J. observed in the Right to Privacy case, "*[t]he duty of the state is to safeguard the ability to take decisions – the autonomy of the individual – and not to dictate those decisions.*"

In any case, crypto-assets are founded on the scientific breakthrough made in Satoshi Nakamoto's 2008 paper,[66] a breakthrough that has been acknowledged by computer scientists worldwide[67] as well as by the RBI and other Indian government authorities in various reports. In short, crypto-assets enable the transfer of value over the Internet without central intermediaries, something that was not achieved prior to 2008 despite various attempts. In fact, even the Committee Report states that crypto-assets do not have inherent value "*beyond the utility their underlying technologies represent*", thereby in fact recognizing that there is value in crypto-assets due to the utility of the technology.

Further, the market forces ascribing value to crypto-assets make it clear that such value is not a result of the irrational exuberance of a few participants. The total market capitalization of crypto-assets listed on coinmarketcap.com (considered one of the leading market data websites in the crypto-asset industry) as of May 2020 was approximately 261 billion USD.[68] In addition, crypto-assets have received investment and recognition from reputed institutions and individuals including Massachusetts Institute of Technology, Harvard University, JP Morgan, Fidelity, Samsung, Visa, Mastercard, Microsoft, Ratan Tata, Khosla Ventures, and many others.[69]

---

[66] Nakamoto (n 2).

[67] For example, Arvind Narayanan and Jeremy Clark (n 4) 15 states, '*Understanding all these predecessors that contain pieces of bitcoin's design leads to an appreciation of the true genius of Nakamoto's innovation*'; Yossi Gilad (n 5) states, '*Cryptographic currencies such as Bitcoin can enable new applications, such as smart contracts and fair protocols, can simplify currency conversions, and can avoid trusted centralized authorities that regulate transactions.*'

[68] Based on data from coinmarketcap.com as of May 2020.

[69] *MIT Digital Currency Initiative* <https://dci.mit.edu/> accessed 4 June 2020; Luke W. Vrotsos and Cindy H. Zhang, 'Harvard Invests Millions in New Cryptocurrency' (*The Harvard Crimson*, 12 April 2019) <https://www.thecrimson.com/article/2019/4/12/hmc-crypto-investment/> accessed 4 June 2020; 'J.P. Morgan creates Digital Coin for Payments' (*J.P. Morgan*, 14 February 2019) <https://www.jpmorgan.com/global/news/digital-coin-payments> accessed 4 June 2020; Colin Harper, 'J.P. Morgan Opens Accounts for Bitcoin Exchanges- Coinbase and Gemini Up First' (*Forbes*, 12 May 2020) <https://www.forbes.com/sites/colinharper/2020/05/12/jp-morgan-opens-accounts-for-bitcoin-exchanges--coinbase-and-gemini-up-first/> accessed 4 June 2020; *Fidelity Digital Assets* <www.fidelitydigitalassets.com> accessed 4 June 2020; Billy Bambrough, 'Samsung is Quietly Becoming A Major Bitcoin, Crypto and Blockchain Player' (*Forbes*, 18 February 2020) <https://www.forbes.com/sites/billybambrough/2020/02/18/samsung-is-quietly-becoming-a-major-bitcoin-crypto-and-blockchain-player/> accessed 4 June 2020; Michael del Castillo, 'Visa Grants Coinbase Power to Issue Bitcoin Debit Cards' (*Forbes*, 19 February 2020) <https://www.forbes.com/sites/michaeldelcastillo/2020/02/19/

This indicates a degree of sophistication in the crypto-asset market which cannot be written off with a cursory remark.

Committee Report's Reason: Crypto-assets are volatile and the subject of speculation and price manipulation.[70]

Response: Recent events in the stock and commodities markets have shown that volatility is a characteristic not unique to crypto-assets. For instance, in October 2019, the shares of a large telecom company fell by 35% in two days and by over 80% since the start of the year.[71] The crises affecting banks and non-banking financial institutions also took their toll. In February 2018, in just two days, approximately 5 lakh crore Indian Rupees of value was erased from stocks listed on the Bombay Stock Exchange (BSE).[72] In September 2018, the market capitalization of BSE-listed stocks fell by 8.47 lakh crore Indian Rupees in five days.[73] The price of certain stocks fell by up to 60% within a single day.[74]

---

visa-grants-coinbase-power-to-issue-bitcoin-debit-cards/#34061f3b2e83> accessed 4 June 2020; Kevin Helms, 'Visa Files Patent for Cryptocurrency System to Replace Cash' (*Bitcoin.com*, 15 May 2020) <https://news.bitcoin.com/visa-cryptocurrency-system/> accessed 4 June 2020; Avi, 'Mastercard Patents a Method to Manage Cryptocurrency "Fractional Reserves"' (*Bitcoin.com*, 18 July 2018) <https://news.bitcoin.com/mastercard-patents-a-method-to-manage-cryptocurrency-fractional-reserves/> accessed 4 June 2020; 'Ethereum Cryptocurrency and Blockchain Full Guide' (*Microsoft*) <https://www.microsoft.com/en-us/p/ethereum-cryptocurrency-and-blockchain-full-guide/9n-0mjg5x40n8> accessed 4 June 2020; 'Ratan Tata, American Express invest in digital currency startup Abra' (*The Economic Times*, 24 October 2015) <https://economictimes.indiatimes.com/small-biz/startups/ratan-tata-american-express-invest-in-digital-currency-startup-abra/articleshow/49496937.cms> accessed 4 June 2020; Jeff Kauflin, 'Startup Raises $23 Million to Make Crypto Trades Faster and Stealthier' (*Forbes*, 16 August 2018) <https://www.forbes.com/sites/jeffkauflin/2018/08/16/startup-raises-23-million-to-make-crypto-trades-faster-and-stealthier/> accessed 4 June 2020.

70 Committee Report (n 57) 29.

71 'Vodafone Idea Share hits Fresh All-time Low on SC Verdict, Nosedives 35% in Two Days', (*Business Today*, 25 October 2019) <https://www.businesstoday.in/markets/company-stock/vodafone-idea-share-hits-fresh-all-time-low-on-sc-verdict-nosedives-35-in-two-days/story/386718.html> accessed 4 June 2020.

72 Sriram Iyer, 'Indian Markets Have Just Lost Over $75 Billion—But it's Not all Jaitley's Fault' (*Quartz India*, 6 February 2018) <https://qz.com/india/1199373/bse-blowout-indian-markets-have-lost-over-75-billion-but-its-not-all-arun-jaitleys-fault/> accessed 4 June 2020.

73 'Investors Poorer by Rs 8.5 lakh Crore as Market Turmoil Continues for Fifth Day' (Times of India, 24 September 2018) <https://timesofindia.indiatimes.com/business/india-business/investors-poorer-by-rs-8-5-lakh-crore-as-market-turmoil-continues-for-fifth-day/articleshow/65935108.cms> accessed 4 June 2020.

74 'On Edge: On the Volatility in Indian Markets' (*The Hindu*, 24 September 2018) <https://www.thehindu.com/opinion/editorial/on-edge/article25022243.ece> accessed 4 June 2020.

In October 2019, shares of certain mid-sized banks fell by over 21% in intraday trade, and the shares of one of these banks – Yes Bank – shot back up by 33% two days later.[75] At its low in October 2019, shares of this bank – which was once the country's sixth largest private sector lender – had fallen so as to erode 92% of investors' wealth from its record high just 14 months earlier.[76] Later, in the same month, the price rose by 39% in intraday trading and by 60% in one month.[77]

In March 2020, the COVID-19 pandemic resulted in 52 lakh crore Indian rupees of investor losses on the Indian equity market, erasing nearly six years of gains in one fell swoop.[78]

To compare, the annualized volatility of Bitcoin was 166.45% as of March 27, 2020,[79] while the annualized volatility of Yes Bank and Zee Entertainment Enterprises Limited derivatives as of March 28, 2020 was 428.5% and 170.65% respectively.[80]

Yet it cannot be the Committee Report's case that securities trading ought to be prohibited because of high volatility.

This is not to say that volatility and price manipulation in the crypto-asset market ought to be ignored; instead, it should be dealt with by regulation.

---

[75] Shubham Raj, 'After Market: Tuesday Turmoil Costs Equity Investors Rs 1.85 Lakh Crore; YES Bank, RBL Bleed' (*ET Markets*, 1 October 2019) <https://m.economictimes.com/markets/stocks/news/after-market-tuesday-turmoil-costs-equity-investors-rs-1-85-lakh-crore-yes-bank-rbl-bleed/articleshow/71394559.cms> accessed 4 June 2020.

[76] Ami Shah and others, 'Death by a Thousand Cuts! How Rana Kapoor's 'Diamond' YES Bank Turned into a Smallcap' (*ET Markets*: 2 October 2019) <https://economictimes.indiatimes.com/markets/stocks/news/death-by-a-thousand-cuts-how-rana-kapoors-diamond-yes-bank-turned-into-a-smallcap/articleshow/71396716.cms?from=mdr> accessed 4 June 2020.

[77] 'Yes Bank Shares Rally 39% on Binding Offer of $1.2 bn From Global Investor' (*Moneycontrol News*, 31 October 2019) <https://www.moneycontrol.com/news/business/markets/yes-bank-shares-rally-25-on-binding-offer-of-1-2-bn-from-global-investor-4589871.html> accessed 4 June 2020.

[78] Amit Mudgill, 'Corona Carnage Threatens to Wipe Off Market's Entire Modi-era Gain (*ET Markets*, 23 March 2020) <https://economictimes.indiatimes.com/markets/stocks/news/corona-carnage-threatens-to-wipe-off-markets-entire-modi-era-gain/articleshow/74771891.cms> accessed 4 June 2020.

[79] 'BVOL: Annualized Historical Volatility Index' (*BitMEX*) <https://www.bitmex.com/app/index/.BVOL> accessed 4 June 2020.

[80] 'Quote Yes Bank Limited–YESBANK' (NSE as on April 30, 2020 15:30:31 IST) <https://www1.nseindia.com/live_market/dynaContent/live_watch/get_quote/GetQuoteFO.jsp?underlying=YESBANK&instrument=FUTSTK&type=-&strike=-&expiry=30APR2020> accessed 4 June 2020; 'Quote Zee Entertainment Enterprises Limited–ZEEL' (NSE as on April 30, 2020 15:30:31 IST) <https://www1.nseindia.com/live_market/dynaContent/live_watch/get_quote/GetQuoteFO.jsp?underlying=ZEEL&instrument=-FUTSTK&type=-&strike=-&expiry=30APR2020> accessed 4 June 2020.

This is why securities regulators around the world, including the SEBI, regulate the securities market to a granular level of detail. In fact, the securities market in India in its early stages suffered from the same concerns stated in the Committee Report. Interestingly, a 1948 Government of India report titled 'Report on the Regulation of the Stock Market in India' by P. J. Thomas, independent India's first economic advisor, found as follows:

> The enquiry soon disclosed a serious state of things in the stock market, one which clearly demands Government intervention in the public interest. …
>
> Not only the organisation of the stock market was found defective: its functioning has also often been detrimental to the interests of investors and of the national economy as a whole. Safety for dealings is largely non-existent and proper provision does not exist for equity between parties. Perhaps the most objectionable feature is the violently fluctuating character of prices in the stock market. This has also worked to the detriment of the investing public. Occasionally the market is pushed up by reckless bull operators to unwarranted heights, and the crash that necessarily follows leads to wide-spread liquidation and loss: even such a pitiable situation, let it be noted, is utilised by powerful bear syndicates to hammer prices down and to extort as much money as possible from investors by causing panicky selling in the market. This has been going on for long in the Indian stock market…[81]

This report ultimately recommended regulation (and not prohibition) of the stock market to counter these negative aspects.

Similarly, any volatility and price manipulation in crypto-asset markets ought to be dealt with by regulation and not an outright prohibition. Besides market regulatory measures to prevent sharp price swings and price manipulation, regulators may also consider imposing statutory warnings (akin to those issued for securities market investments) with respect to the crypto-asset market.

Committee Report's Reason: Crypto-assets carry risks for the wider financial system, compromising the ability of central banks to monitor and stabilise the economy.[82]

---

[81] P.J. Thomas, *Report on the Regulation of the Stock Market in India* (Glasgow Printing Co, Howrah for the Ministry of Finance-Government of India 1948) (i) <https://www.sebi.gov.in/sebi_data/commondocs/may-2019/HistoryReport1948_p.pdf> accessed 4 June 2020.

[82] Committee Report (n 57) 30.

Response: The Committee Report does not discuss any empirical evidence to support this reason. Its only analysis in support of this reason is as follows:

> Central banks cannot regulate the money supply in the economy if non-official virtual currencies are widely used, as these are decentralised. This restricts their ability to stabilise the economy. In addition, cross-border transactions with non-official virtual currencies can violate limits on the inflow and outflow of money, particularly as such transactions happen irreversibly. This compromises another important lever of monetary policy.

The second point is easily dealt with, since the solution is to regulate cross-border crypto-asset transactions under the Foreign Exchange Management Act, 1999 ('**FEMA**'). FEMA regulates all transfers of value into and outside India, whether of money or goods and services (including 'software').[83] Crypto-assets, which are intangible information, can be subject to the same regime as 'software' under FEMA, and their export and import regulated accordingly.

Regarding the first point on the regulation of money supply and financial stability, a parallel can again be drawn between crypto-assets on the one hand and gold and loyalty points systems on the other. The latter are not legal tender but are widely used in the mainstream economy for the storage and transfer of value and, yet, are not banned. Some aspects relating to gold are specifically regulated by various Indian laws,[84] and holding and trading it is a lawful activity. Similarly, to this author's knowledge, loyalty points systems– despite wide mainstream use among a number of popular merchants[85]– are not specifically regulated[86] and would only be subject to generally applicable laws like the contract law and consumer protection law. Being similar in many aspects to gold (which is also decentralized and an

---

[83] Eg, Foreign Exchange Management Act 1999 (FEMA), ss 2 (l), 2 (p), and 7, which present the definitions of 'export', 'import', and provision on export of 'goods', read with reg 2 (vii), Foreign Exchange Management (Export of Goods & Services) Regulations 2015 which gives the definition of 'software' and treatment in line with 'goods'; FEMA, s 5, read with RBI Master Direction – Import of Goods and Services (RBI/FED/2016-17/12, FED Master Direction No. 17/2016-17, as amended), which provides for a regime on import of 'goods'.

[84] Eg, RBI Master Direction – Import of Goods and Services (RBI/FED/2016-17/12, FED Master Direction No. 17/2016-17, as amended).

[85] The Most Expensive Items Ever Auctioned: Double Eagle Coin (n 64).

[86] Reserve Bank of India, *Certificates of Authorisation issued by the Reserve Bank of India under the Payment and Settlement Systems Act, 2007 for Setting up and Operating Payment System in India* (2009) <https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/ATH190315ENTPSP.PDF> accessed 4 June 2020, where no authorization(s) appears to have been issued for loyalty points systems.

important store of value), crypto-assets can be regulated similarly by the RBI as far as monetary policy and financial stability goes.

Importantly, there has been no empirical finding by the Committee Report or the RBI (the regulator of monetary policy and financial stability) showing a current or threatened risk posed by crypto-assets to monetary policy or financial stability. In fact, the RBI publishes detailed biannual financial stability and monetary policy reports,[87] where it empirically analyses the impact of various global and domestic factors on the Indian economy. These factors include stressed sectors of the economy, asset quality and other aspects of the health of financial institutions, consumer behaviour, geopolitical risks, global economic conditions, commodity prices (including gold and oil prices), and U.S. dollar liquidity, among others. On the contrary, there is no such economic analysis on crypto-assets in the RBI's financial stability reports or monetary policy reports barring a high-level summary on 'virtual currency' in 2013.[88] That summary included all types of virtual currencies including in-game virtual currencies, and only concluded that "*[t]he regulators are studying the impact of online payment options and virtual currencies to determine potential risks associated with them.*"[89] There has since been no empirical, economic finding on any such potential risks.

In fact, the RBI found in a 2017 working group report that "*their [crypto-assets'] influence on financial services and the wider economy is negligible today, and it is possible that in the long term they may remain a product for a limited user base on the fringes of mainstream financial services*"[90] and in its 2018 annual report that "*cryptocurrency may not currently pose systemic risks*".[91]

---

87 Reserve Bank of India, *Half Yearly Financial Stability Report* <https://www.rbi.org.in/Scripts/FsReports.aspx>; <https://www.rbi.org.in/Scripts/HalfYearlyPublications.aspx?head=Monetary%20Policy%20Report> accessed 4 June 2020.

88 Reserve Bank of India, 'Financial Sector Regulation and Infrastructure' in *Financial Stability Report June 2013* (June 2013) ch III, 62 <https://www.rbi.org.in/scripts/PublicationReportDetails.aspx?ID=709> accessed 4 June 2020.

89 ibid.

90 Reserve Bank of India (Central Office-Mumbai), *Report of the Working Group on FinTech and Digital Banking* (November 2017) 9 <https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WGFR68AA1890D7334D8F8F72CC2399A27F4A.PDF> accessed 4 June 2020 (Digital Banking report).

91 Reserve Bank of India, 'Economic Review' in *Annual Report 2017-18* (August 2018) ch II, 48 <https://www.rbi.org.in/scripts/AnnualReportPublications.aspx?Id=1229> accessed 4 June 2020.

At a global level, India is a member of both the G20 and the Financial Stability Board – a global, multilateral expert body – which have found that crypto-assets do not pose a threat to global financial stability.[92]

In case an argument is advanced that a ban on crypto-assets is a pre-emptive measure by way of abundant caution to prevent any potential risk to the financial system, any such pre-emptive measure ought to be – based on the constitutional principles discussed above – a proportionate and reasoned decision based on a consideration of the material facts. To find examples of a proportionate and empirical approach to preventive measures to address financial stability and monetary policy risks, one need not look further than the RBI. In its financial stability reports, it provides detailed empirical economic analysis on the performance and risks of financial institutions and carries out stress tests for factors such as credit risk (including sectoral credit risk), interest rate risk, equity price risk, and others.[93] For preventive measures, it has implemented a Prompt Corrective Action ('**PCA**') framework which it has described as follows:

> The global financial crisis demonstrated the shortcomings of the framework for effective financial crisis management and in many cases the absence of effective resolution mechanism to handle systemic financial institutions. A resolution mechanism is put in place when a financial institution has weakened substantially, but a framework of preventive as well as early intervention measures could potentially arrest the deterioration in financial institutions in the first place. Putting in place a prompt corrective action (PCA) framework that incorporates graded triggers at prespecified levels for taking early actions by the regulators is important for the financial sectors. …
>
> The Reserve Bank of India initiated a Scheme of Prompt Corrective Action (PCA) in 2002 in respect of banks which hit certain regulatory trigger points in terms of capital to risk weighted assets ratio (CRAR), net non-performing assets (NNPA), and return on assets (RoA). … Under the Revised PCA framework, apart from the capital, asset quality and profitability, leverage is being monitored additionally. Under PCA, banks face restrictions on distributing dividends, remitting

[92] Ministry of Finance, Japan, *Communiqué: G20 Finance Ministers and Central Bank Governors Meeting* (Fukuoka-Japan, 9 June 2019) <http://www.g20.utoronto.ca/2019/2019-g20-finance-fukuoka.html> accessed 4 June 2020. Financial Stability Board, *Crypto-assets: Report to the G20 on Work by the FSB and Standard-setting Bodies* (16 July 2018) 1 and 6 <https://www.fsb.org/2018/07/crypto-assets-report-to-the-g20-on-the-work-of-the-fsb-and-standard-setting-bodies/> accessed 4 June 2020.

[93] Reserve Bank of India (n 87).

> profits and even on accepting certain kinds of deposits.[94] (emphasis added)

As shown above, PCA is a financial stability measure imposed by the RBI on particular banks based on a detailed empirical assessment of their asset quality and other factors. Therefore, even assuming crypto-assets were a potential threat to financial stability (though the findings are to the opposite effect as discussed above), a proportionate approach by the Committee to any perceived financial stability or monetary policy concern would have been to carry out – with the help of the RBI and/or independent economic experts –an empirical economic analysis of the issue and propose a balanced response rather than an outright prohibition. An example of such a balanced response could have been for the Committee Report to recommend that the RBI (the relevant regulator) monitor whether particular banks hit the regulatory trigger points with regard to any exposure to crypto-asset activity and impose a suitably tailored form of PCA accordingly. In a similar vein, in its June 2017 Financial Stability Report, the RBI found that the telecom and power sectors were stressed sectors of the economy and, therefore, as a preemptive measure, advised banks to make provisions at higher rates in respect of advances to stressed sectors of the economy, specifically mentioning the telecom sector.[95] There was no outright prohibition on any activities of these stressed sectors.

On the contrary, the Supreme Court in the *IAMAI* case noted that the RBI did not show any semblance of damage to its regulated entities as a result of their relationship with crypto-asset exchanges.[96]

Committee Report's Reason: Crypto-asset transactions are time-consuming and "*[t]he large gap in transaction processing speed between cryptocurrencies (especially Bitcoin), and other electronic payment methods, hinders their ability to be used as medium of exchange [sic].*"[97]

Response: There are over 2000 crypto-assets in existence, some of which can process thousands of transactions per second, and some of which are

---

[94] Reserve Bank of India, *Financial Stability Report Issue 17* (RBI-Financial Stability Unit, June 2018) 29 <https://rbidocs.rbi.org.in/rdocs//PublicationReport/Pdfs/0FSR_JUNE2018A3526EF7DC8640539C1420D256A470FC.PDF> accessed 4 June 2020.

[95] Reserve Bank of India, *Financial Stability Report Issue 15* (RBI-Financial Stability Unit, June 2017) <https://rbidocs.rbi.org.in/rdocs//PublicationReport/Pdfs/0FSR_30061794092D8D036447928A4B45880863B33E.PDF> accessed 4 June 2020.

[96] *IAMAI case* paras 6.172 and 6.173.

[97] Committee Report (n 57) 27.

much slower.[98] However, no crypto-asset network, to the author's knowledge, takes more than a day to process a transaction. On the contrary, and by comparison, cheques – a widely accepted and regulated form of payment – typically take at least a day or two to be processed.[99] Ultimately, as stated above, the State is not an authority to dictate the decisions of its citizens and other rights-holders. It is up to rights-holders to decide how they wish to transfer and store value, subject to reasonable restrictions. While some technologies have succeeded, others have failed, and the decisions of the general public determine which technology will succeed. Meanwhile, if the State believes, with rational basis, that intervention is necessary, the constitutional principles above tell us that the answer lies in introducing proportionate consumer protection norms rather than an outright prohibition.

Committee Report's Reason: "*[Cryptocurrencies] provide a degree of pseudonymity, although not complete anonymity, to participants in a transaction. … In some cases, virtual currencies have made criminal activity harder to stop, given the pseudonymity they provide and their cross-border nature*."[100]

Response: Where criminal activity is suspected, law enforcement authorities have been able to use technology to trace the persons behind Bitcoin transactions by analyzing the blockchain and de-anonymizing Bitcoin transactions.[101] The pseudonymous proprietor of the infamous Silk Road network too was uncovered and prosecuted (interestingly, through a low-tech method involving Google searches).[102] Law enforcement authorities in India have also successfully obtained information from Indian crypto-asset exchanges in order to trace criminal suspects and enforce tax obligations.[103] There

---

[98] Zane Witherspoon, 'A Hitchhiker's Guide to Consensus Algorithms: A Quick Classification of Cryptocurrency Consensus Types' (*Hackernoon*, 29 November 2017) <https://hackernoon.com/a-hitchhikers-guide-to-consensus-algorithms-d81aae3eb0e3> accessed 4 June 2020.

[99] Eg, State Bank of India, *Cheque Collection Policy – 2015* <https://www.sbi.co.in/portal/web/customer-care/cheque-collection-policy> accessed 4 June 2020.

[100] Committee Report (n 57) 27.

[101] Kelly Phillips Erb, 'IRS Followed Bitcoin Transactions, Resulting in Takedown of the Largest Child Exploitation Site on the Web' (*Forbes*, 16 October 2019) <https://www.forbes.com/sites/kellyphillipserb/2019/10/16/irs-followed-bitcoin-transactions-resulting-in-takedown-of-the-largest-child-exploitation-site-on-the-web/#2c55a0971ed0> accessed 4 June 2020. This fact has also been recognized by the Committee Report, which states, '*since the underlying Blockchain broadcasts a new transaction whenever it is verified under the consensus systems, some extent of linkability is possible*.'

[102] Nathaniel Popper, 'The Tax Sleuth Who Took Down a Drug Lord' (*The New York Times*, 25 December 2015) <https://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html> accessed 4 June 2020.

[103] Archana More, 'Hackers Siphon Off Funds from BoM to Invest in Bitcoin' (*Pune Mirror*, 25 April 2017) <https://punemirror.indiatimes.com/pune/cover-story/

are some crypto-assets, known as 'privacy coins' (ZCash and Monero are common examples), where transactions may be difficult to trace if not carried out on an exchange which verifies the identity of its participants.

To the extent that crypto-asset transactions are pseudonymously, universally, and irreversibly recorded on the blockchain, or are carried out on an exchange which verifies identity, crypto-asset transactions are more traceable than transactions in physical cash or goods which are not recorded on any such distributed ledger. To the extent that crypto-asset participants may obfuscate their identity, whether by using privacy coins or otherwise, transactions resemble physical cash or goods transactions, where forensic analysis may or may not lead to traceability. Therefore, crypto-asset transactions are either more traceable or at par with physical cash and goods transactions, depending on the context.

Just as existing laws, including the Information Technology Act, the Indian Penal Code, 1860 ('**IPC**'), Prevention of Money Laundering Act, 2002 ('**PMLA**'), the Income Tax Act, 1961, the Prize Chits and Money Circulation Schemes (Banning) Act, 1978, FEMA, and other laws are effectively used to enforce criminal law, tax, and regulatory obligations on participants in other kinds of transactions, the same laws are already being used to investigate and prosecute fraudulent activity in crypto-asset transactions. For instance, proponents of the allegedly fraudulent GainBitcoin scheme (cited in the Committee Report as an instance of criminal activity involving crypto-assets) were arrested and prosecuted on the basis of some of these laws.[104] The Central Government has stated in Parliament,

> Presently, there is no separate law for dealing with issues relating to cryptocurrencies. Hence, all concerned Departments and law enforcement agencies, such as RBI, Enforcement Directorate and Income Tax

---

hackers-siphon-off-funds-from-bom-to-invest-in-bitcoin/articleshow/58350202.cms> accessed 4 June 2020; Vishwas Kothari, 'Pune Cops Move Sessions Court Seeking Rs 8.42 Crore' *The Times of India* (Pune, 3 October 2019) <https://timesofindia.indiatimes.com/city/pune/cops-move-sessions-court-seeking-rs-8-42-crore/articleshow/71414172.cms> accessed 4 June 2020; 'Bitcoin Crackdown: Income Tax Department to Send Notices to 4-5 Lakh HNIs for Suspected Tax Evasion' (*Business Today*, 19 December 2017) <https://www.businesstoday.in/current/economy-politics/bitcoin-cryptocurrency-income-tax-notices-hnis-bitcoin-trading/story/266269.html> accessed 4 June 2020.

[104] Archana More, 'Court Denies Bail to Six Key Accused' (*Pune Mirror*, 15 August 2018) <https://punemirror.indiatimes.com/pune/crime/court-denies-bail-to-six-key-accused/articleshow/65406906.cms> accessed 4 June 2020; Outlook Web Bureau, 'Raj Kundra Grilled by Enforcement Directorate in Bitcoin Money Laundering Case' (*Outlook India*, 5 June 2018) <https://www.outlookindia.com/website/story/raj-kundra-grilled-by-enforcement-directorate-in-bitcoin-money-laundering-case/312317> accessed 4 June 2020.

> authorities, etc. take action as per the relevant existing laws. Similarly, police/courts take action on IPC offences.

India has seen a plethora of high-stakes frauds in the securities market, commodities market, and financial sector over the past few decades;[105] yet these markets continue to be permitted within the bounds of regulation, with criminal activity prosecuted under the above laws. There is no reason why the crypto-asset market should be singled out as a case to be prohibited and not regulated.

In a paper by Nishith Desai Associates, titled 'Building a Successful Blockchain Ecosystem for India: Regulatory Approaches to Crypto-Assets' (the '**Regulatory Suggestions Paper**'), co-authored by this author, we have proposed a detailed set of regulatory options, including bringing crypto-asset activity within the PMLA and licensing crypto-asset intermediaries like exchanges, to further address the concerns regarding the use of crypto-assets for illegal activity.[106]

Therefore, a mere possibility of use in criminal activity is not a ground for an outright prohibition, but calls for regulation.

---

[105] 'PACL Head Bhangoo Arrested Over Alleged Rs 45,000-Crore Investment Scam' *NDTV Profit* (New Delhi, 9 January 2016) <https://www.ndtv.com/business/head-of-pacl-arrested-over-alleged-rs-45-000-crore-investment-scam-1263707> accessed 4 June 2020; Samanwaya Rautray, 'Sahara Group Says it Cannot Pay Rs 36,000 Crore in 18 Months Time' (*ET Bureau*, 8 July 2015) <https://economictimes.indiatimes.com/news/politics-and-nation/sahara-group-says-it-cannot-pay-rs-36000-crore-in-18-months-time/articleshow/47981154.cms?from=mdr> accessed 4 June 2020; 'Karnataka Ponzi Scam: IMA Jewels Chief Mansoor Khan Summoned to Appear Before ED on June 24 (*India Today*, 20 June 2019) <https://www.indiatoday.in/india/story/-karnataka-ponzi-scam-mansoor-khan-summoned-to-appear-before-ed-on-june-24-1552834-2019-06-20> accessed 4 June 2020; 'All You Need to Know About the Saradha, Rose Valley Scams: 10 Points' (*NDTV*, 4 February 2019) <https://www.ndtv.com/india-news/all-you-need-to-know-about-the-saradha-rose-valley-scams-10-points-1987848> accessed 4 June 2020; 'Rs 2,276-Crore Speak Asia Scam Mastermind Held' (*Deccan Herald*, 27 November 2013) <https://www.deccanherald.com/content/371301/rs-2276-crore-speak-asia.html> accessed 4 June 2020; Vivek Law, 'Home Trade Scam: Beyond its Star-studded Campaign, the Financial Services Portal had Nothing' (*India Today Magazine*, 20 May 2002) <https://www.indiatoday.in/magazine/economy/story/20020520-home-trade-scam-beyond-its-star-studded-campaign-the-financial-services-portal-had-nothing-795259-2002-05-20> accessed 4 June 2020; Press Trust of India, 'Ketan Parekh Sentenced to 2 Rears RI by CBI Court' (*Financial Express*, 4 March 2014) <https://www.financialexpress.com/archive/stock-broker-ketan-manharlal-parekh-sentenced-to-2-years-ri-by-cbi-court/1230877/> accessed 4 June 2020; Securities and Exchange Board of India, *Action against Harshad Mehta, Videocon, BPL and Sterlite* (Ref No. PR 71/2001, 19 April 2001) <https://www.sebi.gov.in/media/press-releases/apr-2001/action-against-harshad-mehta-videocon-bpl-and-sterlite_17608.html> accessed 4 June 2020.

[106] Nishith Desai (n 17).

Committee Report's Reason: "*[Cryptocurrencies] are decentralised networks with no central authority. … Transactions are irreversible, and if a wrong transaction is made, there is no method of redress.*"[107]

Response: Examples of decentralized phenomena which are not banned include: commodities, including gold and other precious metals; and the Internet. To take the example of gold, there is no central authority which issues gold or regulates its supply. Similarly, there is no central authority regulating messages or content on the Internet. With regard to irreversibility, transactions in physical cash and goods, and the messages on the Internet are also irreversible. A mistakenly sent email or message online cannot be recalled except if the relevant intermediaries allow it. The handing over of physical cash or physical goods cannot be 'reversed' except by consent, contract, or by process of law. With respect to the Internet, consumers have recourse mainly because of the intermediaries they deal with e.g., financial institutions or e-commerce businesses, and not because the Internet has any grievance redressal mechanism of its own. Similarly, consumers are protected with respect to physical cash or goods transactions by merchants and generally applicable laws like criminal laws and consumer protection laws, rather than any feature of the cash or goods themselves.

To this extent, crypto-assets are at par with the above phenomena. The lack of a central authority or the irreversibility of transactions is therefore not a cause for an outright ban. However, intermediaries in the crypto-asset space perform a crucial function because they may hold consumer assets and funds in trust and settle purchase and sale transactions. To that extent, they resemble custodians or securities market intermediaries.[108] Our Regulatory Suggestions Paper proposes that such intermediaries should be licensed and supervised, and suggests the routes under Indian law by which this can be done.[109]

Committee Report's Reason: "*Miners of a currency can collude to earn more revenue by "forking", a currency, or changing the programming protocol to benefit themselves. This could put consumers' finances at risk.*"[110]

Response: The extent of control of miners (who are essentially validators of transactions) over a crypto-asset network varies according to the particular crypto-asset. Many new crypto-assets have tried to avoid the

---

[107] Committee Report (n 57) 27 and 29.
[108] This is not to say that crypto-assets are necessarily 'securities' (see the Regulatory Suggestions Paper, supra).
[109] Nishith Desai (n 17).
[110] Committee Report (n 57) 29.

concentration of power in particular miners, eg, Algorand.[111] In any event, the control of miners or other participants on a crypto-asset network is akin to the control of a Board of Directors or majority shareholders over a company. Participants in a crypto-asset network should do their due diligence on the technology underlying the network, the development team, and other participants in the network, just as shareholders in a company should do their due diligence on the management and fundamentals of a company. This is not to say that the issue of potentially *mala fide* forking in certain crypto-assets should be left unaddressed. Rather, just as shareholders' rights are protected in companies, regulation (rather than an outright prohibition) should be introduced to protect consumers. Because crypto-assets are generally global networks, with participants scattered around the world, such regulation should ideally be introduced by way of a multilateral treaty at the international level. Because a less invasive measure is available and because a similar phenomenon (shareholder rights) is addressed differently, an outright prohibition on this ground would be disproportionate and arbitrary.

Committee Report's Reason: "*The loss of a private key, analogous to a password, of a virtual currency wallet could mean that the amount held in the wallet is lost permanently. … Balances in wallets can be stolen by the use of malware, and there is evidence that such malware is resistant to anti-virus software.*"[112]

Response: This reason is essentially a cybersecurity concern. Interestingly, there were 53,081 cyber-security incidents in India during the year 2017 alone.[113] This was stated by the Minister for electronics and information technology in 2018, who also stated, "*[w]ith the proliferation and vast expansion of Information Technology and related services, there is a rise in instances of cyber crimes including financial frauds, using bank cards and e-wallets in the country like elsewhere in the world.*"[114] Cybersecurity concerns are endemic to all online businesses, including regulated financial intermediaries and other established enterprises. Indian corporations which have been subjected to cyberattacks include Axis Bank, Bank of Maharashtra,

[111] Jing Chen and Silvio Micali, 'ALGORAND' (2016) <https://algorandcom.cdn.prismic.io/algorandcom%2Fece77f38-75b3-44de-bc7f-805f0e53a8d9_theoretical.pdf> accessed 4 June 2020.

[112] Committee Report (n 57) 29.

[113] Government of India-Ministry of Home Affairs, Rajya Sabha, *Unstarred Question 891('Technology to Stop Cyber Crimes')* dated February 9, 2018.

[114] ibid.

Cosmos Bank, Indian Railway Catering and Tourism Corporation (IRCTC), Reliance Jio, Star, and Union Bank.[115]

Cyber-crimes are actionable under the Information Technology Act, 2000.[116] The Information Technology Act also prescribes reasonable security practices and procedures with regard to sensitive personal data or information. Crypto-asset activity is also subject to this regime.[117] If crypto-assets are subject to heightened cybersecurity risk, there is no reason why heightened obligations cannot be prescribed under the Information Technology Act for crypto-asset intermediaries.[118]

As far as the loss of a private key is concerned, many crypto-asset intermediaries provide a 'forgot password' facility if they are in control of the crypto-assets.[119] If they do not, the answer lies in an analogy with the physical world. The loss of valuable things is an issue as old as civilization, and it can only be addressed by the holder exercising due care and caution, and the legal system prosecuting theft.

In addition, there is no evidence provided as to how malware targeting crypto-asset wallets is any more resistant to security / anti-virus software than any other type of malware. It is well-known that in the cybersecurity sphere in general, malware developers and security researchers are involved in an ongoing 'technological arms-race'.[120]

Therefore, cybersecurity is not a reason to prohibit the use of crypto-assets. A proportionate approach would require any cybersecurity concerns to be addressed through regulation and not a prohibition.

---

[115] PTI, 'Cosmos Bank's Server Hacked; Rs 94 Crore Siphoned Off in 2 Days' (*The Economic Times*, 14 August 2018) <https://economictimes.indiatimes.com/industry/banking/finance/banking/cosmos-banks-server-hacked-rs-94-crore-siphoned-off-in-2-days/articleshow/65399477.cms> accessed 4 June 2020; Vinod Mahanta and Sachin Dave, 'How India Inc is Losing its Cybersecurity War' (*The Economic Times*, 14 October 2017) <https://economictimes.indiatimes.com/tech/internet/how-india-inc-is-losing-its-cybersecurity-war/articleshow/61074845.cms> accessed 4 June 2020.

[116] Eg, s 66.

[117] Crypto-asset activity would involve a 'computer' and would hence be covered by s 43 read with s 2(1)(i) of the Information Technology Act 2000.

[118] There is a fairly broad power to make rules under s 87 of the Information Technology Act 2000.

[119] Eg, *Unocoin* <https://www.unocoin.com/in> accessed 4 June 2020; *Coinbase* <https://www.coinbase.com/password_resets/new> accessed 4 June 2020.

[120] Eg, Alex Ayers, 'Security Think Tank: Addressing the Malware Arms Race' (*Computer Weekly*, 2 September 2016) <https://www.computerweekly.com/opinion/Security-Think-Tank-Addressing-the-malware-arms-race> accessed 4 June 2020.

Committee Report's Reason: "*The mining of non-official virtual currencies is very resource intensive. … Already, Bitcoin mining has used as much electricity as all of Switzerland, with the [Bank for International Settlements'] report terming it an environmental disaster. … The diversion of such large amounts of energy resources to mining virtual currencies can have unfavourable long-term economic consequences. Further, the energy-intensive nature of cryptocurrencies must be examined along with the data localisation requirements proposed by the RBI as well as the proposed Personal Data Protection Bill, 2018. The proposed Bill provides that the Central Government may notify categories of personal data that shall only be stored or processed in India. Reading that with another provision, which already provides for at least one copy of personal data to be stored in India, cryptocurrencies could potentially take up an enormous amount of energy in an already power-starved India.*"[121]

Response: The Committee Report provides no data on how much electricity is consumed by crypto-asset mining in India. It also does not attempt to provide an estimate of the same. While the statement that Bitcoin mining has used as much electricity as all of Switzerland initially appears convincing as a supporting fact, it breaks down on closer analysis. The data shows that 74% of Bitcoin mining nodes are concentrated in 10 countries, and India is not even in the top 20 countries.[122] Japan, which is ranked number 10, contributes to 2.04% of Bitcoin mining nodes. While data regarding the percentage contribution to Bitcoin mining of India does not appear to be available, given its rank at number 28, it can be surmised to contribute significantly less than 2.04%. The United States and Germany, the top 2 countries, contribute to 25.70% and 20.06% of mining nodes respectively, and neither have prohibited crypto-asset activity but take regulatory approaches towards it. Interestingly, Switzerland, a country with a population less than Bengaluru,[123] is number 13 on the list (implying that Bitcoin mining is a non-trivial proportion of its electricity consumption). Still, Switzerland does

[121] Committee Report (n 57) 29 and 30.

[122] *Datalight* <https://datalight.me/blog/researches/infographics/datalight-publishes-a-list-of-countries-with-the-largest-number-of-bitcoin-nodes/> accessed 4 June 2020; Matthew Beedham, '3 Countries Host Over 50% of the World's Bitcoin Nodes' (*The Next Web*, 2 February 2019) <https://thenextweb.com/hardfork/2019/02/27/3-countries-50-perecent-bitcoin-network/> accessed 4 June 2020.

[123] 'Swiss Population Hits 8.5 Million Mark for First Time' (*The Local*, 27 August 2019) <https://www.thelocal.ch/20190827/85-million-inhabitants-and-rising-what-switzerlands-latest-population-figures-reveal> accessed 4 June 2020; 'Bengaluru's Migrants Cross 50% of the City's Population' (*The Times of India*, 4 August 2019) <https://timesofindia.indiatimes.com/city/bengaluru/bengalurus-migrants-cross-50-of-the-citys-population/articleshow/70518536.cms> accessed 4 June 2020.

not prohibit Bitcoin mining but regulates crypto-asset activity in a nuanced manner.[124]

Regarding the potential consequences of the draft Personal Data Protection Bill, 2018, the Committee Report does not analyze why the effect of any data localization requirements on the crypto-asset industry would be more than the effect on any other industry e.g., online cloud storage platforms. According to Fortune, data centers consume about 2% of electricity worldwide whereas Bitcoin is estimated to consume much less (between 0.165% and 0.33% of electricity worldwide).[125]

Interestingly, the Committee Report cited a study to state that an estimated 19 households in the United States can be powered for one day by the electricity consumed in a single Bitcoin transaction. By contrast, the Fortune report mentioned above contained this anecdote: "*The music video for "Despacito" set an Internet record in April 2018… In the process, 'Despacito' reached a less celebrated milestone: it burned as much energy as 40,000 U.S. homes use in a year.*"[126] Yet it could be nobody's case that there should be a ban on online cloud or streaming services due to energy consumption.

In any case, technological advances are reducing the energy consumption concern. In November 2018, Intel was awarded a patent for "*energy-efficient high performance bitcoin mining*".[127] Further, many newer crypto-assets are more energy-efficient than Bitcoin,[128] and new consensus mechanisms like proof-of-stake could end concerns about energy consumption.[129]

Still, if the Committee was apprehensive about the impact of crypto-asset mining on power consumption, it ought to have sought an expert opinion

---

[124] FINMA, 'FINMA Publishes ICO Guidelines' (16 February 2018) <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/> accessed 4 June 2020.

[125] Naomi Xu Elegant, 'The Internet Cloud Has a Dirty Secret' (*Fortune*, 18 September 2019) <https://fortune.com/2019/09/18/internet-cloud-server-data-center-energy-consumption-renewable-coal/> accessed 4 June 2020; Nicola Jones, 'How to Stop Data Centres from Gobbling up the World's Electricity' (*Nature*, 13 September 2018) <https://www.nature.com/articles/d41586-018-06610-y> accessed 4 June 2020.

[126] Elegant (n 125).

[127] Nikhilesh De, 'Intel Wins Patent for Energy-Efficient Bitcoin Mining' (*Coindesk*, 30 November 2018) <https://www.coindesk.com/intel-just-won-a-patent-for-an-energy-efficient-bitcoin-miner> accessed 4 June 2020.

[128] Eg, Rob Matheson, 'A Faster, More Efficient Cryptocurrency' (*MIT News*, 23 January 2019) <http://news.mit.edu/2019/vault-faster-more-efficient-cryptocurrency-0124> accessed 4 June 2020.

[129] GF, 'Why Bitcoin Uses so Much Energy' (*The Economist*, 9 July 2018) <https://www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy> accessed 4 June 2020.

on the topic based on empirical data and scientific analysis. Energy consumption is an inherently statistics-driven field. None of the Committee's members were experts in the field. The Ministry of Power has, to the author's knowledge, to date expressed no concern on the energy consumption associated with crypto-assets.[130] Instead of an empirical analysis, however, the Committee Report has made a speculative statement that crypto-asset activity "*could have unfavourable long-term economic consequences*" and "*could potentially take up an enormous amount of energy in an already power-starved India*". In the event any negative impact of crypto-assets on energy consumption in India is actually found after a scientific study, it should be addressed by proportionate regulation rather than an outright prohibition.

VI. Other Infirmities in the Committee Report

The Committee Report also suffers from the following defects:

1. Contradictions with other government reports: A 'Steering Committee on Fintech Related Issues'[131] ('**Steering Committee**') released its report in September 2019. Significantly, the Steering Committee was chaired by the same official who chaired the Committee. MeitY, RBI, and SEBI, which were also part of the Committee, were also represented on the Steering Committee. Yet, the Steering Committee, whose report was published a few months after the Committee Report, acknowledged the benefits associated with crypto-assets and did not discuss any of the disadvantages cited in the Committee Report.[132] Similarly, other government reports as well as publications of reputed

[130] Based on an automated search of Ministry of Power-Government of India <https://powermin.nic.in/> accessed 4 June 2020.

[131] Department of Economic Affairs, *Report of the Steering Committee on Fintech Related Issues* (Ministry of Finance-Government of India, 2019) 43 <https://dea.gov.in/sites/default/files/Report%20of%20the%20Steering%20Committee%20on%20Fintech.pdf> accessed 4 June 2020 (Steering Committee report).

[132] The Steering Committee report (n 131) 11, 16, 20 and 21 states, "However, the broader fintech landscape all over the world comprises of a variety of day-to-day financial services enhanced by technology. Mobile payments, cryptocurrency, investment advisory, insurance aggregators, peer-to-peer lending and some more services which traditionally required human capital, now form the fintech landscape. fintech comprises of technology-based businesses that compete against, enable and/or collaborate with financial institutions. … Cryptography, as an instrument for fintech, has four key benefits for financial firms: (a) confidentiality, (b) privacy, (c) non-repudiation, and (d) integrity. … Cryptography also forms the backbone of DLT and blockchain based systems such as Virtual Currencies. … 1.2.3 Digital currencies and tokens … The mechanisms surrounding cryptocurrencies, particularly the Blockchain and Initial Coin Offerings (ICOs), are revolutionising the global fintech landscape. The issue of initial coin offerings has emerged as an innovative way of capital raising by fintech businesses. … ICOs generally operate as blockchain-based

institutions have acknowledged both benefits and risks associated with crypto-assets.[133] The Committee Report, however, presents a one-sided picture, discussing none of the benefits associated with crypto-assets. The contradictions between the Committee Report and these other government reports, and the fact of the Committee Report not considering any benefits of crypto-assets (which are material facts which were readily available and ought to have been considered), disclose a non-application of mind that could well be found to fall foul of Article 14 in the event the Draft Bill is enacted into law.

2. Lack of deliberation: The Committee held three formal meetings over its 15-month tenure: on November 27, 2017, February 22, 2018, and January 9, 2019. Until the third meeting, the Committee was split as to whether crypto-assets should be regulated or prohibited. In fact, minutes of the first meeting record that the Committee agreed that "*[t]he banning option is very difficult to implement. It may also drive some operators underground which may encourage use of such 'currencies' for illegitimate purposes*."[134] In the second meeting on February 22, 2018,[135] two members favoured a regulatory approach and two members favoured the banning approach, with the Chairman appearing to lean towards the regulatory option. The Secretary, MeitY, in fact stated that "*India, being a very large economy and in the forefront of technological innovation, should have [an] open attitude towards this phenomenon and develop its options accordingly.*" The Committee then resolved that the Department of Economic Affairs and SEBI would each prepare papers, including a draft law, on the option of regulating crypto-asset activity, while the RBI and CBDT would prepare detailed papers, along with a draft law, on the option of banning crypto-asset activity. However, in the third meeting, held almost a year later, the Committee abruptly appears to have decided on a prohibition and approved a draft report and bill to this effect.[136]

---

funding process that enables the issuance of virtual coins or tokens in exchange for fiat currency or cryptocurrency payment."

[133] Ministry of Finance-Government of India, *Committee on Digital Payments Medium Term Recommendations to Strengthen Digital Payments Ecosystem Report* (December 2016) <https://dea.gov.in/sites/default/files/watal_report271216.pdf> accessed 4 June 2020; Digital Banking report (n 90); Institute for Development and Research in Banking Technology, *Blueprint of Platform for Banking Sector and Beyond* (IDRBT, White Paper, January 2019) <https://www.idrbt.ac.in/assets/publications/Best%20Practices/BCT_2019.pdf> accessed 4 June 2020; Institute for Development and Research in Banking Technology (n 6).

[134] Committee Report (n 57) 82.

[135] Committee Report (n 57) 84-85.

[136] Committee Report (n 57) 90-93.

There is no reasoning provided anywhere in the minutes or elsewhere in the Committee Report as to why prohibition was chosen rather than regulation, especially when members of the Committee were actively considering regulation in just the previous meeting.

Every new technology comes with its share of risks and potential abuse, eg, the Internet as a vehicle for fraud and child pornography. Merely reciting the risks associated with a technology would not show application of mind as to a regulatory solution. The Committee's approach, if followed for the Internet, may have resulted in a law banning the use of the Internet. The Committee Report does not engage with why a balanced regulatory solution, or any measure less invasive than a ban, was not appropriate. Given the constitutional law precedents above emphasizing the importance of rational deliberation, this lack of reasoning in the Committee Report on the choice of a prohibition, and the unexplained change in approach from one meeting to the next, demonstrates a non-application of mind.

3. Lack of expertise and representation: Despite crypto-assets being a technical subject, the Committee did not consist of any technical experts on mathematics, cryptography, crypto-assets or blockchain technology, or any private sector representatives from the software or technical community in India or globally. On the other hand, reports of the IDRBT, a technical body and a government institution set up by the RBI, recognize the benefits associated with crypto-assets.[137] Similarly, the Secretary, MeitY, as stated above, was wary of a prohibitive approach. The Committee Report does not engage with the question of why the benefits of crypto-assets should not be allowed to develop in India. Further, as stated above, though the RBI was represented on the Committee, the Committee Report and the annexed minutes do not indicate whether any theoretical or empirical economic analysis was done on the impact of crypto-assets on the economy. Therefore, as far as both technology and economics are concerned, the Committee Report indicates a lack of expert study.

4. Vagueness: Moreover, certain key provisions of the Draft Bill are legally and conceptually vague. For instance, the very definition of the term 'Cryptocurrency' appears to be misdirected[138] and the operative

[137] Institute for Development and Research in Banking Technology (n 133); Institute for Development and Research in Banking Technology (n 6).

[138] The said definition in cl 2(1)(a) reads as follows, "'*Cryptocurrency', by whatever name called, means any information or code or number or token not being part of any Official Digital Currency, generated through cryptographic means or otherwise, providing a*

clauses imposing the prohibition appear to conflict with each other.[139] Further, unless the State purchases the crypto-assets held by existing holders, it is unclear how such holders are expected to dispose of these crypto-assets, since there would be no willing buyer in India (in view of the threat of criminal prosecution) and there is no clarity on selling to a foreign buyer under FEMA.[140] Regardless of the policy position ultimately taken, the Draft Bill needs to be overhauled by the Legislative Department of the Ministry of Law and Justice. As it currently stands, it could well be argued that it is unconstitutionally vague.

5. 'Blockchain good, crypto bad' narrative: There is a popular narrative, including in the Committee Report, that blockchain technology is desirable while crypto-assets are undesirable. However, a closer examination of the technology suggests otherwise. In a blockchain network with a native crypto-asset, it is the crypto-asset which acts as the incentive to participants to validate transactions. Traditionally, a central party (such as a clearing agency) would validate transactions in exchange for fees, but in crypto-asset networks, the entire network of participants validates transactions in exchange for the crypto-asset as mining rewards or transaction fees. This distributes the risk associated with a central party. While there can be 'blockchain' or distributed ledger technology implementations which do not use a crypto-asset, any blockchain implementation which seeks to be minimize centralization by incentivizing a wide variety of participants will need to have a crypto-asset. These are usually, but not always, public blockchains. This understanding has been expressly confirmed by multiple computer scientists and blockchain technology experts, including Arvind Narayanan, Associate Professor,

---

digital representation of value which is exchanged with or without consideration, with the promise or representation of having inherent value in any business activity which may involve risk of loss or an expectation of profits or income, or functions as a store of value or a unit of account and includes its use in any financial transaction or investment, but not limited to, investment schemes." (emphasis added).

[139] Cls 8(1) and (2) appear not to reconcile with each other, since they provide different punishments for the same offences. Cl 8(1) provides a certain punishment for the violation of '*clauses (e), (g) and/or (h) of sub-section (1) of Section 7*' and cl 8(2) refers to '*subsection (1) of section 7 or clauses (a), (b), (c), (d) and/or (f) of sub-section (1) of Section 7*'. The text in bold indicates overlap between the two, and therefore, uncertainty on the punishment provided for (emphasis provided).

[140] RBI response dated May 9, 2018, to Varun Sethi, stating, '*Virtual Currency is not recognized as currency under Section 2(h) of Foreign Exchange Management Act 1999 (FEMA). Hence, no guidelines have been framed on virtual currencies under FEMA*.' <https://drive.google.com/file/d/1TeePIKQx5G--mg5dsDMHfcH89q7dUHzM/view?usp=drive_open> accessed 4 June 2020.

Princeton University;[141] Vitalik Buterin, co-founder, Ethereum (one of the leading blockchain networks used by both enterprises and governments);[142] and Andreas Antonopoulos, author, 'Mastering Bitcoin' and 'Internet of Money';[143] and implicitly by Turing award winners and Massachusetts Institute of Technology professors who have developed the crypto-asset system 'Algorand'.[144] There is also literature to suggest that 'private blockchains' are not particularly innovative, and have been in existence since the 1990s.[145] The following are some examples showing that crypto-assets are demonstrably intertwined with blockchain technology:

- 'Bankchain' (an alliance of over 35 reputed banks and institutions including State Bank of India SBI, HDFC Bank, ICICI Bank, Deutsche Bank, Citibank, and National Payments Corporation of India (NPCI)), whose slogan is 'Blockchain for Banks' and which is the leading body in the Indian financial sector seeking to implement blockchain technology, cited the use of a "*crypto-token*" for its use-cases.[146]
- The Enterprise Ethereum Alliance, which is a global consortium of over 500 reputed institutions globally, including Accenture, Deloitte, Government of Andhra Pradesh, HP, Infosys, J.P. Morgan, Microsoft, and Samsung seeking to implement blockchain technology, uses the Ethereum blockchain, which natively has a crypto-asset, Ether.[147]
- The IDRBT report titled 'Blueprint of Blockchain Platform for Banking Sector and Beyond' (2019) contains multiple references to

---

[141] Arvind Narayanan and Jeremy Clark (n 4); Arvind Narayan, '"Private Blockchain" is Just a Confusing Name for a Shared Database' (*Freedom to Tinker*, 18 September 2015) <https://freedom-to-tinker.com/2015/09/18/private-blockchain-is-just-a-confusing-name-for-a-shared-database/> accessed 4 June 2020.

[142] Allen Scott, 'Vitalik Buterin: Russia's Crypto Ban Would Stifle Blockchains' (*Bitcoin.com*, 17 May 2016) <https://news.bitcoin.com/buterin-ban-russia-stifle-blockchains/> accessed 4 June 2020.

[143] Andreas Antonopoulos, 'Bitcoin Q&A: "Blockchain, not Bitcoin"' (*YouTube: aantonop*, 7 June 2018) <https://www.youtube.com/watch?v=r2f0HlaRdgo> accessed 4 June 2020.

[144] Yossi Gilad (n 5).

[145] Arvind Narayanan (n 141); Also see (n 7 and n 8).

[146] Eg, A Bankchain document titled 'Primechain-P5: The Blockchain for Moving Money Globally' dated 19 March 2018, on file with the author, states a 'key feature' of the solution to be '*[r]eal world asset-backed* crypto tokens *provide liquidity*' and that '*[b]lockchains are provably immutable and enable the rapid transfer and exchange of* crypto-tokens *(which can represent assets) without the need for separate clearing, settlement and reconciliation.*' (emphasis added).

[147] *Enterprise Ethereum Alliance* <https://entethalliance.org/> accessed 4 June 2020.

the use of the Ethereum blockchain network (which functions based on the crypto-asset Ether) as well as to the term "*digital assets*".[148]

- A report co-authored by the National Association of Software and Services Companies (NASSCOM), whose members include Infosys, Microsoft, Wipro, Cognizant, Tata Consultancy Services and many others, states,

  "There is need for positive signaling from the Government of India, and efforts to drive the growth of the Blockchain ecosystem in India through provision of timely and well-defined regulatory guidance. … India needs to act fast and work consultatively with the key stakeholders in the crypto/blockchain community and provide regulatory certainty and clarity around blockchain technology (specifically around cryptocurrencies and digital tokens)."[149] (emphasis added)

  A subsequent statement of NASSCOM – after taking note of the Committee Report – recommends a regulatory rather than prohibitory stance towards crypto-assets.[150]

- Similarly, a study by Incrypt, a non-profit organisation, based on a survey of 97 blockchain software developers in India, found that open, public blockchains (powered by crypto-assets) can be a new growth driver of the Indian economy in a similar manner that the IT services industry was, and that 84% of the blockchain developers surveyed believed that if the government does not allow crypto-assets, they may move abroad or only work on foreign projects / startups.[151]

The above reasoning may have been dealt a blow by the decision in the *IAMAI* case which states that distributed ledger technology and virtual

---

[148] Institute for Development and Research in Banking Technology (n 133).

[149] *NASSCOM Avasant India Blockchain Report 2019* <https://www.nasscom.in/knowledge-center/publications/nasscom-avasant-india-blockchain-report-2019> accessed 4 June 2020.

[150] "*NASSCOM believes that the recent proposal of the Inter-ministerial Committee of the Government to ban all cryptocurrencies barring those that are backed by the Government, is not the most constructive measure. Instead, the government should work towards developing a risk based framework to regulate and monitor cryptocurrencies and tokens. A ban would inhibit new applications and solutions from being deployed and would discourage tech Startups. It would handicap India from participating in new use cases that cryptocurrencies and tokens offer.*" NASSCOM, *Banning Cryptocurrency is not the Solution, a Regulatory Framework must be Developed: NASSCOM*(2019) <https://www.nasscom.in/sites/default/files/media_pdf/Banning_cryptocurrencies_is_not_the_solution_a_regulatory_framework_must_be_developed.pdf> accessed 4 June 2020.

[151] Incrypt, *The Incrypt Policy Report: Realising India's Blockchain Potential* (August 2018) 22 <https://www.incrypt.co/policy> accessed 4 June 2020.

currencies can be separated.[152] However, the Court does not appear to have entered into a consideration of the above factors. Moreover, it is not being contended in this article that there can be no distributed ledger technology / blockchain technology without crypto-assets. It is only being stated that crypto-assets are essential to many important applications of blockchain technology, as demonstrated by the examples above. In the words of Vitalik Buterin, one of the foremost experts in the space and the person who conceived of the Ethereum network, "*if there's no cryptocurrency [...] then at least public blockchains would not work. Private chains could if some kind of solution is developed but the blockchain as a system would be severely restricted.*"[153] Therefore, the Committee Report's stated recommendation to promote distributed ledger technology would mean that what would be promoted is a limited, narrow use of the technology, rather than its full potential. There is no discussion of this nuance in the Committee Report.

VII. Comparative Perspective

The G20 is an international forum consisting of the world's leading economies, which is recognized as the "*premier forum for international economic cooperation*".[154] According to a 2014 statement, G20 members represented around 85 per cent of global gross domestic product, over 75 per cent of global trade, and two-thirds of the world's population.[155] The members of the G20 are: Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Republic of Korea, Mexico, Russia, Saudi Arabia, South Africa, Turkey, United Kingdom, United States, and European Union.[156]

While these jurisdictions differ in political and constitutional values, none of the G20 members have introduced an outright ban on crypto-asset activity. The Draft Bill, if introduced, would be the most extreme measure

[152] *IAMAI case* paras 6.136 and 6.137.
[153] Scott (n 142).
[154] G20 2020 Saudi Arabia, *About the G20* (g20.org) <https://g20.org/en/about/Pages/default.aspx> accessed 4 June 2020.
[155] G20 Australia 2014, *G20 Members* <https://web.archive.org/web/20140203221840/http://www.g20.org/about_g20/g20_members> accessed 4 June 2020.
[156] G20 2020 Saudi Arabia, *G20 Participants* (g20.org) <https://g20.org/en/about/Pages/Participants.aspx> accessed 4 June 2020.

introduced by any of these jurisdictions. China,[157] India,[158] Indonesia,[159] and Saudi Arabia[160] are the countries which currently contain severe restrictions on crypto-asset activity, although none of these restrictions amount to an outright ban in the nature of the Draft Bill. More importantly, jurisdictions which India draws guidance from and whose constitutional values resemble those of India, including Australia,[161] Canada,[162] the European Union

---

[157] Chi Jingyi, 'Ruling Signals Nation Likely to Loosen Controls Over Digital Currencies' (*Global Times*, 18 July 2019) <http://www.globaltimes.cn/content/1158377.shtml> accessed 4 June 2020; Jacob Blacklock and Steve Shi, 'China' in Josias Dewey (ed), *Blockchain and Cryptocurrency Regulation 2020* (2nd edn, Global Legal Insights 2020) <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/china> accessed 7 June 2020.

[158] The RBI circular dated 6 April 2018, prohibiting banks and other financial institutions from facilitating crypto-asset transactions (which was set aside by the Supreme Court in the *IAMAI case*). <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11243&Mode=0> accessed 4 June 2020.

[159] 'Futures Exchange Authority Issues Regulation on Cryptocurrency' (*The Jakarta Post*, 13 February 2019) <https://www.thejakartapost.com/news/2019/02/13/futures-exchange-authority-issues-regulation-on-cryptocurrency.html> accessed 4 June 2020; *Regulation of Cryptocurrency Around the World* (Law Library of Congress, June 2018) <https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf> accessed 4 June 2020.

[160] 'The Virtual Currencies Are Not Regulated Inside the Kingdom of Saudi Arabia' (*Saudi Arabian Monetary Authority*, 12 August 2018) <http://www.sama.gov.sa/en-US/News/Pages/news12082018.aspx> accessed 4 June 2020; 'A Statement on Launching "Aber" Project' (*Saudi Arabian Monetary Authority*, January 2019) <http://www.sama.gov.sa/en-US/News/Pages/news29012019.aspx> accessed 4 June 2020; Stephen O'Neal, 'From Qatar to Palestine: How Cryptocurrencies Are Regulated in the Middle East' (*Coin Telegraph*, 4 September 2018) <https://cointelegraph.com/news/from-qatar-to-palestine-how-cryptocurrencies-are-regulated-in-the-middle-east> accessed 4 June 2020.

[161] Australian Securities and Investments Commission, *Senate Inquiry into Digital Currency, Submission by the Australian Securities and Investments Commission* (Submission 44, December 2014) <http://www.aph.gov.au/DocumentStore.ashx?id=4b6d105f-3e0a-4d52-aaab-1f35842ed5f1&subId=302297> accessed 4 June 2020; Webb Henderson, 'Australia' in *The Virtual Currency Regulation Review* (The Law Reviews, 2nd edn, November 2018) <https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-1/1176625/australia> accessed 4 June 2020; Peter Reeves, 'Australia' in Josias Dewey (ed), *Blockchain and Cryptocurrency Regulation 2020* (Global Legal Insights, 2nd edn, 2020) <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/australia> accessed 4 June 2020.

[162] Alix d'Anglejan-Chatillon and others, 'Canada' in *The Virtual Currency Regulation Review* (The Law Reviews, 2nd edn, November 2018) <https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-1/1176638/canada> accessed 04 June 2020; Canadian Staff Notice, Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets (CSA Staff Notice 21-327, 16 January 2020) <https://www.osc.gov.on.ca/documents/en/Securities-Category2/csa_20200116_21-327_trading-crypto-assets.pdf> accessed 4 June 2020.

('**E.U.**'),[163] South Africa,[164] the United Kingdom,[165] and the United States[166] all allow crypto-asset activity within the bounds of regulation. Other common law jurisdictions not in the list, such as Hong Kong,[167] New Zealand,[168] and Singapore,[169] too follow this approach.

---

[163] European Commission, 'Strengthened EU Rules to Prevent Money Laundering and Terrorism Financing' (European Commission Fact Sheet, 15 July 2018, vol VI, annex A 22) <https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=610991> accessed 4 May 2020; Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843> accessed 4 June 2020.

[164] Angela Itzikowitz and Ina Meiring, 'South Africa' in Josias Dewey (ed), *Blockchain and Cryptocurrency Regulation 2020* (Global Legal Insights, 2nd edn, 2020) <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/south-africa> accessed 4 June 2020; *Regulation of Cryptocurrency Around the World* (Law Library of Congress, June 2018) <https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf.> accessed 4 June 2020.

[165] Peter Chapman and Laura Douglas, 'UK' in *The Virtual Currency Regulation Review* (The Law Reviews, 2nd edn, November 2018) <https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-1/1176672/united-kingdom> accessed 4 June 2020; Stuart Davis, Sam Maxson, and Andrew C. Moyle, 'United Kingdom' in Josias Dewey (ed), *Blockchain and Cryptocurrency Regulation 2020* (2nd edn, Global Legal Insights 2020) <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/united-kingdom> accessed 6 June 2020; UK Government, *Cryptoassets Taskforce: Final Report* (October 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf> accessed 4 June 2020.

[166] Michael S. Sackheim and others, 'USA' in *The Virtual Currency Regulation Review* (The Law Reviews, 2nd edn, November 2018) <https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-1/1176673/united-states> accessed 4 June 2020; Joe Dewey, 'USA' in Josias Dewey (ed), *Blockchain and Cryptocurrency Regulation 2020* (Global Legal Insights, 2nd edn, 2020) <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa> accessed 4 June 2020.

[167] Henry Yu, 'Hong Kong' in Josias Dewey (ed), *Blockchain and Cryptocurrency Regulation 2020* (2nd edn, Global Legal Insights 2020) <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/hong-kong> accessed 4 June 2020.

[168] Deemple Budhia and Tom Hunt, 'New Zealand' in *The Virtual Currency Regulation Review* (2nd edn, The Law Reviews, November 2018) <https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-1/1176659/new-zealand> accessed 4 June 2020; Individual income tax (Questions & Answers: Cryptocurrency and tax), New Zealand Inland Revenue (undated) <https://www.classic.ird.govt.nz/income-tax-individual/cryptocurrency-qa.html> accessed 4 June 2020; Tax Information Bulletin, Inland Revenue Department (July 2019) <https://www.classic.ird.govt.nz/resources/1/c/1c6029d0-611c-4a15-9cbf-b712129ab76c/tib-vol31-no7.pdf> accessed 4 June 2020.

[169] Laney Zhang, 'Singapore: Payment Services Act Passed, Regulating Cryptocurrency Dealing or Exchange Services'(Global Legal Monitor, 17 April 2019) <https://www.loc.gov/law/foreign-news/article/singapore-payment-services-act-passed-regulating-cryptocurrency-dealing-or-exchange-services/> accessed 4 June 2020; Adrian Ang V-Meng and others, 'Singapore' in *The Virtual Currency Regulation Review* (2nd edn, The Law Reviews, November 2018) <https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-1/1176666/singapore> accessed 4 June 2020.

This is not to say that India should not think for itself. However, all of these jurisdictions, as well as the G20 as a body, have recognized that there are risks associated with crypto-assets, and the risks they recognize resemble some of the risks cited in the Committee Report. However, their reaction has not been to resort to an outright prohibition. They have sought to extend existing laws to crypto-asset activities and develop new regulations where necessary (specific anti-money-laundering laws in Canada and the E.U. being examples). There are at least 41 significant jurisdictions adopting a regulatory approach (these include countries with foreign exchange controls, such as South Africa).[170] While all of these laws are in their infancy, and may well require reiteration as the technology progresses, the key learning for India is that the risks cited in the Committee Report do not necessitate a prohibition.

The international experience hence shows that less invasive measures are available, and that there is no reason why India cannot regulate crypto-asset technology – giving a nod to both liberty and innovation – rather than prohibiting it outright.

The Supreme Court in the *IAMAI* case appears to deal a blow to the comparative approach by rejecting it in the context of the RBI circular on virtual currencies.[171] However, it does so because: (a) of India's statutory scheme, (b) of India's economic conditions, and (c) it appears to consider whether the global approach was *by itself* a ground to challenge the RBI circular. However, the reason for the comparative approach in this article is on a different footing: (a) since the Draft Bill is itself a statute, it is the constitutional scheme that is relevant and not the statutory scheme; (b) the comparative approach can be applied if it is shown that the impact of crypto-assets on India's economic condition is not unique to India; and (c) most importantly, the comparative approach in this article is not intended to be a ground of challenge in itself, but to merely act as persuasive evidence demonstrating the availability of less invasive measures to address a similar problem. The Court in the *IAMAI* case in fact endorses this approach since it referred to an E.U. Parliament report rejecting an outright ban while examining whether the RBI had considered the availability of alternative, less invasive measures.[172]

---

[170] Based on the author's analysis as of August 2019, these jurisdictions are as follows: 1. Argentina, 2. Australia, 3. Brazil, 4. Canada, 5. The EU, 6. France, 7. Germany, 8. Italy, 9. Japan, 10. Mexico, 11. Russia, 12. South Africa, 13. South Korea, 14. Turkey, 15. UK, 16. USA, 17. Austria, 18.Belgium, 19. Czech Republic, 20. Denmark, 21. Finland, 22. Greece, 23. Hong Kong, 24. Hungary, 25. Iceland, 26. Ireland, 27. Israel, 28. Malaysia, 29. Malta, 30. Netherlands, 31. New Zealand, 32. Norway, 33. Philippines, 34. Poland, 35. Portugal, 36. Singapore, 37. Spain, 38. Sweden, 39. Switzerland, 40. Taiwan, 41. Thailand.

[171] *IAMAI* case paras 6.129 and 6.130.

[172] *IAMAI* case paras 6.162-6.164.

VIII. Conclusion: Is the Draft Bill A Reasonable Restriction?

The *IAMAI* case, in its setting aside of the RBI circular on virtual currencies, is a powerful affirmation that the Supreme Court's long-established principles of proportionality squarely apply to the crypto-asset sphere.

For the reasons stated in this article, the Draft Bill is unlikely to be a reasonable and proportionate restriction on the fundamental rights named above. It proposes an imprisonment term of up to 10 years for the use of 'cryptocurrency' for nearly any purpose, including buying, selling, storing, and providing 'cryptocurrency-related services'.[173] As stated in the *Aadhaar* case, cited above, the presumption of criminality is treated as disproportionate and there cannot be sweeping provisions targeting entire categories of persons (in this case, persons dealing with crypto-assets, estimated to be 50 lakh in number) as suspicious. In line with the *Chintaman Rao* case, the banning of legitimate activity has no rational connection to, and goes much in excess of, the purpose of the draft legislation, which is only intended to curb unlawful activity, protect consumers, and preserve financial stability.

As shown by the above point-by-point responses, none of the Committee Report's reasons in support of the Draft Bill hold up to close scrutiny when one examines whether they can be used to justify an outright prohibition. Further, any remaining concerns which are legitimate can be effectively addressed with less invasive measures. There is no rational basis for the proposed prohibition or for why less invasive measures cannot be implemented to achieve the Draft Bill's objectives. Even violations of FEMA – which is a statute with similar aims to the Draft Bill – are civil offences and not criminal offences; moreover, FEMA is a regulatory statute and not an outright prohibition. Similarly, the PMLA provides checks and balances on various sectors prone to money laundering (eg, real estate and precious metals),[174] rather than ban such activities altogether. We have suggested many less invasive options for crypto-asset regulation in India in our Regulatory Suggestions Paper.[175] The international experience, summarized above, also provides persuasive evidence to show that a variety of less invasive measures are available to address the same concerns.

---

[173] Draft Bill, cl 7.
[174] Prevention of Money Laundering Act 2002, s 2(1)(sa).
[175] Nishith Desai (n 17).

In fact, as the Committee itself recognized in its first meeting, and as discussed in our Regulatory Suggestions Paper,[176] banning crypto-asset activity is likely to be counter-productive. Legitimate activity is stopped while the government loses oversight of illegitimate activity, which can in fact be monitored through the records maintained by regulated crypto-asset exchanges and wallet providers. The government has already used the records maintained by crypto-asset exchanges to aid in its criminal investigations and prosecutions. A ban on crypto-asset activity would remove this important law enforcement aid. Signs of this counter-productive effect already emerged after the RBI circular on virtual currencies.[177]

Further, for the detailed reasons stated above, the Draft Bill may be considered arbitrary to the extent that:

(a) crypto-assets are being treated differently from other phenomena like physical cash, commodities (particularly, gold), securities, loyalty points systems, and the Internet, though each of the concerns in the Committee Report applies to one or more of these phenomena;

(b) the underlying Committee Report is one-sided and does not proceed on a rational and scientific basis; and,

(c) certain provisions like the very definition of, and prohibition of dealing in, crypto-assets are vague, leading to a "*boundless sea of uncertainty*", a phenomenon frowned upon by the Supreme Court.[178]

As far as the interest of commerce and innovation is concerned (a factor which may be relevant in an assessment of a restriction "*in the interest of the general public*" under Article 19(6)), as stated above, various software industry voices, including NASSCOM, the leading software industry trade body, have stated that the Committee Report's recommendation of an outright ban is excessive, and that risk-based regulation should be adopted instead.

---

[176] Nishith Desai (n 17).

[177] Reserve Bank of India (n 91) which states, '*Developments on this front need to be monitored as some trading may shift from exchanges to peer-to-peer mode, which may also involve increased usage of cash. Possibilities of migration of crypto exchange houses to dark pools/cash and to offshore locations, thus raising concerns on AML/CFT and taxation issues, require close watch.*'; 'Dabba Trading sees an Upsurge in Wake of RBI's Cryptocurrency Ban' (Business Today, 30 July 2018) <https://www.businesstoday.in/current/corporate/dabba-trading-sees-an-upsurge-in-wake-of-rbi-diktat-banning-crypto-currencies/story/280800.html> accessed 4 June 2020 which states, '*Ever since the banks were stopped from providing financial services to digital exchanges, the trade of Bitcoin through Dabba trading has increased manifold, and the whole purpose of stopping the flow of illicit money seems to have been defeated.*'

[178] *State of M.P. v Baldeo Prasad*, AIR 1961 SC 293.

The balanced outlook has perhaps been best summarized by Christine Lagarde, Managing Director of the International Monetary Fund, who wrote,

> A judicious look at crypto-assets should lead us to neither crypto-condemnation nor crypto-euphoria. Just as a few technologies that emerged from the dot-com era have transformed our lives, the crypto-assets that survive could have a significant impact on how we save, invest and pay our bills. That is why policymakers should keep an open mind and work toward an even-handed regulatory framework that minimizes risks while allowing the creative process to bear fruit.[179]

[179] Christine Lagarde, 'An Even-handed Approach to Crypto-Assets' (*IMF Blog*, 16 April 2018) <https://blogs.imf.org/2018/04/16/an-even-handed-approach-to-crypto-assets/> accessed 4 June 2020.

Competition Law Limits on Ride Sharing Enterprises – Taking into Account the Experience in India

Max Huffman[*]

Abstract *New economy competition policy is on the forefront of enforcers' minds across the globe, with numerous competition agencies engaged in competition advocacy efforts regarding the sharing economy generally or ride sharing specifically. In a sharing economy firm, extra-firm contracting may be as efficient as that occurring intra-firm. By reducing search and transaction costs, the sharing economy enables transactions that could not occur in a pre-internet economy. The sharing economy grew strongly in developed economies, all of which were burdened with legacy permitting systems such as taxicab medallions or zoning regulations and other oversight limiting public lodging. The promise in economies with substantial development ahead of them is much greater. However, with highly diffuse suppliers and consumers contracting through enterprises with substantial market presence, areas of competition policy concern include conspiracies, exercises of bargaining power, and productive agreements that may nonetheless limit competition and thereby require careful analysis of overall competitive effects. Finally, there is the possibility of an agreement creating both efficiencies and threatening competitive consequences, which must be evaluated holistically to appreciate its overall impacts. No clear competition law violation will exist in all cases. However, continual attention to areas of concern will be warranted for the foreseeable future.*

[*] Professor of Law, Indiana University Robert H McKinney School of Law. Thank you to the Indian Journal of Law and Technology for inviting this contribution and providing helpful edits and comments, to Prannv Dhawan, III Year, BA LLB (Hons), National Law School of India University, Bengaluru, for research and drafting assistance, and to Professor Bing Chen, Christa DeNeve, and Patrick Wright.

I. Introduction

The sharing economy has changed how we work and transact globally.[1] New economy competition policy is on the forefront of enforcers' minds across the globe. In the European Union ('**the EU**') and the United Kingdom ('**the UK**'), detailed reports on competition and market structure in digital markets spell out enforcement priorities.[2] The United States ('**the US**') Federal Trade Commission produced a detailed sharing economy report in 2016[3] and created its 'Technology Enforcement Division' to investigate, among other things, digital platform markets.[4] The Organisation for Economic Cooperation and Development ('**the OECD**') has made digital markets, and sharing economy enterprises specifically, the foci of its competition forum,

[1] *See*, Niam Yaraghi and Shamika Ravi, 'The Current and Future State of the Sharing Economy' (Brookings India Impact Series, 2017) 4 <https://www.brookings.edu/wp-content/uploads/2016/12/sharingeconomy_032017final.pdf> accessed 9 December 2019.

[2] Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, *Competition Policy for the digital era: Final report* (European Commission Directorate General for Competition, 2019) <http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf> accessed 9 December 2019; Jason Furman et al, *Unlocking Digital Competition: Report of the Digital Competition Expert Panel* (Competition and Markets Authority, 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf> accessed 9 December 2019.

[3] Federal Trade Commission, *The "Sharing" Economy: Issues Facing Platforms, Participants, and Regulators* (2016) 11 <https://www.ftc.gov/system/files/documents/reports/sharing-economy-issues-facing-platforms-participants-regulators-federal-trade-commission-staff/p151200_ftc_staff_report_on_the_sharing_economy.pdf> accessed 3 July 2019 (FTC Report).

[4] Federal Trade Commission, 'FTC Technology Enforcement Division' (2019) <https://www.ftc.gov/about-ftc/bureaus-offices/bureau-competition/inside-bureau-competition/technology-enforcement-division> accessed 9 March 2020; Federal Trade Commission, 'FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets' (Press Release, 2019) <https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology> accessed 9 December 2019.

and enforcers around the globe have contributed their insights and experience to those programs.[5] As of this writing, the United Nations Conference on Trade and Development ('**UNCTAD**') is coordinating a book project on the digital economy, including the sharing economy. Competition agencies in several jurisdictions have drafted their own or contracted out reports on the implications of the sharing economy for competition and consumer protection.[6] According to a 2019 International Competition Network survey, at least 10 competition agencies around the globe, including both the oldest and best funded (such as the US Federal Trade Commission) and the newer/less wealthy (such as the Croatia Competition Agency AZTN and Panama's Competencia), had engaged in competition advocacy efforts regarding the sharing economy generally or ride sharing specifically.[7]

The Competition Commission of India ('**the CCI**') has given close attention to these markets, by way of conducting a recent market study on e-commerce, including attention to the platform economy (excluding ride-sharing),[8] and contributing reports to last year's OECD roundtable[9] and to a recent UNCTAD meeting.[10] As the Chairperson of the CCI noted in a recent speech,

> [W]e are witnessing the emergence of the "digital economy". The dawn of this new economy has brought with it alterations in the contours of market, transformations in the ways of doing business, ways of communication, and of transactions. Digital technology is transforming markets at an unprecedented scale and pace. Business models, market access mechanisms, ways of communication and transactions are all being reshaped by digital mediation. The ongoing shift of markets

---

5 *See*, for example, Directorate for Financial and Enterprise Affairs Competition Committee, Organisation for Economic Co-operation and Development, *Taxi, ride-sourcing and ride-sharing services* (DAF/COMP/WP2(2018)1, 2018) <https://one.oecd.org/document/DAF/COMP/WP2(2018)1/en/pdf> accessed 9 December 2019 (OECD Report).

6 Australian Competition and Consumer Commission, *The Sharing Economy and the Competition and Consumer Act* (2015) <https://www.accc.gov.au/system/files/Sharing%20Economy%20-%20Deloitte%20Report%20-%202015.pdf> accessed 9 December 2019.

7 International Competition Network Advocacy Working Group, 'Report on ICN Members Recent Experiences (2015-2018) in Conducting Competition Advocacy in Digital Markets' (2019) <content/uploads/2019/06/AWG_AdvDigitalMktsReport2019.pdf> accessed 9 December 2019.

8 Competition Commission of India, *Market Study on e-Commerce in India* (2020) <https://www.cci.gov.in/sites/default/files/whats_newdocument/Market-study-on-e-Commerce-in-India.pdf> accessed 9 December 2019.

9 *See*, note by India in Directorate for Financial and Enterprise Affairs Competition Committee (n 5).

10 Intergovernmental Group of Experts on Competition Law and Policy, *Emerging issues before CCI relating to Digital Economy – Contribution by The Republic of India* (2019) <https://unctad.org/meetings/en/Contribution/ciclp18th_cont_India.pdf> accessed 9 December 2019 (UNCTAD Submission).

> towards a digital platform-centric configuration has opened up new opportunities while also posing new challenges for both market participants and regulators.[11]

Individuals transact with individuals, through sharing economy enterprises, for service contracts on a one-off basis; each service contract is an atom in any definable service market.[12] With highly diffuse suppliers and consumers contracting through enterprises with substantial market presence, areas of competition policy concern are many. These include conspiracies governing competitively sensitive subjects such as price, output, and quality; exercises of bargaining power conferred by a dominant position, including both the ability to establish a supra-competitive price and the ability to discriminate in price among similarly situated consumers; and productive agreements that may nonetheless limit competition and thereby require careful analysis of overall competitive effects.

Conspiracy, productive agreement, and abuse of dominance are unlikely to arise together. The competitive concern that emerges appears to depend on how we define the structure of a sharing economy enterprise. If we identify a centralised, single firm, with substantial market presence, pricing, output, and quality decisions, including differences in offerings as among similarly situated consumers, this presents a concern for abuse of dominance. As an example, a ride-sharing enterprise that acquires 50% or more of the share for ride hailing in a particular market and is determined by operation of law to employ its drivers and to sell services to consumers in competition with taxi operators, might readily be considered to have dominant market position.[13] This abuse of dominance may be manifested upstream as well as in the labour input market, in which individual suppliers compete for transactions and lack bargaining power vis-à-vis the enterprise.[14]

If, by contrast, we identify a nearly infinitely diffuse set of suppliers, combined in a loose alliance for marketing and distribution purposes, with the sharing economy enterprise filling the role of a joint agent, decisions on

---

[11] Ashok Kumar Gupta, 'Opening Remarks' (Antitrust Global Seminar Series, New Delhi, 8 February 2019) para 7 <http://www.cci.gov.in/sites/default/files/speeches/Opening_Remarks.pdf?download=1> accessed 9 December 2019.

[12] *See*, Mark Anderson and Max Huffman, 'The Sharing Economy Meets the Sherman Act: Is Uber a Firm, a Cartel, or Something In Between?' (2017)(3) Columbia Business Law Review 859 (outlining six defining features of the sharing economy).

[13] This would be the case if ride sharing drivers were treated as employees, as they recently have been held to be by the Cour de Cassation in France. *See*, *Judgment n°374 (19-13.316)* ECLI:FR:CCAS:2020:SO00374 (Courde Cassation, Chambre sociale).

[14] *See*, Julian Nowag, 'UBER between Labour and Competition Law' (2016) 3 Lund Student EU Law Review 95 (identifying the Scylla and Charybdis of abuse of dominance and anti-cartel prohibitions facing sharing economy enterprises).

price, output, and quality reached through the enterprise represent agreements among competitors.[15] This is the form of sharing economy enterprise that ride sharing enterprises purport to be – and, in markets including the US, have largely succeeded in being treated as.[16] Such agreements among suppliers tend to be treated, on their face, as violations of competition law, with criminal penalties in those jurisdictions that impose them and substantial fines elsewhere.[17] The strength of this rule is such that agreements are considered void ab initio or on a per se basis (with the choice of Latin phrases jurisdiction dependent).

Finally, there is the possibility of a productive venture, an agreement creating both efficiencies and threatening competitive consequences, which must be evaluated holistically to appreciate its overall impacts. This is where courts' treatment of ride sharing enterprises can be expected to be evaluated. Regulators and courts will be reluctant to allege and to find hard core cartel agreements buried in what many consider to be innovative twists on production and employment, which may promise substantial welfare gains – with benefits perhaps distributed among a new class of entrepreneurs, historically dependent on others for employment opportunities.

On a broad analysis of competition policy concerns arising in ride sharing, no one claim stands out as the obvious competition harm. Several possible claims exist, however, depending on the structure of the enterprise, the particular jurisdiction's laws governing both competition and employment, and the strength of the market in which it is situated. The nature of the competition law concerns calls to mind the adage, "*where there is smoke, there is fire*"; while no clear competition law violation will exist in all cases, continual attention to areas of concern will be warranted for the foreseeable future.

II. Antitrust Principles of Single Firms

The structure of sharing economy enterprises calls into question the legal rules and economic understanding surrounding the business firm. In an

---

[15] ibid.

[16] United States National Labor Relations Board – Office of the General Counsel, *Uber Technologies, Inc Cases 13-CA-163062, 14-CA-158833, and 29-CA-177483* (Advice Memorandum, 2019) 3 <https://apps.nlrb.gov/link/document.aspx/09031d4582bd1a2e> accessed 9 December 2019 ("*Applying the common-law agency test, we conclude that the UberX and UberBLACK drivers were independent contractors*"); *See contra*, California Assembly Bill No. 5 2019 <https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB5> accessed 9 December 2019 (broadening the definition of 'employee' under California state law).

[17] *See*, Anderson and Huffman (n 12) 902-04.

old-economy enterprise, the firm is easily defined as a centrally owned and organised enterprise that owns its own capital stock and employs its labour force, subject to well established laws governing the employment relationship. The old economy firm achieves efficiency benefits from integration that decrease as its scale becomes unwieldy. In a free market economic system, where the law favours competition to centralised planning, the firm is permitted to grow organically without intervention from regulators. As a matter of economic policy, including competition policy, the firm (once defined) is less likely to be restricted in its intra-firm operations. This has relevance to an analysis of the antitrust consequences of the sharing economy, which presents ambiguity as to the definition of a firm, by adopting attributes of old-economy firms, both in terms of labour force and capital stock.

A. The Law – United States and India

The concept of the single firm is the barrier between competition law theories based on agreement and those based on single-firm dominance. In the US, this is a distinction between Section 1 and Section 2 of the Sherman Antitrust Act, 1890 ('**the Sherman Act**').[18] Multiple firms are rarely challenged under Section 2 (although a claim of conspiracy to monopolise is theoretically possible).[19] India's Competition Act, 2002 ('**the Competition Act**') likewise follows this structure, outlawing certain agreements in Section 3 and certain activities by dominant firms in Section 4.[20]

The single firm-multiple firm divide breaks down in the presence of a 'collective dominance' theory, which the EU has nominally followed and which is expressly included in many national competition laws.[21] Under a collective dominance theory, more than one firm collectively making up a dominant share of the market can be challenged for conduct that otherwise serves as the basis for liability for an individually dominant firm. In this manner, it is closely comparable to a theory of harm based on 'tacit collusion' or

---

[18] 15 USC, ss 1, 2.

[19] *See*, 15 USC, s 2 (outlawing "*combin[ing] or conspire[ing]… to monopolize*". *See generally*, Joseph P Bauer et al, *Kintner's Federal Antitrust Law* (first published in 1980, Anderson Publishing Company 2013) 16-154 (the offense of conspiracy under s 2 is superfluous because the same facts will support a violation of s 1, which is an easier claim to prove).

[20] The Competition Act 2002, ss 3, 4. Most, if not all competition law systems around the globe follow a similar structural divide between agreements and single-firm dominance. *See,* for example, the Treaty on the Functioning of the European Union, arts 101, 102; the Anti-Monopoly Law of the People's Republic of China, arts 13, 17.

[21] In India, collective dominance is not recognised as a basis for liability under s 4 of the Competition Act. *See*, *Dish TV India Ltd v Hathway Cable and Datacom Ltd* 2014 SCC OnLine CCI 35.

'oligopoly conduct', which causes consternation in the US system but does not present a basis for a violation of the US antitrust laws.[22] Collective dominance theory erodes the distinction between concerted and unilateral conduct, but as a practical matter is uninteresting in the context of the sharing economy. The 'concert' in the sharing economy is so thickly populated that no theory of joint action, other than express collusion, might provide a basis for liability under any competition law system.

Thus, the unilateral conduct-concerted conduct divide is a worldwide phenomenon in applying competition principles to the sharing economy. Concert, if it exists, is a function of individual competitors reaching agreement through the sharing economy enterprise, using the technology platform as a meeting place for reaching an agreement on price, output, or other facet of competition. In an ordinary market, concert among thousands or millions of highly diffuse providers would be exceedingly unlikely. However, the ease of transactions made possible by a sharing economy works equally well in terms of coordinating a conspiracy among horizontal competitors.

Dominance, if it exists, should never be a function of a single supplier in a sharing economy market achieving dominant share. Instead, it should be a function of the sharing economy enterprise achieving dominance by locking up a substantial share of the matches between suppliers and consumers. Dominance is likely to be measured in terms of the number of matches between suppliers and consumers transacting on the particular technology platform. For example, in ride sharing, if in a particular month in a particular geographic location there are 1 million matches, the dominant firm might have 500,000, or whatever proportion the particular jurisdiction determines triggers status as a dominant firm under its laws.

B. Single Firm Analysis under the Competition Act

There is limited authority on single firm analysis under India's Competition Act. The Competition Act is more explicit than US law in its distinguishing of single entities from associations of enterprises for purposes of cartel claims. The Competition Act includes a definition of 'enterprise', and defines the concerted conduct prohibition as handling agreements involving "*an enterprise or association of enterprises*."[23] This formed the core of the defendants' argument in *National Insurance Co. Ltd.* v. *CCI*, ultimately

---

[22] *See*, Ioannis Kokkoris, 'The Development of the Concept of Collective Dominance in the ECMR' (2007) 30 World Competition 419, 420.

[23] The Competition Act 2002, ss 1, 3.

failing to convince the court that four competing insurers and their regulator could not be considered together as a single enterprise.[24]

One author analysed the development of the single enterprise doctrine under the competition law of India, dating to the Monopolies and Restrictive Trade Practices Act, 1969.[25] Jain details the progressive definition of 'enterprise' in a series of revisions to the competition laws, including the degree to which that definition encompasses government entities. Jain then explains, in depth, the 2017 *National Insurance Companies* decision. In Jain's interpretation, the court in *National Insurance Companies* noted the individual board management of the respective defendants and the lack of regulatory involvement in the management of the companies. The case thus reflects a determination that the enterprises and their regulator were not operating together as a single entity.

It is possible that the broad definition of enterprise in Section 1 of the Competition Act requires Indian courts to reach further than a court or regulator in the US would. An argument that a cartelist might be a single entity with its regulator would be frivolous under US law.[26] The broader definition of an enterprise in India could perhaps be traced to the nationalisation of insurance in 2002 (the same year the Competition Act took effect), which presented a unique single entity problem.[27] In spite of that nationalisation, the broad enterprise definition in the Competition Act – covering departments of government – reached the individual cartelists.[28] The court's analysis on the merits of the single entity question is entirely consistent with the US approach. Such a recognition of the lack of common purpose – what Anderson has called the sharing of profits and losses – both among the cartelists and between the cartelists and the regulator, is in keeping with the US approach to the single entity doctrine.[29]

Thus, while the law in India is not well developed, we see strong analogues between the single entity analysis in India and that in the US, where

---

[24] *National Insurance Co Ltd v Competition Commission of India* (2017) Comp LR 1, paras 5, 12 (*National Insurance Company*).

[25] Chirayu Jain, 'Single Economic Entity Doctrine in India' (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3184957> accessed 9 December 2019.

[26] Though an analogy might be made to a state action or regulatory immunity defense in US law. cf *Parker v Brown* 1943 SCC OnLine US SC 4 : 87 L Ed 315 : 317 US 341 (1943) (US Supreme Court holds that a state-mandated cartel is exempt from antitrust challenge); *Credit Suisse Securities (USA) LLC v Billing* 2007 SCC OnLine US SC 59 : 551 US 264 (2007) (securities laws preclude antitrust claims in case of 'clear repugnance').

[27] *National Insurance Company* (n 24) para 12.

[28] *National Insurance Company* (n 24) para 13 [citing s 2(h) of the Competition Act].

[29] cf Mark Anderson, 'The Enigma of the Single Entity' (2014) 16 University of Pennsylvania Journal of Business Law 497, 526-47 (explaining conflicting single entity decisions).

the law has been developed over many decades of experience with a variety of common ownership situations. The analysis in the following subpart describes the importance of the single entity question to deciding the application of competition law principles in ride sharing.

C. The Antitrust Firm in the Sharing Economy

Anderson and I discuss the sharing economy and its impact on theories regarding the antitrust firm in our 2017 article, 'The Sharing Economy Meets the Sherman Act: Is Uber a Firm, a Cartel, or Something in Between?'.[30] There, we identify the central tension in a legal theory built on transaction costs in extra-firm contracting: antitrust law favours intra-firm conduct because it is easy to coordinate and to manage efficiently, and that efficiency promises benefits to consumers.[31] Extra-firm contracting offers less central control and reduced efficiencies, so coordination is more likely to result in consumer harm.[32] In a modern platform industry, however, extra-firm contracts can be concluded as efficiently as can intra-firm contracts in traditional industry structures, with similarly substantial coordination of operations among contracting parties. The benefits flowing from intra-firm contracts are no longer unique.

Anderson and I go further than merely observing that extra-firm contracting may be as efficient as that occurring intra-firm. We contend that by reducing search and transaction costs, the sharing economy "*enable[s] transactions that could not occur in a pre-internet economy.*"[33] The central innovation in platform-based contracting is to eliminate the transaction costs that previously made one-off contracts impossible. The result is that nearly infinitely diffuse competitors – in the case of ride sharing, both drivers (competing for customers) and passengers (competing for rides) – are able to centralise their operations to achieve efficiencies of scale, while remaining competitors with regard to much of what they do.[34] These areas of remaining competition include "*matters such as where to operate, what parts of the day to offer services, and . . . when to service or replace the vehicles.*"[35]

Ride sharing drivers compete in other ways, both articulable and less so, including cleanliness, friendliness, diving ability, and provision of additional products or services (such as a bottle of water in the cup-holder). Passengers

---

[30] *See*, Anderson and Huffman (n 12).
[31] *See generally*, Anderson and Huffman (n 12) 888.
[32] Anderson and Huffman (n 12) 888-89.
[33] Anderson and Huffman (n 12) 882.
[34] Anderson and Huffman (n 12) 883-84.
[35] Anderson and Huffman (n 12) 884.

also compete, through whatever they can do to maximise their ratings to make drivers more inclined to respond to their summons. In theory, these ratings competitions should allow a nearly infinite number of facets of competition among drivers and passengers alike. It is even possible to imagine a form of price competition, based on tipping (by passengers) or discounting (by drivers). Practically speaking, however, objective facets of competition are greatly limited in service of the efficiency of commodification.

By reflecting both the central operational control of a single firm and the highly competitive nature of a market characterised by sole proprietorships, sharing economy firms, including ride sharing enterprises, are ambiguous in their competition policy implications. Anderson and I diagrammed the problem as shown in Figure 1.

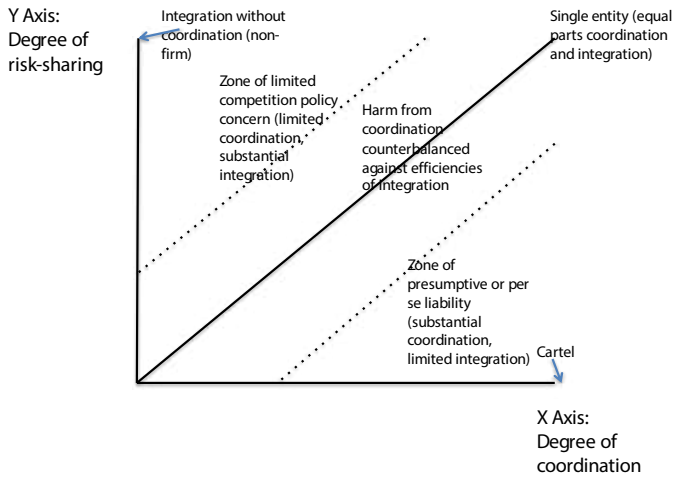

Figure 1

The figure demonstrates that efficiency increases as erstwhile competitors move upward along the Y-axis toward greater risk sharing, a concept detailed in the US Supreme Court's *Copperweld* decision as one driven by the sharing of profits and losses.[36] Under the current state of law in most jurisdictions, competition law recognises either a single entity or multiple

[36] *Copperweld Corp v Independence Tube Corp* 1984 SCC OnLine US SC 147 : 81 L Ed 2d 628 : 467 US 752 (1984), 768-72 (coordinated activity between parent company and

competitors, a binary categorisation that can mean the difference between liability or immunity.[37] Studying the sharing economy shows that risk sharing is instead a matter of degree, with integration sufficient to achieve single firm efficiencies only at the far reach (the high point on the Y-axis) and disintegration sufficient to prevent any efficiencies from being realised at the extreme low point on the Y-axis. Sharing economy enterprises are arrayed along the Y-axis according to their particular terms.

Anderson and I analysed the state of several leading enterprises at the time of our 2017 publication,[38] but with variations in terms of service, any such array is subject to substantial change. (For example, between the drafting and publication of our 2017 article, one important term of service – tipping – changed in the Uber enterprise, leading to a different bargaining dynamic).[39]

The X-axis on Figure 1 is well understood in all competition law systems, showing the degree of coordination among competitors. At the extreme (far right) point, coordination reflects a cartel agreement; at the far-left point, there is a lack of coordination reflective of full competition; and in the middle, there is coordination on less sensitive matters such as information sharing. Developed competition policy systems have long appreciated that this is a sliding scale of coordination,[40] although the binary per se/rule of reason distinction remains in both statutory enactments and common law interpretations.

Anderson's and my significant contribution to the analysis of the antitrust firm, based on our study of the sharing economy, was that each agreement should be analysed both in terms of its place on the X-axis and its place on the Y-axis, rather than deciding ab initio that a particular enterprise was either exempt from scrutiny for all cases (because a single firm) or was subject to scrutiny in all cases (because a multiplicity of competitors). The pricing term in a normal sharing economy enterprise, most notably the price per ride that all ride sharing drivers agree to charge, would be a price fix – but

wholly-owned subsidiary must be viewed as that of a single enterprise for the purpose of Sherman Act s 1 analysis; single enterprise incapable of conspiracy).

37 Anderson and Huffman (n 12) 917.

38 Anderson and Huffman (n 12) 927.

39 Anderson and Huffman (n 12) 874.

40 *See,* for example, *California Dental Association v Federal Trade Commission* 1999 SCC OnLine US SC 51 : 143 L Ed 2d 935 : 526 US 756 (1999) (no categorical line between restraints giving rise to intuitively obvious inference of anticompetitive effects; inquiry should look to restraints' circumstances, details and logic).

because of the sharing of risk among the erstwhile competitors under the Uber umbrella, it should be subject to rule of reason scrutiny.[41]

Due largely to the features Anderson and I analysed in 2017, the sharing economy grew strongly in developed economies, all of which were burdened with legacy permitting systems such as taxicab medallions or zoning regulations, and other oversight limiting public lodging. However, the promise in economies with substantial development ahead of them is much greater, also for the reasons we describe. Either, or both, of (1) a lack of historic permission for private enterprise, and (2) the failings of centralised economic direction, have left many economies without competitively attractive offerings in industries affected by the sharing economy. At the same time, these economies have substantial pent-up entrepreneurial supply waiting to be unleashed through activity that can arbitrage restrictions on entrepreneurship. Sharing economy enterprises can capitalise on this untapped supply with the technical improvements allowing the efficiency of integrated ownership, producing entire industries that may have been lacking.

III. Ride Sharing Markets – United States and India

Ride sharing has a venerable history around the globe as a non-market or grey-market alternative to taxis and car ownership. Examples include carpooling by commuters. 'Slugging' is a form of carpooling found in Washington DC (USA) that involves lines of commuters waiting at known pick-up locations for rides on the major highways either south or north of town, enabling drivers to take advantage of the High Occupancy Vehicle lanes and avoid congestion, with a history dating at least to the Arab oil embargo. The phrase 'gypsy cabs' refers to unlicensed (and therefore law violating) taxicabs in the US. According to sharing economy enterprise Wikipedia, other terms – 'black cabs' in China, 'white cards' in Hong Kong, 'taxi pirate' or 'pirrataxi' (Mexico, Scandinavia), among others – are in use around the world, demonstrating the worldwide ubiquity of the practice.[42] Ride sharing is also the best known example of a sharing economy enterprise, with Uber (US), Ola (India), Didi (China), Grab (Vietnam), and other app-based enterprises achieving massive scale in a short period of time.

---

[41] Anderson and Huffman (n 12) 927-29. Anderson and I concluded that the quick-look rule of reason was appropriate for Uber, although that conclusion is likely relaxed in light of permissive app-based tipping.

[42] 'Illegal Taxicab Operation' (*Wikipedia,* 2019) <https://en.wikipedia.org/wiki/Illegal_taxicab_operation> accessed 26 May 2019. When writing about the sharing economy, I am more willing than in ordinary scholarship to rely on Wikipedia, itself a sharing economy enterprise, for easily verifiable factual observations.

In economies with substantial room for growth, such as that in India, the sharing economy has particular promise. Early development of a robust transportation infrastructure is likely one of the strongest explanations for the success in US economic development in the 19th and 20th centuries. Ride sharing allows for that transportation infrastructure to grow in a grass roots manner in economies not yet so developed. In addition, infrastructure growth presents substantial danger for corruption when managed centrally, the threat of which is reduced when the growth happens at the grass roots level. In light of these observations, it should not be a surprise that the ride sharing industry in India is characterised by a large number of competitors and, by all appearances, substantial competitiveness.

A. Taxis and Ride Sharing – United States

The US ride sharing market has achieved substantial penetration into consumer transportation generally, with reports that 36% of people in the US had used a ride sharing app in 2018.[43] Survey results also show that 97% of US consumers have heard of ride sharing services.[44] Uber and Lyft are a functional oligopoly nationwide in matching services, with Uber at 64% share and Lyft at 33% share (approximate figures) of a market presumably based on rides taken.[45] Market share, as determined by the number of drivers on an app, is 87.6% for Uber and 75.1% for Lyft, reflecting substantial 'multi-homing' (whereby one driver offers services on more than one app). According to a news report summarising one survey, another metric, business travel receipts, shows a substantial but narrowing gap between Uber and Lyft, with Uber at 79% and Lyft at 21% of the share of business travel receipts (apparently in the US).[46]

On a worldwide basis, determined by the amount of investment in their enterprises prior to initial public offerings (in January 2019), Uber was first with $24 billion in investment, with Chinese firm Didi following closely with $21 billion, Southeast Asian firm Grab third with $7.1 billion, Lyft fourth with $5 billion, and Indian firm Ola Cabs fifth with $3.4 billion.[47]

---

[43] 'Ridesharing services in the US – Statistics & Facts' (*Statista*, 2019) 14 <https://www.statista.com/study/54807/ridesharing-services-in-the-us/> accessed 20 July 2019.

[44] (n 43) 19.

[45] (n 43) 11. Statista fails to explain the basis for its market share calculations.

[46] Wolf Richter, 'Uber and Lyft are gaining even more market share over taxis and rentals' (*Business Insider*, 30 July 2018) <https://www.businessinsider.com/uber-lyft-are-gaining-even-more-market-share-over-taxis-and-rentals-2018-7> accessed 9 December 2019.

[47] 'Lyft' (*Statista*, 2019) 7 <https://www.statista.com/study/58248/lyft/> accessed 9 December 2019.

In terms of global revenue, Lyft's – drawn from Canada and the US only – was $2.18 billion in 2018.[48] Lyft gave 551 million rides in North America in 2018.[49] Uber's worldwide revenue, drawn from North America as well as other continents (and thus not a good comparison to Lyft, in terms of relevant market share), was $11.3 billion in 2018.[50] Uber gave 5.3 billion worldwide rides in 2018.[51]

Local share of ride sharing enterprises in the US is more textured than the national or worldwide comparisons disclose. In terms of consumer spend (on an average per-person basis), San Francisco is the largest local ride-sharing market in the US, followed by Boston, New York, Washington D.C., and Philadelphia.[52] In these five largest markets, the closest competition is in San Francisco, with Lyft customers averaging $89 monthly spend and Uber customers averaging $110 monthly spend. In every case, the monthly average spend on Uber exceeds Lyft, with the greatest distinction – $95 versus $55 – in Boston.[53]

Relative to traditional taxis, ride sharing has made substantial inroads. One news source, drawing data from a provider of business travel expense management services, notes an increase from the first quarter of 2014 to the second quarter of 2018 in the share of business travel ground transportation receipts from 8% (2014) to 70.5% (2018).[54] This 70.5% statistic leaves the remainder of the market divided among rental cars and traditional taxis, whose share decreased over the same period from 55% to 22% (rental cars) and 37% to 5% (taxis).[55]

Ride sharing is not yet profitable for the leading US enterprises, at least in terms of traditional accounting metrics of profit. According to the Lyft registration statement for its 2019 Initial Public Offering, "*We have incurred net losses each year since our inception and we may not be able to achieve or maintain profitability in the future. We incurred net losses of $682.8*

---

48 (n 47) 12, 37.

49 (n 47) 13.

50 'Uber Technologies' (*Statista*, 2019) 13 <https://www.statista.com/study/54895/uber-technologies/> accessed 9 December 2019.

51 (n 50) 16.

52 (n 50) 10. Based on an average of transactions from 50,000 users in each locality, this is an imperfect statistic for purposes of determining market share, which might be better analysed in terms of total spend or total rides in a particular locality.

53 (n 50) 10.

54 Michael Goldstein, 'Dislocation and its Discontents: Ride Sharing's Impact on the Taxi Industry' (*Forbes*, 8 June 2018) <https://www.forbes.com/sites/michaelgoldstein/2018/06/08/uber-lyft-taxi-drivers/#4b601fec59f0> accessed 9 December 2019 (summarising a study by business travel software firm Certify); Richter (n 46).

55 ibid.

million, $688.3 million and $911.3 million in 2016, 2017 and 2018, respectively."[56] Uber, likewise, disclosed, "*We have incurred significant losses since inception, including in the United States and other major markets. We expect our operating expenses to increase significantly in the foreseeable future, and we may not achieve profitability.*"[57] Despite that, recent news reports suggest stock price increases for both companies based on earnings by Uber meeting expectations.[58] There is also the question of whether the data being gathered on riders, which cannot be meaningfully represented in accounting metrics, might nonetheless represent value that in hindsight will demonstrate profitability even today.

In the US, ride sharing represents a substantial share on a per-user basis of the overall sharing economy use. In 2018, 66 million adults in the US used a sharing economy service. 16 million used sharing economy lodging services. 18 million used ride sharing.[59] Another prominent sharing economy use model, coworking spaces, had much less penetration in 2018, with less than a million individual users.[60]

B. Taxis and Ride Sharing – India

In the 2016 'Report of the Committee Constituted to Propose Taxi Policy Guideline to Promote Urban Mobility', the Indian Ministry of Road Transport and Highways took an express position favouring a permissive regulatory scheme to liberalise the shared mobility industry.[61] The Report reflects a response to the perceived failure of public transport infrastructure to stem private car ownership and use and attendant congestion and pollution.[62] It seeks to establish a national policy limiting regulatory impediments to the growth of cab aggregators, while expressly permitting regulation

---

[56] *See*, 'Form S-1 Registration Statement – Lyft, Inc' (1 March 2019) 21 <https://www.sec.gov/Archives/edgar/data/1759509/000119312519059849/d633517ds1.htm> accessed 9 December 2019.

[57] *See*, 'Form S-1 Registration Statement – Uber Technologies, Inc' (11 April 2019) 12 <https://www.sec.gov/Archives/edgar/data/1543151/000119312519103850/d647752ds1.htm> accessed 9 December 2019.

[58] Ryan Browne, 'Traders are finally realizing the value of companies like Uber and Lyft, Russian rival says' (*CNBC,* 6 June 2019) <https://www.cnbc.com/2019/06/06/market-realizing-value-of-ride-share-firms-like-uber-lyft-yandex-cfo.html> accessed 9 December 2019.

[59] 'Sharing Services in the US' (*Statista,* 2019) 6-8 <https://www-statista-com.proxy.ulib.uits.iu.edu/study/56029/sharing-services-in-the-us/> accessed 9 December 2019.

[60] ibid 28.

[61] Ministry of Road Transport and Highways, *Report of the Committee Constituted to Propose Taxi Policy Guideline to Promote Urban Mobility* (2016) <https://smartnet.niua.org/sites/default/files/resources/Taxi%20Policy%20Guidelines.pdf> accessed 9 December 2019.

[62] Ministry of Road Transport and Highways (n 61) 8.

designed to ensure safety, consumer protection, and fair terms of service (including pricing).[63]

At the same time, by defining ride sharing enterprises as part of the taxi market, India sought to close the regulatory gap the enterprises sought to exploit – not being treated as taxi services because their sole literal service was providing a transaction platform.[64]

i. Many firms

The Indian taxi market stood at around $6.4 billion in 2016, and is forecast to grow at a compound annual rate of 13.7% during 2017-2022, to reach $14.3 billion. Surging demand for taxi services in India can be attributed to changing lifestyles of travellers and increasing disposable income of consumers, especially in Tier-I and Tier-II cities. The market is witnessing increasing traction as taxis offer hassle free travel experience to customers in addition to various other tangible and intangible offerings such as booking convenience through mobile applications, air conditioning, educated and skilled drivers, multiple payment options, 24×7 customer support, electronic fare meters, GPS-enabled vehicles, etc.[65]

Uber Technologies Inc. and Ola (ANI technologies Pvt. Ltd.) are spending heavily to expand pooled rides, a category considered the next big growth driver for both cab hailing firms. Pooled rides account for 25-30% of overall trips on Ola and Uber in key cities such as Mumbai, Delhi and Bengaluru.[66] Both firms have either dropped fares or are running promotions for ride sharing to attract new customers. For instance, Uber has capped carpooling fares at ₹49 for the first 8 km in Delhi, Bengaluru and Chennai. Ola is offering Share Pass, a subscription-based service launched in November 2018 that provides carpooling at a flat fare, and at a steep discount. Ola is also offering a Share Pass for five trips at ₹1. Usually, the firm offers a five-ride pass for ₹149, while the ones for 20 and 40 rides costs ₹249 and ₹349 per month, respectively, for the first 8 km. Ola recently reported that more than 20

---

63 Ministry of Road Transport and Highways (n 61) 5-7.

64 OECD Report (n 5) 2-3.

65 'India Taxi Market By User Segment (Individuals, Corporate & Tourist), By Payment Mode (Cash, Online Payment & Mobile Wallets), By Vehicle Type (Premium/Luxury, SUV/MPV, Hatchback & Sedan), By Taxi Type (Radio, Regular, Self-Driving), Competition Forecast & Opportunities, 2012 – 2022' (*TechSci Research,* October 2017) <https://www.techsciresearch.com/report/india-taxi-market/1450.html> accessed 9 December 2019.

66 *See,* for example, Manish Singh, 'Uber Reaches 500 Million Rides in India, Reveals Interesting Statistics' (*Gadgets 360*, 3 August 2017) <https://gadgets.ndtv.com/apps/news/uber-india-500-million-rides-uberpool-driver-rider-statistics-1733047> accessed 9 December 2019.

million carpool rides had been pre-sold through its Share Pass subscription offering.[67]

India's growing transportation industry has even attracted foreign players such as Tripda, which launched in India in 2014. "*We are focused on long distance carpooling and inter-city rides and hope that India will be among our top three markets apart from Brazil and USA in less than a year*" said Nitish Bhushan, country manager of Tripda in India. The company had planned to expand to Mumbai next in order to sign on commuters on the Mumbai-Pune highway,[68] but saw its operations shut down in 2015.

BlaBlaCar is mostly preferred for long-distance inter-city travel while Ola/Uber are preferred for shorter distances. In general,

> With BlaBlaCar, the car owners have the opportunity to share their long-distance ride with passengers traveling on the same route. Owners do this by specifying the itinerary and price for the ride. Interested co-travellers can coordinate with the car owner through a private messaging system of BlaBlaCar or over the phone. The co-travellers then pay their contribution to the owners directly.[69]

ii. Ola and Uber

According to fact-finding by the Director General for Competition, Ola is the largest provider of app-based ride sharing in India. Ola is a domestic firm with operations dating to 2010.[70] It describes itself as a taxi aggregator and not a taxi company. In this way, it follows the business model of Uber.[71] Uber is second in market presence to Ola, having begun operations in India in 2013.[72] Although the business model differs from 'radio taxis',

---

[67] Sayan Chakraborty, 'For Ola and Uber, India's shared taxi market is the next battleground' (*Livemint*, 6 June 2017) <https://www.livemint.com/Companies/zurwJmatKucNvacjRmwxLK/Shared-rides-the-next-battleground-for-Ola-Uber.html> accessed 9 December 2019.

[68] Payal Ganguly and Aditi Shrivastava, 'Startups offering ride-shares set to gain as taxi aggregators face roadblocks across states' *Economic Times* (Mumbai, 16 December 2014) <https://economictimes.indiatimes.com/small-biz/startups/startups-offering-ride-shares-set-to-gain-as-taxi-aggregators-face-roadblocks-across-states/articleshow/45531225.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst> accessed 9 December 2019.

[69] Archna Oberoi, 'How BlaBlaCar works: Business Model and Revenue Streams' (*Daffodil*, 13 March 2019) <https://insights.daffodilsw.com/blog/how-blablacar-works-business-model-and-revenue-streams> accessed 9 December 2019.

[70] OECD Report (n 5) 2.

[71] *Fast Track Call Cab (P) Ltd v ANI Technologies (P) Ltd* 2017 SCC OnLine CCI 36, paras 7-12.

[72] OECD Report (n 5) 2.

which own their cars rather than operate platforms where drivers and riders interact, the Director General concluded the Ola was a substitute for radio taxis. However, despite greater than 60% market share, Ola was not a dominant player due to substantial competition from Uber and an eroding market share.[73]

Ola and Uber each provide substantial competitive constraint on the other's possible dominance. Evaluating allegations of abuse of dominance by Ola, the CCI held that market share is an inadequate measure of competitive position in the market for cab aggregators.[74] Fierce competition by Uber and a lack of switching costs, including the presence of multi-homing (consumers using brands interchangeably), rendered Ola's substantial share in the particular city in question unconvincing. According to the CCI's OECD report, there are cases involving group ownership arguments through which Ola's and Uber's shares might be aggregated for the purpose of determining dominance.[75]

Because the existing investigations and litigation in India regarding ride sharing turn on questions of dominance, the Anderson-Huffman analysis of the sliding scale of integration, and its interplay with the degree of coordination, is not readily applied.

IV. Antitrust for a World of Self Employment

Ride sharing is the most prominent application of sharing economy technologies and enterprise structures, but the world of self-employment is not limited to ride sharing. Instead, the possibility of low-to-zero transaction cost contracting raises the possibility of revolutionising nearly any services market. As I describe above, these markets will be populated by a functional infinity of suppliers and of consumers, each lacking any bargaining power vis-à-vis each other. This leaves three areas of likely concern for antitrust inquiry: (1) conspiracy among individual suppliers, either en masse through the sharing economy enterprise as intermediary or in isolated localised sub-markets; (2) abuse of dominance by the enterprise itself, harming either competitors (and thus competition) or consumers or suppliers on either side of the platform; and (3) mergers or consolidations involving enterprises.

---

[73] OECD Report (n 5) paras 9, 12-13, 22-23.
[74] OECD Report (n 5) 6.
[75] OECD Report (n 5) 7.

A. Market Definition

The first step in any antitrust analysis of sharing economy enterprises will be that of market definition. The enterprise, as that concept is used here and in prior scholarship, is comprised of a functionally infinite number of suppliers, a matching service (platform) and a seeming infinity of transactions among suppliers and consumers. Courts and commentators have struggled with whether the market is best understood to be: (1) the service in which the enterprise operates (e.g., ride sharing enterprises in the taxi market); (2) a narrower market specific to the sharing economy nature of the enterprise (e.g., a market for app-based ride sharing); or (3) a market for matching suppliers with consumers. If the definition is the third, there are at least two markets in sharing economy enterprises – the market for matching and the market for supplying rides. Which market is used will influence the subsequent analysis of antitrust theories.

The correct answer, for most antitrust analyses, is to treat the enterprise as straddling two markets – one for matching and one for services. The matching market is populated by sharing economy platforms, and in most jurisdictions, is likely to be oligopolistic or monopolistic. The matching market has natural monopoly characteristics, with high up-front costs (developing the app, developing an installed user base) and lower marginal costs (selling the app after achieving market penetration).[76] Further, the matching market boasts both direct and indirect network effects, whereby increased use of an app heightens its value to all users, making it more likely that a new user will opt for the existing app rather than a new entrant.[77] The matching market is also the market in which entry barriers are greatest, because of the need to enter at scale to compete against substantial positive network externalities enjoyed by existing firms.[78]

The services market will be populated by sharing economy enterprises as well as old-economy firms and in some cases, even individual entrepreneurs.

---

[76] *See generally*, N Gregory Mankiw, *Principles of Microeconomics* (6th edn, Southwestern 2012) 302 (natural monopoly where the high up-front costs are continually diluted by increased use).

[77] *See*, Jean-Charles Rochet and Jean Tirole, 'Two-Sided Markets: An Overview' (2004) Institut d'Economie Industrielle Working Paper <http://web.mit.edu/14.271/www/rochet_tirole.pdf> accessed 9 December 2019; Carl Shapiro and Hal Varian, *Information Rules: A Strategic Guide to the Network Economy* (1st edn, HBS Press 1999) 173-226 (discussing the phenomenon of network effects and their importance as entry barriers); David Evans and Richard Schmalensee, *Matchmakers: The New Economics of Multisided Platforms* (1st edn, HBR Press 2016) 21, 22, 25 (defining direct and indirect network effects and the resulting 'first mover advantage').

[78] Evans & Schmalensee (n 77).

Thus, a sharing economy enterprise in a ride sharing market competes with taxis, while a sharing economy enterprise in a lodging market competes with hotels. How to understand the services market is a more complicated question, depending on whether the enterprise is treated as a single entity or as a contract relationship among atomistic suppliers and the platform.

India defines app-based ride sharing enterprises as 'cab aggregators', a regulatory classification that encompasses Uber, Ola, and like enterprises. A cab aggregator is "*a digital intermediary or market place for a passenger to connect with a driver for the purpose of transportation*."[79] This reflects an approach that highlights the role of the platform, rather than the enterprise in its entirety, in the market definition process. There is not a comparable announcement on a nationwide basis of how markets will be defined in the US, likely because of the lack of public investigation of sharing economy industries and the failure of private litigation to reach the highest-level court. For example, in its 2016 report on the sharing economy, the US Federal Trade Commission did not make an effort to define possible antitrust markets.[80]

B. Dominance

From the perspective of competition policy, most of the interest worldwide in sharing economy markets has been in the area of abuse of dominance, with Ola or Uber the target of a private or public enforcement action. Dominance as a theory might be argued in either a market for matching (the service provided by the platform) or a market for the service provided by the enterprise (e.g., taxi services). Under the latter market definition, courts in the US have correctly been reluctant to find dominance, based on the ease of entry into ride sharing and insufficient evidence of dominant market share.[81]

Dominance is an odd theory of harm in the sharing economy space for a host of reasons. These include: (1) small firms (relative to old economy analogies); (2) ease of switching; (3) seeming ease of entry; and (4) localised markets.

---

[79] (n 9).

[80] *See generally*, FTC Report (n 3).

[81] *See*, for example, *Philadelphia Taxi Association v Uber Technologies* 886 F 3d 332 (2018), 341-42 (3d Cir) (no "*dangerous probability of achieving monopoly power*" in the presence of low entry barriers and no allegations of market share); *DeSoto Cab Co v Uber Technologies Inc* 2018 US Dist LEXIS 226261, 20-27 (ND Cal) (dismissing monopolisation claims under US law on the basis of a lack of barriers to entry and a lack of a dangerous probability of recouping losses incurred through monopolisation).

i. Small firms

Initially, the firms serving as platforms in sharing economy enterprises may not themselves be impressively large, relative to old-economy counterparts. The service providers are not treated as employees except in jurisdictions where an employment relationship is decreed by law. The platform does not own the vehicles, or other capital assets used to provide services – a fact that may be changing as firms like Uber experiment with self-driving vehicles. Uber's market valuation immediately after its initial public offering was $75 billion, a substantial sum but less impressive for a competitor to taxis in 65 countries and 600 cities worldwide.[82] In the absence of large size, a ride sharing platform's competitive advantage relies largely on technological advantage, including the quality of the software deployed and the use of data to enhance transaction efficiency.

ii. Switching

Switching between sharing economy enterprises is relatively simple for both consumers and suppliers. This is because signing up for an app requires single digit minutes and involves merely entering basic personal information and payment details. Evidence suggests that both consumers and suppliers 'multi-home', using more than one platform either to provide or to consume services. Multi-homing and other factors ensuring ease of switching are regularly cited as evidence that sharing economy enterprises lack market power sufficient to give rise to theories of abuse of dominance.[83] In the absence of a lock-in effect from joining an app, of the sort that consumers experience in signing up for a particular technological standard (whether operating system, music streaming format, or the like), it is difficult to state a theory under which even substantial market share is likely to lead to a price or quality effect.

iii. Easy entry

Entry has been assumed to be easy in app-based markets because: (1) existing world-beating firms owe their start to small cadres of thinly-capitalised entrepreneurs; (2) the existing technology industry is populated by extremely high-valued firms, such as Google, Amazon, Apple, and Microsoft, each flirting with $1 trillion in market capitalisation, who can enter or fund entry on a

---

[82] Mansoor Iqbal, 'Uber Revenue and Usage Statistics (2019)' (*Business of Apps*, 10 May 2019) <http://www.businessofapps.com/data/uber-statistics/> (accessed 9 December 2019).

[83] Yaraghi and Ravi (n 1) 19 (differentiating sharing economy enterprises from social networks because of the lack of lock-in effects).

whim; and (3) private venture capital is available to fund promising start-up enterprises. A 2017 analysis of the sharing economy in India supports the ease of entry hypothesis, noting "*new start-ups being registered every week which offer new products and services using digital platforms*."[84]

A counterpart to the ease of entry story is the combination of network effects and the treasure trove of data held by first movers. These factors are frequently cited as evidence that start-ups will not be able to penetrate existing markets. There is reason to believe these facts are not as important as they might seem. Data for sharing economy markets can be expected to have localised value. Thus, data from US consumers is unlikely to be valuable when marketing to consumers in India (and vice versa). Even within a country, at least one as large and economically and culturally diverse as India or the US, data from one local market may not be meaningful in a different local market. As possible proof of this claim, Uber's success has largely been in western markets, with regional competitors Ola (India), Yanex (Russia), Didi (China), and Grab (Vietnam) out-competing, and in three of those examples, actually eliminating the competitive threat from Uber.

iv. Localised markets

Much of the story regarding dominance in the sharing economy relates to the sheer worldwide or nationwide scope of the leading firms.[85] Another approach suggests that dominance may be best viewed as a function of local rather than worldwide markets. Ride sharing enterprises have characteristics of both: (1) nationwide or worldwide, and (2) localised, markets.[86] In support of the broader geographic market definition, consumers might be expected to choose among competing sharing economy enterprises based in part on geographic reach, including worldwide brand penetration – making sheer scale a competitive feature. In support of the narrower market definition, consumers can, and do, 'multi-home', selecting among competitors at a local level. For example, a world traveller might have an Uber app, a Didi app, a Grab app, and an Ola app, all on the same smartphone, and select the one best suited to the particular geography on a given day. Which effect – preference for broad reach or preference for local options – outweighs which is ambiguous. This undermines an argument that worldwide scale equates to dominance in any one locality.

---

[84] Yaraghi and Ravi (n 1) 5.

[85] For example, Hubert Horan, 'Will the Growth of Uber Increase Economic Welfare?' (2017) 44 Transportation Law Journal 33, 64-69.

[86] *See*, Francesco Russo and Maria Luisa Stasi, 'Defining the Relevant Market in the Sharing Economy' (2016) 5 Internet Policy Review 8-9 <https://policyreview.info/node/418/pdf> accessed 9 December 2019.

Features of sharing economy enterprises that serve to limit entry, including the scalability of data resources, are muted in the case of localised markets. This is because individual consumers are (primarily) local, so data regarding riders in one city necessarily excludes the conduct of riders in a different city. It is also because cultural, ethnic, religious, economic, or other differences between cities, states, or nations, render algorithms that facilitate competition in one place less valuable in another. As an example, an algorithm might predict the importance of having cars available at the airport, based on travel habits of the population on which the algorithm is based. If the population of another city has different travel habits, the algorithm will be of limited use. For that reason, sheer worldwide scale is of limited importance when competition is localised. This conclusion is bolstered by the reality of limits on the success of globally dominant players in specific geographic locales.[87]

C. Agreement/Conspiracy

Conspiracy is and will remain an area of substantial concern in the context of the sharing economy, which at its core, reflects interconnected markets populated by a large number of individual participants. Anderson and I made this the central thrust of our 2017 article,[88] where we argued for a 'quick look rule of reason' approach to analysing the hub-and-spoke agreements among providers on a sharing economy enterprise. Those agreements, covering price, output, quality, choice, and innovation, strike at the heart of competitive concerns, but they also make possible a unique level of integration that approaches that of a single firm.

The question remains how to treat a theory of harm based on agreement, including: (1) whether the hub-and-spoke conspiracy approach will be followed; (2) what is the approach in a jurisdiction without a middle ground 'quick look' approach like that in the US; (3) what arguments might exist that undermine the necessity of coordination to achieve the integrative efficiencies? Another question relates to suppliers on a sharing economy enterprise, such as drivers in the case of ride sharing, seeking to organise as de facto employees, including whether such organisation itself presents a cartel problem.

i. Hub-and-spoke conspiracy

Hub-and-spoke conspiracy exists where horizontal competitors reach explicit or implicit agreement through an intermediary, perhaps without ever

[87] *See*, subpart B.iii, above.
[88] *See*, Anderson and Huffman (n 12)

communicating among themselves. Examples outside of the sharing economy include the *Apple e-Books* case in the US, where Apple was found to have served as the hub, orchestrating an e-Book pricing conspiracy among e-Book publishers.[89] The legal consequence, liability per se under Section 1 of the Sherman Act, was upheld on appeal.[90]

According to its UNCTAD Submission, the CCI has also considered the possibility of a hub-and-spoke conspiracy in the context of a platform enterprise. Noting two examples of possible hub-and-spoke relationship cartels that were instead investigated as vertical agreements, the CCI summarised its view as follows: "*The CCI is however, aware that even if firms that are distributors do not directly communicate with each other, the fact that they use the supplier as an intermediary or backchannel medium to communicate should not exculpate them from any liability.*"[91]

The CCI's summary reflects a correct understanding of the hub-and-spoke possibility in the sharing economy. However, when applied in the context of ride sharing, the CCI abandoned the hub-and-spoke concept in the absence of proof of communication between suppliers in a sharing economy enterprise. The CCI's UNCTAD Submission described its investigation into the centrally established prices in the Uber enterprise.[92] Quoting the CCI's dismissal of the hub-and-spoke argument, the UNCTAD Submission concludes that Uber drivers' "*acced[ing] to the algorithmically determined prices by the platform (Ola/Uber) . . . cannot be said to be amounting to collusion between the drivers.*"[93] The CCI would require an "*agreement between drivers inter-se to delegate this pricing power*", a stronger showing than is required under US law – and a stronger showing than the UNCTAD Submission itself suggests the CCI would require.[94]

The CCI's approach in *Agrawal* v. *ANI Techs./Uber* may violate basic common law rules regarding what constitutes an agreement among

---

[89] *United States v Apple Inc* 952 F Supp 2d 638 (2013), 647 (SDNY) (agreement between Apple and publishers was at the root of a horizontal price restraint and thus warranted per se treatment; vertical actors need not be the dominant purchaser or supplier to be a traditional 'hub' in a hub-and-spoke conspiracy).

[90] *United States v Apple Inc* 791 F 3d 290 (2014), 298 (2d Cir) (affirming the district court's use of per se treatment as appropriate where, (1) relevant restraint of trade was price fixing, not vertical agreement, (2) coordination was not necessary for the creation of retail e-book market, and (3) prices were set by collusion and not competition) (*Apple Inc*).

[91] UNCTAD Submission (n 10) 3.

[92] UNCTAD Submission (n 10) 3-4 [discussing *Samir Agrawal v ANI Technologies (P) Ltd* 2018 SCC OnLine CCI 86].

[93] UNCTAD Submission (n 10) 4 [quoting *Samir Agrawal v ANI Technologies (P) Ltd* 2018 SCC OnLine CCI 86].

[94] *See*, *Apple Inc* (n 90) 298; UNCTAD Submission (n 10) 3.

competitors, but it likely leads to a result that is consistent with optimal outcomes. I observe below that the Competition Act does not have an obvious analogue to the abbreviated rule of reason analysis Anderson and I argued for in 2017. In its lack, another mechanism is required to preserve the possibility of platform-based ride sharing without exempting entire industries from competition scrutiny. In *Agrawal*, the CCI recognised the ability of drivers to reach agreement on basic terms of service, including algorithmic price terms, without violating competition laws.

ii. Analysis in the absence of 'quick look'

The quick look rule of reason serves as a middle ground between automatic illegality, or per se treatment, and the full rule of reason analysis that proves overly burdensome for most plaintiffs, whether public or private enforcers.[95] It is a procedural tool that permits effective prosecutions of facially harmful conduct while retaining in defendants the ability to defend against claims with evidence of pro-competitive benefits. The US approach to a middle ground might be described as a non-standard, "*an enquiry meet for the case*."[96] Professor Cavanaugh describes the 'quick look' as "*tailor-made for restraints that bear a close family resemblance to price fixing, but are of the type with which courts have little experience or are idiosyncratic in nature*."[97]

Not every jurisdiction has such a procedural mechanism. In the EU, for example, Article 101 of the Treaty on the Functioning of the European Union ('**the TFEU**') distinguishes between automatically illegal conduct[98] and conduct exempt from automatic illegality, "*which contributes to improving the production or distribution of goods or to promoting technical or economic progress*."[99] There is no explicit middle ground, although debates exist as to whether a 'continuum' approach that approximates the US system's quick look analysis is emerging in application.[100]

---

[95] *California Dental Association v Federal Trade Commission* 1999 SCC OnLine US SC 51 : 143 L Ed 2d 935 : 526 US 756 (1999).

[96] ibid 781 (describing the quick look rule of reason as "*an enquiry meet for the case*").

[97] Edward Cavanaugh, 'Whatever Happened to Quick Look?' (2017) 24 University of Miami Business Law Review 39, 40.

[98] Treaty on the Functioning of the European Union, art 101(1).

[99] Treaty on the Functioning of the European Union, art 101(3); *See generally*, European Commission, *Guidelines on the application of Article 81(3) of the Treaty* (2004/C 101/08) [describing the analytical process for the Article 101(3) inquiry].

[100] Alexander Italianer, 'Competitor Agreements under EU Competition Law' (40th Annual Conference on International Antitrust Law and Policy, New York, 26 September 2013) 6 <https://ec.europa.eu/competition/speeches/text/sp2013_07_en.pdf> accessed 9 December 2019.

The Competition Act is closer in form to US antitrust law than to the TFEU. It prohibits agreements that "*cause[] or [are] likely to cause an appreciable adverse effect on competition within India*."[101] The Competition Act then exempts from that prohibition "*any agreement entered into by way of joint ventures if such agreement increases efficiency in production, supply, distribution, storage, acquisition or control of goods or provision of services*."[102] One author, however, argues that the delineation in India is explicit; for agreements not treated as illegal per se, liability requires "*conclusive [proof] on fact that they cause or are likely to cause an appreciable adverse effect on competition*."[103]

In the absence of a quick look approach, a tribunal evaluating ride-sharing agreements must make a determination of whether to treat the agreement on prices and other competitive terms under a per se rule or under a rule of reason – unless the agreement is not a matter of concern because it is considered to take place within the contours of a firm. Research does not uncover cases alleging conspiracy in any jurisdiction that have proceeded to the merits of the claim.[104] The CCI's approach of declining to treat the Uber drivers' vertical agreements with the platform as representing a horizontal conspiracy is a sort of middle ground, producing an outcome not terribly unlike one a quick look analysis might produce.

iii. Ride sharing without coordination

The crux of an argument sceptical of competition law intervention in ride sharing, in the face of the substantial concerns for anticompetitive coordination when individual providers reach agreement through the platform on terms of service including quality and price, is the benefit of ride sharing and the belief that coordination is essential to the functioning of a ride sharing market. It is that sort of argument that underlay Anderson's and my advocacy for a quick-look rule of reason. A response is that even in light of the gains from ride sharing, there may be substantially less restrictive ways to accomplish those gains.

---

[101] The Competition Act 2002, s 3(1).

[102] The Competition Act 2002, s 3.

[103] Shruthi Anand, 'Revisiting Per Se vs Rule of Reason in Light of the Intel Conditional Rebate Case' (*The Centre for Internet and Society,* 4 October 2017) <https://cis-india.org/internet-governance/blog/revisiting-per-se-vs-rule-of-reason-in-light-of-the-intel-conditional-rebate-case> accessed 9 December 2019.

[104] One such allegation, in *Meyer v Uber Technologies Inc*, initially appeared ready to proceed to merits when the trial court held that the arbitration clause in the rider agreement was not enforceable. On appeal, the trial court decision was reversed, and the case was dismissed in favour of arbitration. 868 F 3d 66 (2017), 70, 80 (US Court of Appeals holding that the arbitration clause was enforceable).

Arguments exist that the degree of coordination present in an Uber-style ride sharing app is unnecessary to achieve the objectives of integration.[105] Uber's price and quality coordination, including everything up to rules regarding the kind and condition of the automobile and the driver's fitness for duty as well as the obvious price term, ensures that a passenger need not engage in the challenging process of searching for or of negotiating an individualised transaction. Fundamentally, Uber's coordination solves the three problems presented by anonymity – search costs, transaction costs, and trust. Of those, a ride-sharing economy enterprise would fail if it did not overcome the trust barrier – and if it did not fail, credible arguments would exist for regulatory intervention in any event. Search and transaction costs speak instead to the speed and ease of arranging a transaction. It is possible those parameters can be relaxed without undermining the enterprise in its entirety.

In fact, all cartel agreements serve the basic goals of reducing search and transaction costs. For example, an agreement to divide markets ensures consumers have access to only one supplier; an agreement to fix prices or quality ensures consumers need not devote time and energy to comparison shopping.[106] Competition necessarily increases costs of transacting in favour of improved transaction terms brought about by the competitive environment. The possibility that efficiency of search and transaction may overcome competitively determined transaction terms would upend core principles of economic policy based on competitive markets.

One could argue that a ride sharing enterprise should limit its ambitions to: (1) matching and (2) resolving the trust problem, but ignore the fixing of transaction terms. This would be an Uber-style app that would match rider with driver and offer a simple means to negotiate terms – necessarily slowing the process but ensuring competition on terms of service. A version of this argument would limit the area for competition to price, on a theory of consumer incapacity to evaluate quality, including safety, on an expedited basis. Such a ride-sharing enterprise would offer to consumers a menu of options including driver ratings and offer prices, letting the consumer select quickly the combination of rating and price that best matched his or her needs. Drivers, in turn, would bid on rides, presumably by setting a maximum discount rate from a baseline figure. It is ambiguous whether this reduction in

---

[105] Anderson and Huffman (n 12).

[106] Robert Lande, 'Should Predatory Pricing Rules Immunize Exclusionary Discounts?' (2006) Utah Law Review 863, 866; cf Daniel Crane, 'Rules versus Standards in Antitrust Adjudication' (2007) 64 Washington and Lee Law Review 49, 85-86 (observing that antitrust conduct is beneficial until it tips into harmful behaviour).

coordination would bring with it the expense of the high, and efficient, level of integration ride sharing enterprises offer.

In fact, at least one enterprise, founded in Russia, follows this model. inDriver offers what it bills as a "*fully transparent model*" in which riders bid for a route and negotiation occurs before other terms of service are disclosed.[107] As of this writing, inDriver boasts substantial growth, with 24,000 users in more than 200 cities and 300 million rides completed.[108] News reports indicate that in Driver manages the complexity of real-time negotiation by app by allowing negotiation above an offered fare in 10% increments.[109] Passengers can also choose among competing bids while considering quality indicia including ratings, arrival time, and vehicle information.[110]

iv. Agreement through labour organisation

The coordination concerns discussed in this subpart relate to the phenomenon of a hub-and-spoke conspiracy, arranged by the platform, targeting consumers as the victim. There are other ways to identify conspiracies involving the suppliers on a sharing economy platform, both targeting consumers and targeting the platform. Receptivity to such claims will differ depending on a particular jurisdiction's tolerance of labour interests as a justification for restraints on competition.

a. Labour conspiracy, consumer as victim

The most overt, and almost certainly universally illegal form of supplier conspiracy against consumers in the context of a sharing economy enterprise is a horizontal, off-platform agreement among suppliers to influence the terms of service. If such an agreement is orchestrated through the platform, it implicates the complex interaction between competitive harm and efficiencies discussed above. Where such an agreement is off-platform, it has characteristics of a pure supplier cartel and should be treated as such.

---

[107] Sasha Lekach, 'Russian ride-hailing app comes to America with set-your-own-price scheme' (*Mashable*, 4 December 2018) <https://mashable.com/article/indriver-set-your-price-ride-hailing-apps/> accessed 9 December 2019.

[108] 'About us' (*inDriver*, 2019) <https://indriver.com/en/about_us/> accessed 9 December 2019.

[109] Julie Walmsley, 'Priceline Meets Uber In A Name-Your-Fare Ride Service Arriving In New York' (*Forbes*, 4 December 2018) <https://www.forbes.com/sites/juliewalmsley/2018/12/04/priceline-meets-uber-in-a-name-your-fare-ride-service-arriving-in-new-york/#8fc727068c9f> accessed 9 December 2019.

[110] 'Ride-Hailing Service inDriver Enters US Market with New York City Launch' (*PR Newswire*, 4 December 2018) <https://www.prnewswire.com/news-releases/ride-hailing-service-indriver-enters-us-market-with-new-york-city-launch-300759288.html> accessed 9 December 2019.

As an example, recent news reports from the US market suggest that drivers on platforms including Uber may be agreeing to manipulate the surge pricing algorithm, collectively turning off their apps to reduce the number of drivers in a particular locality to induce surge pricing, before turning the apps back on to take advantage of the price increase.[111] Instances of such conduct have been observed nationwide in the US, but appear to be more concentrated in locations where drivers gather – for example, in ride share lots on airport grounds.

This agreement, if provable, is a hard-core cartel seeking to manipulate prices on the basis of a known algorithm for price setting. It is comparable to the rate-fixing cartel carried out in the context of the LIBOR, whereby cartel members manipulated the rate through a concerted practice of false rate reporting.[112] Fair unanimity in treatment of cartel conduct among jurisdictions suggests this result will be the same in whatever jurisdiction is analysed.

b. Labour conspiracy, platform as victim

Another conspiracy concern is arising relating to the phenomenon of possible labour organisation outside of the ordinary legal structures for labour union conduct. According to a leading treatise on US antitrust law, competition law principles and labour organisation principles are in tension, and must be resolved by balancing between the goals of the respective fields of law.[113] US law carve-outs for labour organisation exist in the context of collective bargaining and related activities by a labour union, as well as for a list of labour activities not involving union conduct.[114] The carve-outs do not completely exempt employees from antitrust liability for conspiracy in violation of Section 1 of the Sherman Act.[115] For example, trial lawyers were held to violate Section 1 by agreeing not to accept court-appointed representations below an agreed amount.[116]

---

[111] *See,* for example, Dalvin Brown, 'Could Uber, Lyft drivers trick the apps to increase surge pricing? Experts say probably' (*USA Today*, 15 May 2019) <https://www.usatoday.com/story/tech/2019/05/15/uber-lyft-drivers-can-probably-manipulate-apps-charge-you-more/3678461002/> accessed 9 December 2019.

[112] *See*, *Gelboim v Bank of America Corp* 823 F 3d 759 (2016), 770-71 (2d Cir) (The US Court of Appeals holding that LIBOR interest rate manipulation allegations stated antitrust claim under s 1 of the Sherman Act).

[113] Earl W Kintner and Joseph P Bauer, *Federal Antitrust Law* (Anderson Publishing Company 1989) s 72.1.

[114] ibid ss 72.1-72.7.

[115] 15 USC, s 1.

[116] *Federal Trade Commission v Superior Court Trial Lawyers Association* 1990 SCC OnLine US SC 11 : 107 L Ed 2d 851 : 493 US 411 (1990), 428-36 (finding per se illegal agreement under US law when lawyers who were unaffiliated in employment reached an agreement not to accept court appointed representations for less than an agreed fee). cf *National*

The approach to labour conspiracies in Europe is more permissive, under the general rule that employees, who are not 'undertakings', are necessarily outside the scope of Article 101 of the TFEU.[117] This carve out for employees would not apply in the case of drivers reaching cartel agreements off-platform, with consumers as victims, as individuals acting in the capacity of sole proprietors meet the definition of an undertaking.[118]

The Competition Act expressly includes associations of 'persons' in its primary prohibition on agreements, distinct from the language of Article 101 of the TFEU and from the statutory exceptions in US law.[119] In the absence of a labour exemption comparable to those found either in statute or as a matter of interplay between competing legal schemes, coordination by drivers to affect prices or terms of service offered either by the enterprise, or by consumers, presents a labour cartel concern under Indian competition law.

V. Conclusion

On attribute of the broad digitalisation of economic activity across the globe, the sharing economy has produced unique enterprise structures in a range of industries, most notably including ride sharing. Its effectiveness as an organisational structure is proved by its rapid worldwide spread and the development of a variety of free standing viable competitors at substantial scale in most distinct regions of the globe. The success of the sharing economy in supplanting old-world enterprise structures raises seemingly opposite questions – one, whether the sharing economy is somehow incompatible with socially acceptable economic structures, and two, whether the sharing economy should be seen as advancing most natural enterprise organisation. If the former, competition law might be a natural check on its growth and possible dominance. If the latter, competition law may need adjustment or at least careful application to avoid stifling a beneficial organisational structure.

Nowhere is the right answer to that question more crucial than in economies that are still on a rapid upward growth trajectory, like that in India.

Society of Professional Engineers v United States 1978 SCC OnLine US SC 69 : 5 L Ed 2d 637 : 435 US 679 (1978), 696 (holding that no-competitive bid agreement among professional engineers, orchestrated by the trade association of professional engineers, violated the Sherman Act).

[117] *Albany International BV v Stichting Bedriifspensioenfonds Textielindujstrie* (1999) Case C-67/96 : (1999) ECR I-5751 : (2000) 4 CMLR 446, paras 213-217 (ECJ) [holding that individual employees were not 'undertakings' for purposes of then-TFEU art 85].

[118] ibid para 214 [citing *Commission v Italy* (1998) Case C-35/96 ECR I-3851 (holding at para 55 that independent customs agents were 'undertakings' under then-TFEU art 85)].

[119] The Competition Act 2002, s 3(1).

Trust Me: Combining Online Dispute Resolution, Law and Blockchain Technology

Tina van der Linden[*]

Abstract *This piece focuses on the unsettled relationship between online dispute resolution, law and smart contracts (and the 'trust' provided by them). It first introduces the ways in which smart contract applications on a blockchain provide the trust required to deal with unknown business partners – trust in the network rather than in an old-fashioned trusted third party. A distinction is also drawn between calculated trust and institutional trust. The piece then attempts to reconcile the trust provided by smart contracts with the demands of business and concludes that some gaps remain. Finally, it examines what online dispute resolution and the law have to offer to deal with these gaps.*

I. Introduction

We require the ability to rely on other people to keep their promises and need some kind of remedy should things go wrong. Both formal and informal normative systems (law and norms, respectively, in Lessig's model)[1] provide for this trust, but they usually come with high transaction costs. Recently, technological possibilities have emerged (code, in Lessig's model) that may provide an alternate and cheaper way to create trust.

This piece examines the ways in which smart contract applications on a blockchain provide the 'trust' required to deal with unknown business partners. It first highlights the ways in which blockchain technology and

[*] Assistant Professor, Faculty of Law, Vrije Universiteit Amsterdam.

[1] Lawrence Lessig, *Code: Version 2.0* (1st edn, Basic Books 2006) 125.

smart contracts are used to create trust. Next, it discusses the nature of trust required to do business with unknown parties and determines the extent to which the two can be reconciled. Finally, it concludes that gaps remain and examines what online dispute resolution ('**ODR**') and the law have to offer as remedies to deal with these gaps.

II. Blockchain Technology and Trust

There are several excellent introductions to blockchain,[2] so we confine ourselves to the briefest possible explanation that allows for an understanding of how transacting on the blockchain creates trust by default.

Since the discovery of the internet, there has been an ongoing search for new ways to transfer money over it in a safe, anonymous and cheap fashion, and preferably, directly between the parties involved in a transaction.[3] The seminal paper by Satoshi Nakamoto[4] largely marks the end of this search. Nakamoto invented blockchain as a way to store transaction data and used it to create the first cryptocurrency – the (in)famous Bitcoin. Blockchain provides a novel way to store data and do business. Nakamoto cleverly combined existing techniques of peer-to-peer networking, asymmetric cryptography and hashing to create a revolutionary new way of bookkeeping – a distributed ledger of transaction records.

Peer-to-peer networking is a well-known alternative to the traditional 'client-server' networking model where each client's computer is connected to and dependent on a central server (and all communication passes through this central server). A peer-to-peer network instead considers computers in the network as each other's equals, or 'peers'. There is no central authority

---

[2] Mark Gates, *Blockchain: Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money* (1st edn, Create Space Independent Publishing Platform 2017); Kevin Werbach, *The Blockchain and the New Architecture of Trust* (1st edn, The MIT Press 2018); De Filippi Primavera and Aaron Wright, *Blockchain and the Law: The Rule of Code* (1st edn, Harvard University Press 2018).

[3] *See*, among others, Ralph C Merkle, 'Protocols for Public Key Cryptosystems' (IEEE Symposium on Security and Privacy, Oakland, April 1980) 122 <https://ieeexplore.ieee.org/document/6233691> accessed 2 January 2020; Chaum D, 'Blind Signatures for Untraceable Payments' in Chaum D et al (eds), *Advances in Cryptology* (Springer 1983); Wei Dai, 'b-money' (1998) <http://www.weidai.com/bmoney.txt> accessed 2 January 2020; Flavio D Garcia and Jaap-Henk Hoepman, 'Off-Line Karma: A Decentralized Currency for Peer-to-peer and Grid Applications' (International Conference on Applied Cryptography and Network Security, New York, June 2005) <https://link.springer.com/chapter/10.1007/11496137_25> accessed 2 January 2020.

[4] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) Bitcoin White Paper <https://bitcoin.org/bitcoin.pdf> accessed 2 January 2020.

and each computer can connect directly to every other computer. No central choking point or point of failure exists. Peer-to-peer networks are mostly popularly known for the decentralised file-sharing applications that they enabled.

Asymmetric cryptography is a technique used to encrypt and decrypt messages between two parties using two different keys, such that a message encrypted by one key can only be decrypted by the other key. The keys are mathematically related but cannot be deduced from one another. Normally, one key of the pair is called the 'private key' and should be kept strictly private. Messages encrypted by one's private key can only be decrypted by one's 'public key', which may be made available publicly. Accordingly, anyone decrypting a message with a public key can be certain that the message was sent by the holder of the corresponding private key.

Hashing is a method to seal a set of data, or, using a different metaphor, to take its fingerprint. If a hash-function is run over a set of data of any length, the output is a specific string of characters of a fixed length, called the hash. Even the minutest change in the original data set will result in a completely different hash if the hash-function is run over it again. Thus, a hash-function can be used to verify the integrity of transaction data, or in other words, to determine if any modifications have been made to said data.

A blockchain is a chain of 'blocks' of transaction data that together make up the ledger of all past transactions. The blockchain is distributed to all the peers participating in the network such that each one has an exact copy of the same ledger. Transactions concern things that can be traded on a particular blockchain, including the coin of that blockchain (like Bitcoin, Ether, or any other cryptocurrency), and possibly other things that can be represented in a digital form such as licenses, tokens, certificates and the like. The current position of each participant in the blockchain can be inferred from the ledger. To initiate a transaction, an individual must send a message containing the details of the transaction (typically, to whom they want to send what amount of money), encrypted with their private key, to the network of peers. Each one of them can verify, using the sender's public key, who the message came from. They can also determine whether or not the sender is actually entitled to the assets they want to transfer, by consulting the ledger and calculating their current position from it.

A number of verified transactions are lumped together into a new block. The new block is sealed by a hash and linked to the previous block in the chain by including the hash of this previous block in the dataset that the hash-function is run over. This process of adding new blocks to the chain

is called 'mining'. In the so-called 'proof-of-work' consensus mechanism popularly used in mining, a number (also called 'nonce', for "*number used once*") has to be determined, which when included in the data-set that the hash-function is run over, yields a hash that is below a certain threshold. This can only be done by trial-and-error – endlessly running the hash-function using random numbers as the nonce, until a nonce is found that yields a hash below the threshold.

This process makes the proof-of-work consensus mechanism extremely energy-demanding. Less energy-consuming ways of mining have been proposed,[5] but proof-of-work is still widely used. Proof-of-work can be compared to solving a Sudoku – the puzzle can be really hard to solve, but that a particular solution found is correct, is obvious. Successful miners are rewarded for the 'hard work' invested through transaction fees paid by initiators of transactions on the blockchain, and possibly, an extra amount in the coin of that particular blockchain (if so provided by that blockchain's protocol).

The fact that the hash of the previous block is included in the data which the hash-function is run over, establishes the required link. Tampering with transaction data would yield a different hash, which means that the data in all previous blocks could, for all practical purposes, be considered immutable. A change in the data would require a recalculation of all subsequent blocks because the hash value changes. A majority of the peers would need to approve of this recalculation, which is practically infeasible.[6] Alternatively, all the peers in the network would be able to see that something is wrong.

Thus, we have a distributed ledger of transactions that is immutable and requires no single controlling authority. Anyone can be a peer and verify that the approved transactions are indeed valid, and anyone can join the mining process. There is no way to rewrite history – at least not unnoticed. If we compare this with the more traditional way of processing transactions, where a bank (or another centralised institution) keeps track of each individual's position, approves and handles transactions, and remains in charge of all the administration, it is clear that the trust we invest in these intermediary 'trusted third parties' can instead be provided through blockchain networks.

---

[5] Fahad Abdullah Saleh, 'Blockchain Without Waste: Proof-of-Stake' (2020) Economics of Networks eJournal <https://www.semanticscholar.org/paper/Blockchain-Without-Waste%3A-Proof-of-Stake-Saleh/03d1b883e9d8474212094e5764646bc6450cf565?p2df> accessed 2 January 2020.

[6] Apart from the theoretical possibility of a so-called 51% attack, where an attacker manages to convince 51% of the mining nodes to validate a certain transaction, in which case it would go through.

What is described above is a so-called 'public' blockchain. There are, however, other variants. For instance, the policy by which peers are admitted to a certain blockchain may differ. If membership is restricted to a particular group, the network is termed as a 'private' or 'consortium' (permissioned) blockchain. A private blockchain can be organised in a way that best serves the purpose that the blockchain is created for – possibly, sacrificing some of the traditional public blockchain's characteristics. In particular, a central authority may re-appear – setting the rules, approving transactions (so that the energy-consuming proof-of-work mechanism can be avoided) or handling the admission of peers to the blockchain. Sacrificing the characteristics of a public blockchain comes at the price of trading the immutable trust provided by the network, as it introduces the externality of placing trust in a central authority. Nonetheless, trust may be thought of as a sliding scale – it is not a matter of all or nothing. A chain created by interlocking blocks and a ledger distributed over a reasonable number of parties may still create more trust than a central administration controlled solely by one party would, in the integrity of the data and the validity of approved transactions.

III. Smart Contracts and Trust

Smart contracts are best viewed as vending machines that 'live' on a blockchain. If you push a button and pay a specified amount of money, it gives you something in return – in case of a vending machine, a snack or a soft-drink, and in case of a smart contract, anything that can be delivered by a computer program (including ownership records, licenses, tokens, etc.) – possibly, with extended capabilities in the form of remote controlled Internet-of-Things devices (e.g., providing access to an apartment, a car, … you name it).

A smart contract is a piece of software that runs automatically on a blockchain. It may be thought of as a non-human participant that is triggered by initiating a transaction, following which its code is executed in processing the transaction, so that all the peers in the network are involved in the verification process. A smart contract may constitute a public offer that can be triggered by anyone fulfilling the conditions, or it may embody an agreement between two or more specific parties. The trust created by a smart contract is determined by the extent to which it can be relied on to be executed exactly as coded. That said, breach of contract in the sense of failure to deliver can be ruled out – once triggered, the execution of the smart contract cannot be stopped.

For smart contracts that need information from, or aim to provide an effect in the physical world (also called the 'real' world or 'off-chain' world),

an interface from and/or to the physical world is needed. In terms of trust, this interface is the most vulnerable point. Information from the real world is provided to a smart contract (inbound) by so-called Oracles, named after the function of specific priestesses in Greek mythology. Three kinds of Oracles can be distinguished:[7]

- Hardware, such as sensors and scanners,
- Software, such as information from online sources or inferences derived from data originating from other sources (e.g., a combination of sensor data and data from online sources)
- Human, such as a certification officer or an arbiter.

To understand the functions of Oracles, the following example of a mother wishing to transfer an amount of money to her son on his 18th birthday is considered. She could implement this promise through a smart contract, to make sure that no matter what, the money is transferred to the son on the date set, thus precluding her from changing her mind or the money being paid out to creditors in case of a bankruptcy. However, if the mother wants to set a condition, e.g. that the son should not have developed the habit of smoking by his 18th birthday, things become more complicated and reliance on Oracles may be required. In this context, the smart contract could provide for a number of authoritative sources that verify if the condition is met. We could think of some kind of sensor or hardware Oracle that analyses the son's breath (where the son would need to be prompted and consent to have his breath analysed), or a human Oracle – a person that can be trusted to take a decision in this matter. These options could be pre-programmed in the smart contract itself, or the matter could be left open – giving someone (either a third party or the mother herself) the authority to solve the matter. Also, a clear definition of 'the habit of smoking' is needed. What if the son shares an office with a smoker, and thus cannot help passive or secondhand smoking? Does smoking e-cigarettes, cigars or pipes count as smoking? How is smoking measured or assessed? What if the son has recently given up smoking? How much time must have passed?

If and when it is established that the son has not started smoking, he automatically receives the money pledged – there is no way to stop the transaction or change the amount. And in case it is established that he does smoke, the smart contract should ideally provide for an alternative destination for the money, for example, back to the mother or as a donation to an asthma fund.

---

[7] George Levy, 'What is a blockchain oracle?' (12 July 2018) <https://www.youtube.com/watch?v=S_1cWBWsS_I&feature=youtu.be> accessed 2 January 2020.

Another well-known example of the use of Oracles is placing a bet on the weather through a smart contract, as described, among others, by Koulu.[8] A and B place a bet on what the weather will be at a specific moment, at a specific place, by placing some money in a smart contract. Official weather reports (software Oracle) can be used to verify the weather, and the smart contract can then pay the winner. This is an illustration of how a difference of opinion between two parties may be resolved by reference to an authoritative source, and how the consequences of this solution may be executed automatically. This is very similar to how a dispute would be resolved using a smart contract application on a blockchain – which is of course what the example is meant to illustrate.

The level of trust provided by a smart contract depends considerably on the reliability of the Oracles used. In that sense, an Oracle is again a single point of failure – once the Oracle is compromised (hacked or bribed), the smart contract will be executed as coded, but on the basis of false data. Other sources of failure include damaged or out-of-order sensors and scanners, bugs in the software, incorrect or biased input data, and human error. Several approaches have been proposed to make Oracles more reliable, such as combining different kinds of Oracles, using Oracles which aggregate information from a variety of sources, or implementing the Oracle on its own consensus-based blockchain.[9]

Further, like all software, a smart contract may contain mistakes (forgivingly called 'bugs'). This may include 'normal' coding mistakes. However, it may also be the case that something went wrong in translating the parties' intentions, as expressed in natural language, into computer code. These may be problems of interpretation. It may be that there are assumptions underlying the legal text, that are not included in the code – or vice versa, that the code rests on certain unwarranted assumptions. From past attempts to build so-called legal expert systems (computer programs aimed at supporting legal reasoning), we know that the translation of law into computer code is not as

---

[8] Riikka Koulu, 'Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement' (2016) 13(1) SCRIPTed – A Journal of Law, Technology & Society 40, 69.

[9] *See*, among others, John Adler et al, 'Astraea: A Decentralized Blockchain Oracle' (IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, August 2018) <https://www.semanticscholar.org/paper/Astraea%3A-A-Decentralized-Blockchain-Oracle-Adler-Berryhill/45f581d9c5a12f6f67956baaab71d877600e13cb> accessed 2 January 2020; John Adler, 'The State of Decentralized Oracles' (*ConsenSys Media*, 28 September 2018) <https://media.consensys.net/the-state-of-decentralized-oracles-df45bf0dc51d> accessed 2 January 2020.

straightforward as it may seem at first glance.[10] It may therefore be a good idea to include the hash of the natural language version of the contract into the smart contract itself, in order to have conclusive evidence of what the parties intentions were in normal 'legalese'.[11] This combination of a natural language version of a contract and its implementation through code is an example of a Ricardian contract.[12]

Some commercially relevant and practical examples of smart contracts include applications in container logistics,[13] identity management,[14] event ticketing,[15] participation in companies,[16] and healthcare.[17] It is easy to find many other examples of blockchain pilots and use cases. Supply chain management is a well-known use-case of smart contracts on a blockchain.[18] Say, for instance, that we want to follow the path of a box of mangos through a supply chain, all the way from the farmer who harvests the mangos to the supermarket that sells them to end-consumers. The mangos will be put in a box, and someone (a human Oracle) will need to verify that it is indeed this quantity of mangos of this quality that is inside the box. In other words,

---

[10] *See*, among others, Anne von der Lieth Gardner, *An Artificial Intelligence Approach to Legal Reasoning* (1st edn, The MIT Press 1987); Tina Smith, *Legal Expert Systems: Discussion of Theoretical Assumptions* (1st edn, Tano 1995); Mirna El Ghosh et al, 'Towards a Legal Rule-Based System Grounded on the Integration of Criminal Domain Ontology and Rules' (2017) 112 Procedia Computer Science 632; Frans H van Eemeren and Bart Verheij, 'Argumentation Theory in Formal and Computational Perspective' (2017) 4(8) The IfColog Journal of Logics and their Applications 2099.

[11] As proposed by Mattereum, *see*, 'Smart Contracts. Real Property' (2020) Mattereum Working Paper <https://mattereum.com/wp-content/uploads/2020/02/mattereum_workingpaper.pdf> accessed 2 January 2020.

[12] *See*, I Grigg, 'The Ricardian Contract' (First IEEE International Workshop on Electronic Contracting, San Diego, 2004) <https://ieeexplore.ieee.org/document/1319505> accessed 2 January 2020; Usman W Chohan, 'What Is a Ricardian Contract?' (2017) University of New South Wales Discussion Paper <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3085682> accessed 2 January 2020.

[13] Port of Rotterdam Authority, 'ABN AMRO, Samsung SDS and the Port of Rotterdam Authority are launching a container logistics blockchain pilot' (Press Release, 2018) <https://www.portofrotterdam.com/en/news-and-press-releases/abn-amro-samsung-sds-and-the-port-of-rotterdam-authority-are-launching-a> accessed 2 January 2020.

[14] *See*, 'Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust' (2018) Sovrin Foundation White Paper <https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf> accessed 2 January 2020.

[15] *See*, 'Aventus White Paper: The Ultimate Blockchain Guide' (2020) Aventus White Paper <https://www.aventus.io/wp-content/uploads/2020/03/The-Aventus-Whitepaper-2020-.pdf> accessed 2 January 2020.

[16] *See*, 'Stem: A Blockchain Platform for the future of Capital Distribution through Private Company Shares (Security Tokens)' (2018) Stem White Paper <https://corporate-rebels.com/Blog/wp-content/uploads/2018/11/Stem-Whitepaper.pdf> accessed 2 January 2020.

[17] Peng Zhang et al, 'Chapter One - Blockchain Technology Use Cases in Healthcare' (2018) 111 Advances in Computers 1.

[18] *See*, 'Transform supply chain transparency with IBM Blockchain' (*IBM*, 18 June 2018) <https://www.ibm.com/downloads/cas/1VBZEPYL> accessed 2 January 2020.

a certificate will be produced by someone with the authority to issue such a certificate, and this certificate will be linked to the physical box (e.g. by sealing it to the box and adding a unique identifier to it), allowing it to be scanned and recorded on its journey. The box is put together with many other boxes in a container (the contents of which will also be certified and recorded), which is then shipped together with many other containers to another part of the world.

As lawyers, we are programmed to use our imagination to think of as many things as possible that may go wrong. There is always the possibility of fraud. A creepy crawler may accidentally end up in the box and eat all the mangos. The container may be blown off the ship on the high seas, the ship itself may be lost – many things may go wrong that are not necessarily recorded or prevented by the blockchain system governing the supply chain. In other words, the weakest link is the interface with the physical world, which is unpredictable and messy. The traditional issues that come with the application of abstract pre-formulated rules to subsequently arising concrete cases (such as open texture, vagueness, unforeseen circumstances etc.)[19] do not go away if smart contracts are used.

In sum, a smart contract application creates trust in the other party complying with their part of the deal as programmed. It is important to note that the weakest point is the interface to the real world (Oracles), and that all the traditional challenges of applying rules to concrete cases still remain. A blockchain cannot be considered as a single source of truth in the sense that any fact registered on the blockchain therefore, by definition, corresponds to the truth in the physical world.[20] At most, a blockchain creates trust in the peers' consensus on the truth of the facts recorded on the blockchain. There may still be a gap between the actual physical world and its representation in a database.

IV. Trust Required to do Business

We, humans, are only human. As such, we are subject to all the restrictions that come with our 'condition humaine'. We are very fragile, vulnerable and

---

[19] *See*, among others, HLA Hart, *The Concept of Law* (1st edn, OUP 1961); William Twining and David Miers, *How to Do Things with Rules* (5th edn, CUP 2014); Gardner (n 10); Smith (n 10).

[20] *See*, among others, John Plansky, Tim O'Donnel and Kimberly Richards, 'A Strategist's Guide to Blockchain' (*strategy+business*, 11 January 2016) 7 <https://www.pwc.no/no/publikasjoner/Digitalisering/sb82_A_Strategists_Guide_to_Blockchain.pdf> accessed 2 January 2020.

mortal. We have only limited rationality,[21] and face difficulty in sacrificing our own short term interest for the collective long term interest – even if such collective long term interest is also in our self-interest. This is sadly illustrated by our struggle to save our planet from our own destructive behaviour.

In order to survive, we need to cooperate. Cooperation means striking deals with others, promising to do something in exchange for a promise by the other party – you scratch my back and I'll scratch yours. Between parties that have a long term (business) relationship, keeping promises is quite evidently in their own self-interest. In other words, trust may not be a big issue. However, for one-shot transactions between parties that do not know each other, the situation is very different – how can you rely on the other party to keep their promise, if defecting is in their own short-term interest?

Our capitalist society is built on the premise that if everyone pursues their own best interest (within certain limits), everyone is better off. So, a mechanism is needed to make sure that defecting in a one-shot transaction with an unknown party is not in one's own best interest. This is, of course, where law comes in. Should someone fail to live up to their promise, you can sue them: "*See you in court!*". The law provides for remedies, in theory at least, not only in case the other party fails to meet their promises because of their own self-interest, but also if there is a misunderstanding about the agreement itself, or in cases of force majeure. In contract law, notions like (common) mistake, frustration of contract, misrepresentation etc. were developed to deal with the various things that may go wrong and to establish a fair distribution of the risks involved in trade.

However, even if a legal remedy may be available in theory, that does not always mean that it is possible or feasible to sue someone. Barriers in terms of costs, effort involved, and estimated chances of success are good reasons to accept an unfair situation instead of taking legal action. In some cases, a substitute may be available in the form of an Alternative Dispute Resolution ('**ADR**') procedure, such as arbitration or mediation. When ADR takes place online, it is usually called ODR.

Another mechanism to make sure that defecting in a one-shot transaction with an unknown party is not in one's own best interest, is reputation. Your reputation as a reliable business partner may be an important factor in other people's willingness to do business with you. The law provides mechanisms which allow you to build up a reputation (trademarks, test marks, labels) and to guard it (libel, slander). Obviously, communication is crucial

[21] Daniel Kahneman, *Thinking, Fast and Slow* (1st edn, Farrar, Straus and Giroux 2011).

for reputation to be effective as an indicator of trustworthiness. Accordingly, reviews, ratings and other public feedback and evaluation mechanisms are important but should be reliable.

Thus, we see the notion of trust arising at different points in the account above. You need to trust someone to do business with them, you need to trust the legal procedure to provide you with a fair remedy, and you need to trust reviews and ratings.

At least three different types of trust are distinguished in scholarly literature – calculative trust, personal trust, and institutional trust.[22] Of these types, both calculative and institutional trust are relevant to the decision to do business with unknown business partners.

For our purposes, calculative trust can be understood as the outcome of the comparison of the estimated profit that a transaction will bring with the risk that things will go wrong and the damage that would then arise. Institutional trust, again for our purposes, can be understood as the trust in a certain institution and/or the procedure facilitated by the institution in question. In particular, that if a legal remedy is sought, a fair trial[23] will take place, and that the subsequent decision by the court will be meaningfully enforced. Or for ODR – that the dispute is decided in a fair way (by independent and impartial jurors or arbitrators, who consider all the evidence and are open to both parties' arguments, etc.), and that the decision will be complied with (or enforced). In the institutional trust required for a legal or ODR procedure is also present an element of calculation – there are transaction costs (time involved, possibly legal advice, uncertainty about the outcome etc.) that are weighed against the estimated chances of success.

Institutional trust is also required for the process by which reviews and ratings are produced – we should be able to rely on their truthfulness and on the fact that no negative reviews and ratings were deleted by the interested party. Some intermediaries (such as booking sites) are in a position to guarantee true reviews in the sense that only those who actually booked are given the opportunity to write a review (not excluding the possibility of fake bookings in order to be able to write a favourable review). However, the transactions costs (fee paid to the booking site) perhaps outweigh the benefit of a fake review.

---

[22] Oliver E Williamson, 'Calculativeness, Trust, and Economic Organization' (1993) 36(1) The Journal of Law and Economics 453, 485-486.

[23] As expressed by Article 6 of the European Convention on Human Rights (ECHR).

Personal trust is described by Williamson to be present when one party consciously refuses to monitor the other party, is predisposed to ascribe good intentions to the other party when things go wrong, and treats him or her in a discrete structural way.[24] Given the design of the blockchain as immutable and transparent, and with its democratic consensus mechanism, the mining nodes lack the ability to act upon their personal interests – unless they are able to ally with 51% of the network. Therefore, personal trust is not relevant on a blockchain. Indeed, parties do not necessarily know (nor do they need to know) each other's identity.

In sum, the trust required to trade with unknown business partners consists in calculated trust that they will fulfill their promises and institutional trust in reputation, and in case something does go wrong, that the matter will be resolved fairly.

V. Matching Trust by Smart Contracts with Trust Required to do Business

In this section, we examine how the trust offered by smart contract applications on a blockchain provides for the trust required to trade with unknown business partners.

If indeed the trust needed to trade with unknown business partners can be provided by smart contract applications on a blockchain, this is very good news for start-ups that are yet to build up a reputation or a network of business partners. It is also good news for parties that operate from jurisdictions that do not provide a reliable or stable back-up legal structure to enforce agreements, as well as for small scale businesses or consumers/citizens that do not have easy access to (or trust in) traditional financial or government institutions. On a blockchain, it does not matter where you are located physically – at least not for the decision of others to do business with you. Blockchain based smart contracts thus have a truly enabling potential for a more equal and fair distribution of business opportunities across the globe.

The calculated trust that the other parties will fulfill their promises can to some extent be provided for by smart contract applications on a blockchain. The fact that a smart contract will perform exactly as programmed can be added to the list of things (consisting of death and taxes)[25] that you can be absolutely certain of in life. The words 'exactly as programmed' are

---

[24] Williamson (n 22) 483.

[25] First mentioned, reportedly, by Christopher Bullock in *The Cobbler of Preston* in 1716, and famously quoted by Benjamin Franklin in a letter to Jean-Baptiste Leroy in 1789.

crucial here, because as indicated earlier, software may contain bugs and smart contracts are no exception to this. Further, there may be differences of interpretation and cases of force majeure. In particular, the truth of facts recorded on the blockchain is limited to the consensus of the parties validating the transactions, as explained earlier. Beyond that, there is no guarantee to the actual truth. Accordingly, there is still plenty of room for things to go wrong and for conflicts to arise.

In cases where conflicts do arise, what often turns out to be crucial is what can be proven. Here, the blockchain ledger of transactions comes in very handy because there is (in theory) solid evidence of everything that happened on the blockchain. However, the solidity (and therefore, the trustworthiness) of such evidence obviously hangs together with the way the blockchain is organised. A private or consortium blockchain where only one or a few peers validate transactions, and which is not secured by a consensus mechanism specifically intended to prevent tinkering (such as proof of work), will not deserve the same amount of trust in the truthfulness of the ledger as a completely public blockchain will.

Moreover, as explained earlier, the ledger only reflects the consensus of the peers. For transactions that can be verified digitally, this is fine, but for those that have a link to events in the real world, it is important to realise that consensus of peers is not the same thing as truth in an empirical sense. Sometimes, it is claimed that an advantage of using a blockchain for recording data is that it provides a single source of truth.[26] In my view, this is misleading – a blockchain can at best provide a single source of consensus. The actual truth may be something very different.

Thus, even if we can trust a smart contract to perform exactly as programmed, there is always the possibility that something may go wrong. What is therefore required is institutional trust that in case something does go wrong (as in the examples given above), conflicts will be resolved in a fair manner.

VI. Filling the Gaps with Online Dispute Resolution and Law

Due to the possibility that something may go wrong and the corresponding need for institutional trust, it is advisable for businesses using smart contracts to incorporate appropriate dispute resolution mechanisms.

---

[26] *See*, Plansky and others (n 20) 7.

A rather straightforward way to do so is to use a so-called 'multisig arrangement' (where an action can go through if two out of three signatories approve it) in the smart contract itself, for cases in which a party's consent or approval is needed before an action can take place. For example, a contract states that the quality of goods delivered or service provided can be assessed by the recipient before a payment is made. In cases where the quality is sufficient, there would be only two parties to the agreement. If, however, the recipient finds that the quality is below standard, the signature of a third party (arbitrator) would be needed to authorise the action,[27] thereby giving the arbitrator the responsibility to assess the quality and decide on the dispute.

As discussed earlier, there is also an initiative to store (the hash of) a traditional contract in the smart contract (so that there is always evidence of the original natural-language version of the contract that the parties agree on – a so-called Ricardian contract), together with a built-in ODR mechanism, involving human arbitrators. This is the original idea of the start-up Mattereum.[28]

Additionally, there are blockchain applications that offer alternative dispute resolution, such as Kleros[29] and Aragon.[30] The idea is that the parties to a dispute (that may or may not involve blockchain transactions) use a smart contract to have independent jurors decide on their dispute. Anyone interested can apply for the position of juror – providing possible job opportunities for people who might otherwise have a difficult position on the labour market. Such a scheme can be called a Crowdsourced Online Dispute Resolution model.[31] The jurors are incentivised by game theory to look into the dispute seriously and decide either for the plaintiff or for the defendant, such that a juror who votes along with the majority gets paid in the coin of that particular application, while a juror with a minority vote loses his or her stake. From a theory of law perspective, this is a very interesting and

---

[27] Vitalik Butarin, 'Bitcoin Multisig Wallet: The Future of Bitcoin' (*Bitcoin Magazine*, 13 March 2014) <https://bitcoinmagazine.com/articles/multisig-future-bitcoin-1394686504> accessed 2 January 2020.

[28] Mattereum (n 11).

[29] Clément Lesaege, Federico Ast, and William George, 'Kleros Short Paper v1.0.7' (2019) Kleros White Paper <https://kleros.io/static/whitepaper_en-8bd3a0480b-45c39899787e17049ded26.pdf> accessed 2 January 2020.

[30] 'Aragon Network' (2019) Aragon White Paper <https://github.com/aragon/whitepaper> accessed 2 January 2020.

[31] *See*, for a proposal of a model for fair Crowdsourced Online Dispute Resolution (CODR), Daniel Dimov, 'Crowd sourced Online Dispute Resolution' (PhD thesis, Leiden University Center for Law and Digital Technologies 2017) 149-166 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3003815> accessed 2 January 2020. It is not at all clear how Kleros or Aragon comply with the elements identified here for a fair CODR procedure.

not uncontroversial way to look at adjudication. Jurors, thus incentivised, will vote for what they think the majority of jurors will vote for. This is not necessarily the 'right' answer,[32] or the most just answer. Take for example a case where the most just answer is not evident from a quick glance at the case, and which instead requires an active effort to look at all the details, weigh up the interests etc.

How can a juror in such situation be confident that all the other jurors put in the effort of really looking into the case? It may very well be that their safest bet (just like everyone else's) is to go for the quick solution, and that may not be the most just.

Finally, if all else fails, we always have good-old law to fall back on. Everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations, according to Article 10 of the Universal Declaration of Human Rights.[33] Of course, there may be hurdles to sue a party located in a different jurisdiction, but private international law does provide for solutions, at least in theory.

Blockchain applications do not operate in a legal vacuum.[34] Like internet mediated communication, blockchain applications concern real people in the real world with real assets. At the interface between blockchain and the real world, so at the exchanges, where cryptocurrencies are spent or where the effects of smart contracts materialise, the long arm of the law may appear, and seize, tax, protect or enforce as it sees fit. And that is as it should be, because the law exists for a reason.

VII. Conclusion

The relationship between trust, blockchain, ODR and law is still rather confusing and needs further attention and study.

It seems clear that blockchain can organise trust in a new and different way, and that this may have far-reaching consequences. Some business

---

[32] If a single right answer exists at all, which is not uncontroversial. *See*, the discussion between Hart and Dworkin in Hart (n 19) and Ronald Dworkin, *Taking Rights Seriously* (5th edn, Harvard University Press 1978). Also discussed, among others, in Richard Bellamy, 'Ronald Dworkin, Taking Rights Seriously' in Jacob T Levy (ed), *The Oxford Handbook of Classics in Contemporary Political Theory* (OUP 2015).

[33] In the determination of his civil rights and obligations, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law (ECHR, art 6).

[34] *See*, for a detailed account on the relation between blockchain and law, Werbach (n 2).

models will become outdated, and other business opportunities will arise. Traditional trusted third parties like banks and public notaries may need to reinvent themselves and find new ways in which they can offer added value, now that the trust they used to deliver can be provided by blockchain-based applications. However, there remain certain shortcomings – the trust provided by smart contracts needs to be complemented by the availability of legal/institutional procedures to fall back on. The availability of an ODR option may enhance trust in blockchain based applications, and ODR may itself be organised as a smart contract – solving the issue of compliance with the decision. It could also be argued that smart contracts prevent disputes to some extent (thus partly putting both ODR and law out of a job), because automatic execution serves to disincentivise breach of contract.

It seems equally clear that the law will need to evolve and develop itself, but that we cannot do without law in the foreseeable future. ODR and law can be seen to complement each other – for cases where the recourse provided by law is inefficient or even inaccessible, ODR may provide a useful solution. Blockchain also needs law – in order to inspire trust, there must be governance and compliance with the existing legal order.

Trust, therefore, is what we all need in order to be able to cooperate and to survive. I can see it in my puppy's eyes.

The Changing Landscape of Intermediary Liability for E-Commerce Platforms: Emergence of a New Regime

Vasundhara Majithia[*]

Abstract *As India becomes the fastest growing market for e-commerce in the world, it is also grappling with the issue of proliferation of counterfeits on e-commerce portals. India's judicial system has awakened to this predicament and in a spate of judgements, has sought to evolve a mechanism balancing the rights of e-commerce platforms as intermediaries via-a-vis the rights of brand owners and public interest at large. This article explores the evolution of intermediary liability in India by examining its legal framework, as well as the jurisprudence developed by Indian courts in this regard. It traces the shift in this jurisprudence from the classical 'free speech' understanding to the 'notice and takedown' regime to a determination of whether e-commerce platforms qualified as 'intermediaries' in the first place. It concludes that while new jurisprudence evolved by Indian courts substantially clarifies the framework of intermediary liability vis-à-vis e-commerce platforms, several challenges lie ahead for both brand owners and e-commerce platforms in addressing this issue. It then seeks to understand these challenges in light of the policies proposed to regulate the e-commerce space, and finally recommends a self-regulatory mechanism to combat the online proliferation of counterfeits.*

[*] Associate, Fidus Law Chambers.

I. Introduction

With the advent of the internet, electronic commerce ('**e-commerce**') has become a driving force of the global economy. The convenience and range of possibilities for consumers, coupled with low costs of inventory management etc., as compared to traditional retail, ensures that the e-commerce industry booms. As per the United Nations Conference on Trade and Development, global e-commerce sales were an estimated USD 29 trillion in 2017, with India in ninth position with sales of USD 400 million.[1] By 2022, e-commerce is projected to become the largest retail channel in the world, surpassing retail outlets for various categories of goods and services.[2]

As per reports, India is the fastest growing market for e-commerce in the world, worth over USD 83 billion in 2018,[3] and is envisaged to grow at 51% per annum to reach up to USD 120 billion in 2020.[4] E-commerce has provided brand owners a new avenue for sales and the potential to penetrate previously undiscovered consumer segments of the Indian market. Market trends in 2018[5] and 2019[6] show that e-commerce growth is driven by the

---

1 United Nations Conference on Trade and Development, 'Lack of digital in development strategies in focus at eCommerce Week' (2019) <https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2032> accessed 13 November 2019.

2 'What's New in Retail: Emerging Global Concepts' (Euromonitor International Report, 2017) <https://blog.euromonitor.com/e-commerce-is-the-fastest-growing-global-retail-channel-through-2022/> accessed 13 November 2019; *See also*, Michelle Grant, 'E-commerce Set for Global Domination – But At Different Speeds' (*Forbes*, 14 August 2018) <https://www.forbes.com/sites/michellegrant/2018/08/14/e-commerce-set-for-global-domination/#1c1941bebfaf> accessed 13 November 2019.

3 United Nations Conference on Trade and Development, 'India's digital services exports hit $83 million says new survey' (2018) <https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=1917&Sitemap_x0020_Taxonomy=UNCTAD%20Home;%20-%202045> accessed 13 November 2019.

4 'E-commerce Industry in India' (*Indian Brand Equity Foundation*, December 2018) <https://www.ibef.org/industry/ecommerce.aspx> accessed 13 November 2019.

5 Ameen Khwaja, 'Tier II, III cities drive e-commerce in India' *Deccan Herald* (Bengaluru, 31 May 2018) <https://www.deccanherald.com/opinion/panorama/tier-ii-iii-cities-drive-e-commerce-india-672765.html> accessed 13 November 2019.

6 'E-commerce brands focus on Tier 2, 3 shoppers during festivals' *The Economic Times* (Mumbai, 28 September 2019) <https://retail.economictimes.indiatimes.com/news/e-commerce/e-tailing/e-commerce-brands-focus-on-tier-2-3-shoppers-during-festivals/71349748> accessed 13 November 2019.

burgeoning middle classes in Tier II and III cities, especially in the festive seasons,[7] as e-commerce provides a convenient method of shopping for a variety of products previously unavailable in these cities.

At the same time, it has also provided a convenient and wide platform for the sale of counterfeit products. As per a survey conducted in India, nearly 20%, or one in five consumers, claimed that they had received a counterfeit product from a leading e-commerce website in the preceding six months of the survey.[8] India's judicial system has also awakened to this proliferation of counterfeits on e-commerce portals, and in a spate of new judgements, begun coming down heavily on several e-commerce platforms which earlier escaped all liability under statutory exemptions granted to intermediaries.

This paper examines the evolution of intermediary liability in India for e-commerce companies. Part I explores the tremendous growth of e-commerce in India, and its expected growth in times to come. In Part II, we highlight the primary laws that govern intermediary liability in India and underline the roles and responsibilities of e-commerce marketplaces. Next, in Part III, we study the jurisprudence evolved by Indian courts in some detail. We begin with analysing the dictum of the Supreme Court of India ('**the Supreme Court**') vis-à-vis free speech principles, and the subsequent shift towards a notice and takedown regime for infringements of intellectual property. We then take a look at the flurry of decisions cracking down upon e-commerce platforms for intellectual property violations and calling into question their legal status as intermediaries in this regard. Further, we examine the conflict of e-commerce marketplaces with direct selling models and end with an analysis of the recent appeal decision which substantially clarified this highly contentious and entangled jurisprudence. In Part IV, we take a look at proposed amendments to the law which will impact the roles and responsibilities of e-commerce marketplaces, and analyse their gaps. Finally, Part V highlights the challenges that lie ahead for e-commerce marketplaces and proposes a self-regulatory mechanism to combat online counterfeiting by following a balanced approach.

---

[7] Peerzada Abrar, 'Festive sale: Tier-II, III cities drive big biz for Flipkart and Amazon' *Business Standard* (New Delhi, 1 October 2019) <https://www.business-standard.com/article/companies/small-cities-usher-in-festive-cheer-for-flipkart-amazon-with-big-business-119093001416_1.html> accessed 13 November 2019; *See also*, 'Tier-2 customers driving the $14.5 billion e-commerce industry in India: RedSeer report' *Money Control* (Mumbai, 17 January 2018) <https://www.moneycontrol.com/news/business/startup/tier-2-customers-driving-the-14-5-billion-e-commerce-industry-in-india-redseer-report-2485383.html> accessed 13 November 2019.

[8] 'Counterfeit or fake products on e-Commerce sites is a much bigger problem than we thought' (*Local Circles*, 1 November 2018) <https://www.localcircles.com/a/press/page/fake-products-on-ecommerce-sites#.XIqlCCgzbIU> accessed 13 November 2019.

II. Applicable Laws

A. The Information Technology Act, 2000

The provisions pertaining to intermediary liability were introduced by way of an amendment[9] to the Information Technology Act, 2000 ('**the IT Act**') in 2008, when the CEO of Bazee.com, an e-commerce marketplace, was arrested after an obscene video clip was offered for sale on the said e-commerce portal.[10] Under Section 2(1)(w) of the IT Act, an 'intermediary' is defined as any person who receives, stores or transmits an electronic record on behalf of another person, or provides any service with respect to that record, and includes online auction sites and online market-places.[11]

The primary provision pertaining to intermediary liability in India is Section 79 of the IT Act.[12] As per this provision, an intermediary will not be liable for any third-party information made available or hosted by them, provided that the function of the intermediary is limited to providing access, and the transmission is not initiated, selected or modified by it. To claim such exemption, it is also necessary that the intermediary observes 'due diligence' while discharging its duties as provided by the IT Act or other guidelines.[13] However, as per Section 79(3) of the IT Act, an intermediary will not be exempted from liability if it has induced, conspired, abetted or aided in the commission of the unlawful act, or if it fails to expeditiously remove or disable access to the unlawful material upon receiving 'actual knowledge' or on being notified by the appropriate government agency about the said data being used to commit the unlawful act.[14]

The exemption granted under Section 79 of the IT Act is also referred to as a 'safe harbour' provision for intermediaries. In the context of e-commerce, some have termed these provisions as a legal 'subsidy'[15] extended towards e-commerce companies, allowing them to scale rapidly, with relatively low costs and little legal compliance involved.

---

[9] *See*, the Information Technology (Amendment) Act 2008.

[10] Nikhil Pahwa, 'A serious and imminent threat to the open Internet in India' (*MediaNama*, 22 January 2019) <https://www.medianama.com/2019/01/223-a-serious-and-imminent-threat-to-the-open-internet-in-india/> accessed 13 November 2019.

[11] The Information Technology Act 2000, s 2(1)(*w*).

[12] The Information Technology Act 2000, s 79.

[13] The Information Technology Act 2000, s 79(2)(*c*).

[14] The Information Technology Act 2000, s 79(3).

[15] Prashant Reddy T, 'Liability, Not Encryption, Is What India's New Intermediary Regulations Are Trying to Fix' (*The Wire*, 28 December 2018) <https://thewire.in/government/liability-not-encryption-is-what-indias-new-intermediary-regulations-are-trying-to-fix> accessed 13 November 2019.

There are two key phrases used in the provision – 'due diligence' and 'actual knowledge'. It would not be unfair to say that the entire regime of intermediary liability revolves around demarcating the thresholds of 'due diligence' and 'actual knowledge', as we will see in the jurisprudence below.

B. Information Technology (Intermediaries Guidelines) Rules, 2011

In 2011, four sets of rules were notified under the IT Act, including the Information Technology (Intermediaries Guidelines) Rules, 2011 ('**the Intermediaries Guidelines**').

In addition to the standards already laid out in the IT Act, Rule 3 of the Intermediaries Guidelines specifies the due diligence to be observed by an intermediary. An intermediary is directed to publish rules and regulations, a privacy policy and a user agreement for its users.[16] Inter alia, the rules and regulations must inform the users not to share any information which infringes any patent, trademark, copyright or other proprietary rights.[17] Further, the intermediary must, upon obtaining knowledge by itself or being provided 'actual knowledge' by an affected person in writing, disable access to such information within thirty-six hours.[18]

III. The Jurisprudence of Intermediary Liability

A. Shreya Singhal and its Aftermath

Shreya Singhal v. *Union of India*[19] is a landmark case which arose when the police arrested two women for posting allegedly offensive and objectionable comments about the death of a political leader on Facebook, leading to their arrest under Section 66A[20] of the IT Act, which in turn resulted in a challenge to the constitutionality of several provisions of the IT Act. While

---

16 The Information Technology (Intermediaries Guidelines) Rules 2011, r 3.

17 The Information Technology (Intermediaries Guidelines) Rules 2011, r 3(2).

18 The Information Technology (Intermediaries Guidelines) Rules 2011, r 3(4).

19 *Shreya Singhal v Union of India* (2013) 12 SCC 73 (*Shreya Singhal*).

20 The Information Technology Act 2000, s 66A: Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device, —

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of

Section 66A was struck down in its entirety, the Supreme Court read down Section 79(3)(b) of the IT Act and Rule 3(4) of the Intermediaries Guidelines, interpreting the word 'knowledge' to mean knowledge only by means of a court order or government notification. Consequently, intermediaries were not liable to takedown anything from their platforms on the basis of a mere user complaint not backed by a court order. Prior to this judgement, 'actual knowledge' under the IT Act and the Intermediaries Guidelines could potentially be interpreted as the intermediary exercising its own judgement, and playing judge, jury and executioner in adjudicating what constitutes 'unlawful information'. This adjudicatory role must be played by a court of law and not a private body in order to prevent a chilling effect on online free expression through private censorship.[21]

This landmark judgement radically altered the threshold of 'knowledge' for holding an intermediary liable for any content it hosted or stored. While the judgement was written in the context of free speech and the liability of intermediaries such as Facebook, the decision was equally applicable to e-commerce marketplaces. Resultantly, e-commerce marketplaces were not obligated to take down listings that brand owners claimed were counterfeit, in the absence of a court order. Accordingly, the due diligence obligations of e-commerce marketplaces in the context of counterfeiting were nearly zero, unless otherwise specified under relevant rules, regulations and policies or directed by a court.

B. Evolution of the 'Notice and Takedown Regime'

In *MySpace Inc.* v. *Super Cassettes Industries Ltd.*,[22] the Division Bench of the Delhi High Court adjudicated upon the parameters and thresholds of intermediary liability with respect to copyright laws, and held that intermediaries must be provided with 'specific knowledge' and that merely a general awareness or apprehension of an intermediary that the content may be infringing will not amount to 'knowledge' and make the intermediary liable.

The court considered the holding in *Shreya Singhal*[23] and observed that this judgement was rendered in the context of the restrictions under Article

such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

[21] *See*, Jyoti Panday, 'The Supreme Court Judgment in Shreya Singhal and What It Does for Intermediary Liability in India?' (*The Centre for Internet and Society*, 11 April 2015) <https://cis-india.org/internet-governance/blog/sc-judgment-in-shreya-singhal-what-it-means-for-intermediary-liability> accessed 13 November 2019.

[22] *MySpace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382 : (2017) 69 PTC 1 (*MySpace*).

[23] *Shreya Singhal* (n 19).

19(2) of the Constitution of India ('**the Constitution**'),[24] i.e. the freedom of speech, and that in the case of copyright laws, it was sufficient for MySpace to receive specific knowledge of the infringing works from the content owner without the necessity of a court order. Therefore, the court held that an intermediary, on receiving 'actual knowledge' or obtaining knowledge from the affected person in writing or through email, was to act within 36 hours of receiving such information and disable access to the infringing content. In this judgment, the Division Bench of the Delhi High Court therefore implemented a 'notice and takedown regime' for intellectual property rights issues and held that the strict free speech standards laid down in *Shreya Singhal* were not required to be applied to intellectual property rights violations, specifically those of copyright.

In the 2017 case of *Kent RO Systems Ltd.* v. *Amit Kotak*,[25] the plaintiff instituted a suit against a seller on eBay, as well as eBay itself, for offering for sale of water purifiers that infringed the designs of the plaintiff. The plaintiffs alleged that as per the IT Act and Intermediaries Guidelines, intermediaries like eBay were expected to observe due diligence such as informing their sellers not to offer infringing products for sale and taking steps to avoid the sale of such products. eBay claimed in its response that it had removed all products complained of and undertook to continue to do so in the future on receipt of any complaint from the plaintiff. eBay contended that it was exempted from liability as it expeditiously removed the infringing products on being notified by the court order, and thus, discharged its due diligence. However, the plaintiffs asserted that once intimated of counterfeiting, the obligation of eBay extends not just to removing that particular product, but also to ensuring that no other infringing products are being hosted on its website.

The Single Judge held that the Intermediaries Guidelines only requires an intermediary to remove infringing listings upon receiving actual knowledge of the same, and that the intermediary cannot be expected to remove infringing products before they have even been complained of. The court held that imposing the obligation of pre-screening on an intermediary effectively converts it into a body that determines whether there is any infringement of intellectual property rights, a legal and technical question, which

---

[24] The Constitution of India 1950, art 19(2): Nothing in sub clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence.

[25] 2017 SCC OnLine Del 7201 : 2017 (69) PTC 551.

the intermediary cannot adjudicate upon. The Single Judge also observed that the hosting of information on eBay being automatic and without human intervention, it was not possible to direct eBay to screen all listings for violation of IP, as this would bring its business to a halt. Further, with respect to the plaintiff's contention that it cannot be expected to be so vigilant all the time to keep looking for infringing products on eBay, the court held that similarly, even eBay cannot be expected to exercise such vigilance.

This judgement was appealed by the plaintiff,[26] where it argued that the pattern of behaviour and conduct of eBay disclosed its knowledge of infringement. The Division Bench held that the observations made by the Single Judge virtually foreclosed the right of the plaintiffs to prove if and how the knowledge threshold was met. Accordingly, the plaintiff was allowed the liberty to establish the 'knowledge' threshold mandated by Section 79(3)(b) by leading evidence at trial. However, since no final judgement has been rendered in this matter yet, it is unclear what factual and evidentiary thresholds may be used by the court to determine eBay's knowledge of infringement.

C. The Decision in Christian Louboutin: A Gamechanger

In *Christian Louboutin SAS* v. *Nakul Bajaj*,[27] the plaintiff brought suit against darveys.com, a website selling imported luxury products in India, on the grounds that Darveys was offering for sale counterfeit and impaired products which infringed its trademarks.

Darveys inter alia claimed that even if there was infringement/counterfeiting, it would not be liable as it was an intermediary whose role was limited to booking orders to various sellers across the globe and dispatching the products to their customers. The question before the court was whether Darveys was an intermediary and thus, exempt from liability for trademark infringement. In this regard, the court sought to take a deeper look at the business model and policies of Darveys. It observed that Darveys was a members' only website which arranged for the transport of products to the customers. Darveys made claims that all its products were 100% genuine, so much so that its authenticity guarantee extended up to the return of twice the money in case the product turned out to be counterfeit. It also placed a seal of authenticity guarantee on the website and claimed that quality checks were

---

[26] *Kent RO Systems (P) Ltd v eBay India (P) Ltd* FAO (OS) (COMM) 95/2017 (Del) (*Kent RO*).

[27] *Christian Louboutin SAS v Nakul Bajaj* 2018 SCC OnLine Del 12215 : (2018) 76 PTC 508 (*Christian Louboutin*).

carried out by a third-party team of trained experts who examined the products before shipping them to customers. Notably, Darveys did not reveal its list of foreign sellers from whom the products were sourced.

The court observed that the policies of Darveys clearly show that it was responsible for listing, pricing, transporting and conducting quality tests on the products. Therefore, Darveys exercised complete control of inventory, and its role was much more than that of an intermediary, i.e. the mere provision of a technical platform as defined under the IT Act. Accordingly, it held that not all e-commerce websites can be categorised as intermediaries, and laid down a list of factors such as transporting, packaging, warehousing, providing quality assurance and authenticity guarantees, advertising the products on the platform, providing call centre assistance etc., which would indicate that the e-commerce entity had crossed the line from an 'intermediary' to an 'active participant', and could thus be liable for its role in the infringing acts. In the court's opinion, e-commerce marketplaces providing such logistical support must not be automatically deemed as intermediaries as their conduct cannot be termed as inactive, passive or merely technical, and they are active participants in the trade.

The court also relied on *MySpace*[28] and interpreted the judgement of *Shreya Singhal*[29] as being in the context of free speech and not of intellectual property infringements in e-commerce. The court noted that in *Shreya Singhal*, Section 79(3)(b) of the IT Act was read down subject to the caveat that a court order or government notification would be necessary in respect of unlawful acts mentioned in Article 19(2) of the Constitution (such as allegedly seditious, defamatory, inciteful or indecent content etc.). Thus, the high threshold of receiving a court order or government notification to obtain 'actual knowledge' was not applicable in respect of intellectual property violations. Further, it held that the 'due diligence' criterion provided under the IT Act must be construed broadly and not restricted merely to the guidelines themselves. Accordingly, Darveys was held liable for trademark infringement, and could not take shelter under the safe harbour provisions of the IT Act.

For brand owners, this judgement was a welcome development as it distinguished between intermediaries and e-commerce companies, which would help prevent the misuse of safe harbour provisions by active participants seeking to escape liability.

---

[28] *MySpace* (n 22).
[29] *Shreya Singhal* (n 19).

However, for intermediaries, the judgement provided several insurmountable challenges. *First*, no rationale is provided for the list of factors which determine whether the platform is an intermediary or not, despite most e-commerce entities engaging in one or more of these activities.[30] *Second*, it is not clear which factors are to be construed positively for the intermediary and which are to be negative, since identification of the seller etc. surely cannot be a negative factor for a platform. Non-identification of the seller was one of the reasons the court held that Darveys was not an intermediary. *Third*, there is no clarity on whether a defaulting intermediary is liable for primary or secondary infringement. *Fourth*, the court did not elaborate on its observation that *Shreya Singhal* will not apply to e-commerce platforms as there is no violation of the right to speech. In fact, the sale and listing of products on online platforms qualifies as commercial speech which is also protected within the ambit of free speech, albeit to a lesser degree when compared with political speech.[31] Instead of the court distinguishing or reading down the judgement in *Shreya Singhal* in the context of commercial speech, it negated its application to e-commerce in toto. *Fifth*, the judgement implies that the phrase "*any service under that record*" provided in the IT Act and Intermediaries Guidelines (which permits the intermediary to provide ancillary services) can only be with respect to electronic record and that no physical services such as transport, delivery etc. are permissible. *Sixth*, the holding that intermediaries have 'broader responsibilities' which go above and beyond the thresholds laid out in the Intermediaries Guidelines lacks sufficient clarity and specificity.

The judgement also presented a direct dichotomy with the Guidelines for Foreign Direct Investment in E-Commerce ('**the FDI Guidelines**') of 2016[32] and 2018.[33] As per the said guidelines, there are two models of e-commerce: marketplace and inventory based. A marketplace model of e-commerce is that which provides an information technology platform to facilitate transactions between a buyer and a seller.[34] An inventory based model is that where the inventory of goods and services is owned by the e-commerce entity and

---

[30] Divij Joshi, 'Delhi High Court Examines Intermediary Liability for Trademark Infringement (Part – II)' (*SpicyIP*, 19 November 2018) <https://spicyip.com/2018/11/delhi-high-court-examines-intermediary-liability-for-trademark-infringement-part-ii.html> accessed 13 November 2019.

[31] *Indian Express Newspapers (Bombay) (P) Ltd v Union of India* (1985) 1 SCC 641 : AIR 1986 SC 515; *Tata Press Ltd v Mahanagar Telephone Nigam Ltd* (1995) 5 SCC 139.

[32] Guidelines for Foreign Direct Investment (FDI) on E-Commerce, Press Note No. 3 (2016 Series), dated 9 March 2016.

[33] Review of the Policy on Foreign Direct Investment (FDI) in e-commerce, Press Note No. 2 (2018 Series), dated 26 December 2018 (FDI Guidelines – 2018 Series).

[34] FDI Guidelines – 2018 Series, para 5.2.15.2.2 (iv).

sold to customers directly.[35] As per the FDI Guidelines 2018, a marketplace model exercising ownership over the inventory will render it to be an inventory based model.[36] A plain reading of this shows that companies having an inventory based model will not be deemed as intermediaries, since they own the inventory and play an active role by directly selling to the customer. However, the ambiguity arises with respect to the marketplace based model of e-commerce. As per the FDI Guidelines, an e-commerce marketplace may provide support services to sellers in respect of warehousing, logistics, order fulfilment, call centre assistance, payment collection and other services, and facilitate payments for sale in accordance with the Reserve Bank of India guidelines in an arms-length manner.[37]

Notwithstanding this, the judgement in *Christian Louboutin* indicates that these factors would go to show that the platform is not an intermediary. However, this aspect of the judgement was in the context of Darveys, an inventory based e-commerce website which was not an intermediary in any case. Accordingly, the judgement should not be read to mean that safe harbour provisions cannot be availed by any e-commerce marketplaces facilitating such ancillary services, which they are permitted to do under the FDI Guidelines. The removal of intermediary status for marketplace e-commerce companies would effectively bring the industry to a halt, as appropriately pointed out by the Single Judge in *Kent RO Systems Ltd*.[38]

D. On the Heels of Christian Louboutin

Post the judgement in *Christian Louboutin*,[39] courts began to apply the principles enunciated therein even to e-commerce marketplaces (as opposed to the inventory based Darveys). In *L'Oreal* v. *Brandworld*,[40] as well as *Skullcandy* v. *Shri Shyam Telecom*,[41] the respective plaintiffs inter alia sued the proprietor of shopclues.com, an online marketplace, on the grounds that it was not entitled to safe harbour protection as its role was much more than that of an intermediary. The court observed that several factors, such as the disclosure of sellers' details on the invoice and website, the existence of a takedown policy for intellectual property infringement etc., pointed to the fact that it was an intermediary. However, several other features, such as a 100% authenticity guarantee, repeated sales of counterfeits, the conduct of

---

[35] FDI Guidelines – 2018 Series, para 5.2.15.2.2 (iii).
[36] FDI Guidelines – 2018 Series, para 5.2.15.2.4 (iv).
[37] FDI Guidelines – 2018 Series, paras 5.2.15.2.4 (iii) and (ix).
[38] *Kent RO* (n 26).
[39] *Christian Louboutin* (n 27).
[40] 2018 SCC OnLine Del 12309 : (2018) 254 DLT 433.
[41] 2018 SCC OnLine Del 12308 : (2019) 77 PTC 155.

the website in not taking measures to stop sales of counterfeits despite so many infringement actions, and the fact that the website had a 'replica' window which encouraged sellers to feature lookalikes/counterfeits, indicated abetment, which was certainly not condonable. Accordingly, the website was disqualified from exemption under Section 79 of the IT Act.

Inter alia, ShopClues was directed to seek the concurrence of the respective plaintiffs prior to uploading a product bearing the plaintiff's marks. Further, upon being made aware of any counterfeit product being sold, it was to notify the seller and take down the product, in case the seller was unable to provide evidence that the product is genuine.

Both these orders of the Single Judge were appealed.[42] The Division Bench held that the findings of the Single Judge that ShopClues was not an intermediary, and the observations of "*proliferation of counterfeits on ShopClues*", "*lack of preventive measures on behalf of ShopClues despite repeated infringement actions against it*" and "*its 'replica' window encourages sellers to post lookalike products*" were rendered without any evidence in this regard being led by the plaintiff, and without giving ShopClues an opportunity to challenge this evidence. ShopClues also averred that the replica window was not for counterfeit products but for replicas of non-protected products. The court ruled that a trial was necessary in the matter to come to a conclusion as to the intermediary status of ShopClues and restored both suits to the Single Judge for further proceedings.

Apart from this judgement, in *Luxottica Group SpA* v. *Mify Solutions (P) Ltd.*,[43] the Delhi High Court held that the e-commerce marketplace kaunsa.com was not a 'pure intermediary', even in the absence of striking factors such as a replica window. The court observed that factors such as the collection of payment on behalf of sellers and the provision of authenticity guarantees were sufficient to strip a platform of its intermediary status.

E. Conflicts with the Direct Selling Model

In *Amway India Enterprises (P) Ltd.* v. *IMG Technologies (P) Ltd.*,[44] the Single Judge of the Delhi High Court passed interim orders in several clubbed law suits filed by direct selling entities such as Amway, Oriflame and Modicare against e-commerce marketplaces such as Amazon, Flipkart,

---

[42] *Clues Network (P) Ltd v L'Oreal* 2019 SCC OnLine Del 7984 : (2019) 78 PTC 251 (*Clues Network*).

[43] 2018 SCC OnLine Del 12307 : (2019) 77 PTC 139.

[44] *Amway India Enterprises (P) Ltd v 1MG Technologies (P) Ltd* 2019 SCC OnLine Del 9061 : (2019) 260 DLT 690 (*Amway*).

Snapdeal, 1MG and Healthkart. The plaintiffs claimed that they distributed healthcare products through a 'direct selling model' whereby they entered into distributorship agreements with their network of direct sellers who were supposed to sell their products directly to the end customer, and were prohibited from selling these products either through retail stores or e-commerce marketplaces. Further, the plaintiffs claimed that their business was regulated by the Direct Selling Guidelines issued by the Central Government, as per which, direct sellers were prohibited from selling on e-commerce marketplaces without approval from the direct selling entities.[45] Therefore, the grievance of the plaintiffs was that e-commerce marketplaces were liable for tortious interference with their contracts by enabling the sale of the plaintiff's products through their platforms. This, they claimed, violated both their contracts with their direct sellers as well as the Direct Selling Guidelines (which they maintained were legally binding upon them) and caused huge financial losses to them and their direct sellers, apart from tarnishing their brand.

The Single Judge of the Delhi High Court held that the Direct Selling Guidelines were 'law' and that they were applicable not just to the direct sellers, but also to e-commerce marketplaces. The court ruled that even in case of genuine products, if the source was dubious or untraceable to the direct seller, such sales were unauthorised by the plaintiff. However, in order to sell on the platform, the seller must be an authorised seller, and have the consent of the trademark owner. Further, the court observed that as per the policies of the concerned platforms, unauthorised and tampered goods could not be sold. Since some instances of tampering were found in the premises of the sellers, the court concluded that the platforms were permitting the sale of tampered products. It held that the return policies and warranties offered by the platforms themselves constituted an impairment of the goods. It also noted that the use of the plaintiffs' trademarks by these platforms for advertising, promotion and meta-tagging to throw up search results was unjustified.

Similar to its stance in several previous cases, the court placed a great deal of significance on the value-added services provided by platforms such as transporting, delivering and advertising. In this context, the court held that the FDI Guidelines (and the definitions therein) would be considered only

[45] Advisory to State Governments/Union Territories on Model Guidelines on Direct Selling 2016, cl 7.6: Any person who sells or offers for sale, including on an e-commerce platform / marketplace, any product or service of a Direct Selling Entity must have prior written consent from the respective Direct Selling Entity in order to undertake or solicit such sale or offer.

once the 'actual role' of e-commerce marketplaces, i.e. active or passive, is established. The due diligence required from a platform would include setting up proper policies and performing takedowns upon receiving 'notice' from the brand owners. The platforms must also implement these policies in earnest, and non-compliance with the same would take them out of the ambit of safe harbour.

Interestingly, the court also held that the platforms were liable for tortious interference with the contracts between the plaintiffs and their direct sellers, since they allowed the sale of the plaintiffs' products despite allegedly being aware of these contracts. The platforms have an obligation to maintain the sanctity of contracts, and the very architecture of these platforms involved 'inducing' the direct sellers to violate their contracts. The court restrained platforms from selling the plaintiffs' products, except by those sellers who produce written permission/consent of the plaintiff, and instructed the platforms to take down any listings pointed out by the plaintiff in the interim within 36 hours.

This judgement further entangled the jurisprudence surrounding e-commerce marketplaces. Most importantly, the judgement continues to hold that e-commerce marketplaces are not 'passive platforms' because they carry out ancillary services, as discussed earlier. The court failed to appreciate that advertising and promotion are automated processes that do not involve human intervention, and are thus, not even within the knowledge of the intermediary purportedly performing such acts. Further, it placed an onus on e-commerce marketplaces to 'enforce' their policies on their users and defined 'due diligence' to mean pre-screening and policing of the platform. The threshold applied was that of 'notice' or a general awareness of the sale of infringing products, and not 'actual knowledge' (by means of a court order or government notification). Therefore, the obligations of policing the brand owner's trademarks, preserving the sanctity of the brand owner's or manufacturer's business model as well as enforcing contracts between the brand owner and other third parties were placed entirely on the platforms, with no efforts required from the brand owners or manufacturers.

F. The Appellate Court Clarifies

This order of the Single Judge in *Amway Enterprises*[46] was appealed in *Amazon Seller Services (P) Ltd.* v. *Amway India Enterprises (P) Ltd.*[47] and set aside. The Division Bench held that the Direct Selling Guidelines were

[46] *Amway* (n 44).
[47] 2020 SCC OnLine Del 454 : (2020) 267 DLT 228 (*Amazon Seller Services*).

only 'model guidelines' and could not be considered binding law. It also held that the established principle of exhaustion[48] was squarely applicable in the present matter, and that sellers on e-commerce platforms were free to re-sell any genuine and untampered products without the consent of the manufacturer or trademark holder. The court further held that the suits were not filed for trademark infringement or passing off, and that Oriflame and Amway were not even owners of their respective trademarks and were accordingly not entitled to these reliefs in any case.

Pertinently, the court held that the Single Judge misinterpreted Section 79 of the IT Act in concluding that it was applicable only to 'passive' intermediaries, since the legislation did not strike a distinction between active and passive intermediaries for safe harbour protection. Carrying forward its previous decision in *Clues Network*,[49] the court effectively set aside the dictum in *Christian Louboutin*[50] and held that the value-added services provided by marketplaces did not dilute their safe harbour protection as online marketplaces were expressly included in the definition of 'intermediaries' under the IT Act. The court acknowledged that the FDI Guidelines 2018 allowed marketplaces to provide these services, and that therefore, there was prima facie merit in the marketplace's contention that packaging and transporting products is not contrary to its role as an intermediary. With respect to tortious interference, the court held that the mere knowledge of contractual stipulations is insufficient to establish this tort and that active efforts on part of the e-commerce marketplace will have to be demonstrated to make a viable case for the same.

Finally, the court held that the evidence on record had several holes and did not prima facie prove that the platforms were tampering with products. The intermediary status of online marketplaces as well as their alleged tortious interference were questions of trial which could not be determined at the interlocutory stage. The case of the direct selling entities failed the tests of prima facie case, balance of convenience and irreparable loss and injury, necessary for obtaining an interim injunction, and thus, the order of interim injunction was set aside. This judgement provides some much-needed clarity in the context of intermediary liability for e-commerce marketplaces, especially with respect to the permissibility of value-added services. It also confirms that the principle of exhaustion will be applicable to e-commerce marketplaces and that sellers are free to sell any products in the interest of a free market. Further, it clarifies that sweeping observations on an

---

[48] *See*, *Kapil Wadhwa v Samsung Electronics Co Ltd* (2013) 53 PTC 112 (*Kapil Wadhwa*).
[49] *Clues Network* (n 42).
[50] *Christian Louboutin* (n 27).

e-commerce marketplace's intermediary status cannot be made on the basis of extraneous factors, and that the same must be decided after a trial.

IV. Proposed Amendments to the Intermediary Liability Regime Pertaining to E-Commerce

A. Draft Information Technology Intermediaries Guidelines (Amendment) Rules, 2018[51]

The Draft Information Technology Intermediaries Guidelines (Amendment) Rules, 2018 ('**the Rules**') largely pertain to the cooperation of intermediaries with law enforcement agencies. The Rules suggests the removal of Rule 3(4) of the Intermediaries Guidelines[52] and instead proposes a new Rule 3(8), whereby intermediaries will be required to takedown information relatable to Article 19(2) in the interests of the sovereignty and integrity of India, public order, decency, morality, defamation etc., upon receiving a court order or being notified by the appropriate government. In contrast, as per the proposed Rule 3(9), intermediaries are required to deploy 'technology-based automated tools' or 'appropriate mechanisms' to proactively identify and remove or disable public access to 'unlawful information or content'. The term 'unlawful information or content' is vague as it is neither defined in the IT Act nor the Rules, and thus, the scope of the intermediary's duty in this regard is ambiguous. This term also implies that the burden of adjudicating what is 'unlawful' falls upon automated technology developed and used by private actors, which could result in arbitrary takedowns of content.[53]

The implementation of this rule will likely lead to a takedown 'overdrive' as the intermediary will have a strong incentive to takedown even lawful content by way of abundant caution to avoid costly legal proceedings.[54] This

---

[51] *See*, the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 (Intermediaries Rules 2018).

[52] Intermediaries Rules 2018, r 3(4): The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes.

[53] *See*, Gurshabad Grover and others, 'Response to the Draft of The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018' (*The Centre for Internet and Society*, 31 January 2019) <https://cis-india.org/internet-governance/resources/Intermediary%20Liability%20Rules%202018.pdf> accessed 13 November 2019.

[54] *See*, Rishabh Dara, 'Intermediary Liability in India: Chilling Effects on Free Expression on the Internet' (*The Centre for Internet and Society*, 10 April 2012) <https://cis-india.org/

tendency can in turn lead to 'censorship by proxy' and have a chilling effect on free speech as well as free trade (in the context of e-commerce).[55] As per this rule, e-commerce intermediaries would be expected to carry our proactive sweeps of their portals, hire teams for the said monitoring and essentially undertake the burden of enforcing the trademarks of brand owners, which is completely contrary to the set principle that it is the onus of the proprietor to enforce his own trademarks. With Rule 3(4) removed, there will be no scope for the 'affected person' (brand owner) to write to the intermediary and demand takedowns of infringing content within 36 hours. While pro-active monitoring for intermediaries may be justified with respect to issues of grave public importance, such as pre-natal sex determination,[56] the same threshold cannot be applied to trademark infringement on e-commerce websites, which involves the proprietary rights of brand owners.

Even though intermediaries such as YouTube employ automated video identification technology known as Content ID,[57] these automated tools are highly capital intensive[58] and will act as a major barrier to entry for homegrown start-ups in the e-commerce space. Further, it is yet to be seen how feasible these tools will be once online marketplaces begin to carry out such assessments for hundreds and thousands of trademarks from across the world.[59] Additionally, the accuracy of automated technologies is not yet widely known, and there exists little clarity on both accountability in case of failure and oversight of decisions made by these automated tools.[60]

---

internet-governance/intermediary-liability-in-india> accessed 13 November 2019.

[55] Grover (n 53) 20; *See*, Seth F Kreimer, 'Censorship by Proxy: the First Amendment, Internet Intermediaries, and the Problem of the Weakest Link' (2006) 155 University of Pennsylvania Law Review 11.

[56] *See*, *Sabu Mathew George v Union of India* (2018) 3 SCC 229 : AIR 2018 SC 578. Here, the Supreme Court directed search engines such as Google, Yahoo and Bing to auto-block advertisements for pre-natal sex selection as an interim measure.

[57] 'How Content ID works' (*YouTube*, 30 September 2015) <https://support.google.com/youtube/answer/2797370?hl=en-GB> accessed 13 November 2019.

[58] Nehaa Chaudhari, 'View: Draft e-commerce policy will wreak havoc on Indian startups' *The Economic Times* (Mumbai, 16 March 2019) <https://economictimes.indiatimes.com/news/economy/policy/view-draft-e-commerce-policy-will-wreak-havoc-on-indian-start-ups/articleshow/68432844.cms> accessed 13 November 2019.

[59] Suneeth Kartaki and others, 'India: Comments On The Draft National E-Commerce Policy' (*Mondaq*, 23 April 2019) <http://www.mondaq.com/india/x/801170/international+trade+investment/Comments+On+The+Draft+National+ECommerce+Policy> accessed 13 November 2019.

[60] Grover (n 53).

B. Draft National E-Commerce Policy, 2019[61]

The Department for Promotion of Industry and Internal Trade released the Draft National E-Commerce Policy ('**the Draft Policy**') for public consultation and comments in February 2019. The primary objective of the Draft Policy is leveraging the benefits of the digital economy and creating a regulatory framework for various stakeholders, in addition to securing data privacy, consumer protection and the promotion of a level playing field for micro, small and medium enterprises and start-ups.[62]

Chapter III (C) of the Draft Policy pertains to counterfeiting and requires e-commerce entities to disclose seller details, ensure that sellers provide an undertaking as to the genuineness of their goods, and provide financial disincentives to sellers found selling counterfeit products. These measures are reasonable and will help to disincentivise the sale of counterfeit products online. Further, in line with the decision in *Christian Louboutin*[63] and its successive judgements, the Draft Policy lays down that trademark owners shall have the option to register themselves with e-commerce platforms, which must inform trademark owners whenever a product bearing their trademark is uploaded for sale.[64] Moreover, in case brand owners so desire, e-commerce platforms shall not list or offer for sale any of their products without prior concurrence.[65]

Additionally, in case of 'high value' goods, cosmetics and goods having an impact on public health, marketplaces will be required to seek the authorisation of trademark owners before even listing the product.[66] As per the Draft Policy, although the post-sale delivery of goods is the responsibility of the seller, in case a customer makes a complaint to the effect that the product is a counterfeit, marketplaces will be liable to return the amount paid by the customer, and to cease to host the counterfeited product on their platforms.[67] Marketplaces will also have to inform the brand owner of the said complaint within 12 hours of its receipt, and takedown the listing if the seller is unable to provide evidence that the product is genuine.[68]

---

[61] *See*, Draft National e-Commerce Policy 2019 <https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf> accessed 13 November 2019.

[62] 'National E-commerce Policy, 2019 – Draft' (*PricewaterhouseCoopers*, 26 February 2019) <https://www.pwc.in/assets/pdfs/news-alert-tax/2019/pwc_news_alert_26_february_2019_national_ecommerce_policy_draft.pdf> accessed 13 November 2019.

[63] *Shreya Singhal* (n 19).

[64] Draft National e-Commerce Policy 2019, para 3.4.

[65] Draft National e-Commerce Policy 2019, para 3.12.

[66] Draft National e-Commerce Policy 2019, para 3.13.

[67] Draft National e-Commerce Policy 2019, para 3.16.

[68] Draft National e-Commerce Policy, para 3.14.

Several of these aspects of the Draft Policy are problematic for the following reasons. *First*, the Draft Policy does not differentiate between e-commerce entities that are marketplace based and those that are inventory based. In fact, the policy effectively removes intermediary protection for all e-commerce platforms, by requiring them to play a more active role, in clear violation of the Intermediaries Guidelines.[69] *Second*, it promotes trade channel monopolisation by allowing brand owners to choose where their products will be sold, which is contrary to Section 30(3) of the Trade Marks Act, 1999. This also violates the principle of exhaustion, as per which the trademark owner's rights are exhausted once the goods are put into the market, and the consent of the trademark owner for reselling of goods (unless impaired) is implied.[70] *Third*, it carves out a different set of rules and creates a monopoly for certain kinds of products, such as 'high value' products without defining the term or setting any threshold of price of the product. Similarly, 'goods having an impact on public health' is also not defined, and could potentially include all drugs, tonics, supplements and food items. *Fourth*, the Draft Policy includes trademark licensees in the definition of 'trade mark owners' and gives them equal rights to enforce the trademarks, which is contrary to Section 28(1) of the Trade Marks Act, 1999, wherein only trademark owners have the right to obtain relief in respect of infringement. *Fifth,* it fails to account for the practical working of e-commerce marketplaces, where the sellers themselves create listings of products, and it is thus not feasible to have the intermediary take permission from brand owners before listing products, as such an arrangement would be nearly impossible to implement, as discussed above. *Sixth*, it discriminates between physical retail hypermarkets and e-commerce marketplaces, since the former is not required to seek any authorisation from the brand owner or take products off its shelves on the basis of a single customer complaint as to counterfeiting.

If the Draft Policy comes into effect, it will severely choke the rising success of e-commerce in India. The capital-intensive regulatory compliances required to pro-actively police counterfeiting, coupled with the shrinking list of products that e-commerce marketplaces are actually allowed to sell due to interference from brand owners, will ensure the decline of this otherwise thriving industry. Further, it will lead to a situation where e-commerce

---

[69] Asheeta Regidi, 'Draft E-Commerce Policy: A Problematic Revision Of Intermediary Rules For Trademark And Copyright Liability' *FirstPost* (Mumbai, 28 February 2019) <https://www.firstpost.com/tech/news-analysis/draft-e-commerce-policy-a-problematic-revision-of-intermediary-rules-for-trademark-and-copyright-liability-6168921.html> accessed 13 November 2019.

[70] *Samsung Electronics Co Ltd v G Choudhary* 2006 SCC OnLine Del 1038 : (2006) 33 PTC 425; *Kapil Wadhwa* (n 48).

marketplaces 'over-comply' with takedown requests so as to eliminate the risk of falling short of their due diligence obligations, as discussed above.

The Draft Policy is also facing severe resistance from sellers. In response to the draft, the All India Online Vendors Association claimed that levying fines against sellers for counterfeiting was a one-sided affair and demanded a dispute redressal mechanism for these allegations. It also demanded the opportunity for sellers to prove their innocence in a court of law, instead of making the marketplace the jury and executioner.[71] Several aspects of the Draft Policy will require reconsideration in line with the recent decision of the Division Bench in *Amazon Seller Services*[72] which expressly upholds the principle of exhaustion even for nutraceuticals and cosmetic products, and states that the balance of convenience must be maintained without adversely impacting e-commerce.

C. E-Commerce Guidelines for Consumer Protection, 2019[73]

In August 2019, the Department of Consumer Affairs published a draft advisory to states on guiding principles for e-commerce businesses to prevent fraud and unfair trade practices, and protect the legitimate rights and interests of consumers in the business-to-consumer space. Under this draft framework, 'e-commerce entities' is defined to include inventory or marketplace models or both.[74] An inventory based model of e-commerce is defined as "*an e-Commerce activity where inventory of goods and services is owned by e-Commerce entity and is sold to the consumers directly*" whereas marketplace based model is defined as "*providing of an information technology platform by an e-Commerce entity on a digital & electronic network to act as a facilitator between buyer and seller.*"[75] While both these models are defined in the draft, all obligations therein are applicable to 'e-commerce entities'. No distinction is made between the roles of players following different models.

---

[71] Asmita Dey, 'E-commerce policy: Vendors want changes in anti-counterfeiting measures' *Financial Express* (Uttar Pradesh, 28 February 2017) <https://www.financialexpress.com/industry/e-commerce-policy-vendors-body-wants-changes-in-anti-counterfeiting-measures/1500787/> accessed 13 November 2019.

[72] *Amazon Seller Services* (n 47).

[73] *See*, Model Framework for Guidelines on e-Commerce for Consumer Protection 2019 <https://consumeraffairs.nic.in/sites/default/files/file-uploads/latestnews/Guidelines%20on%20e-Commerce.pdf> accessed 13 November 2019 (E-Commerce Guidelines for Consumer Protection).

[74] E-Commerce Guidelines for Consumer Protection, guideline 2(c).

[75] E-Commerce Guidelines for Consumer Protection, guidelines 2(g) and (i).

As per these guidelines, an e-commerce entity must provide details about the sellers on its website, including their name, address, email address, and how they can be contacted by customers.[76] E-commerce entities are not permitted to directly or indirectly influence the price of goods and must maintain a level playing field.[77] Further, they may not falsely represent themselves as consumers and post fake reviews or exaggerate the quality or features of the products.[78] An e-commerce entity must also ensure that advertisements are consistent with the actual characteristics of goods and services, and should mention safety and healthcare information relating to the goods and services advertised for sale.[79] This too, raises pragmatic concerns, since most e-commerce platforms do not list products themselves, and all related acts are undertaken by the seller.

Pertinently, if an e-commerce entity is informed by a consumer or comes to know by itself or through another source about any counterfeit being sold on its platform, and is satisfied after exercising due diligence, it shall notify the seller, and if the seller is unable to provide any evidence that the product is genuine, it shall takedown the said listing.[80] These directions seem rather vague, as it is not clear how an e-commerce marketplace would come to know about counterfeiting 'by itself', what 'due diligence' means in this context, and whether a mere customer review would burden the e-commerce marketplace with initiating a probe into the actual quality of goods.

The draft also proposes to hold an e-commerce entity guilty of contributory or secondary liability if it makes assurances about the authenticity of the goods sold on its marketplace or guarantees that the goods are authentic.[81] In this regard, it is important that a clarification be issued distinguishing between a seller making assurances about the authenticity of its product on the product display page, and the e-commerce marketplace itself making these claims in its policies. Further, the terminology used misses out a critical distinction between the legal definition of 'guarantee' and 'warranty'. A guarantee is a tripartite contract where the guarantor is by definition not the principal. It only amounts to a promise that in case the product eventually turns out to not be genuine, the guarantor will ensure that the customer is provided with a genuine product. On the other hand, a warranty means that the person providing the warranty, i.e. the seller, specifically vouches for

---

[76] E-Commerce Guidelines for Consumer Protection, guideline 3(vi).
[77] E-Commerce Guidelines for Consumer Protection, guideline 4(i).
[78] E-Commerce Guidelines for Consumer Protection, guideline 4(iii).
[79] E-Commerce Guidelines for Consumer Protection, guideline 4.
[80] E-Commerce Guidelines for Consumer Protection, guideline 4(ix).
[81] E-Commerce Guidelines for Consumer Protection, guideline 4(x).

the authentic nature of that particular product. Accordingly, authentication guarantees are provided by parties that are not the principal and as such, cannot take an e-commerce marketplace outside the ambit of an intermediary. Finally, this clause proposes imposing 'contributory or secondary liability' upon e-commerce marketplaces, whereas the Trade Marks Act, 1999 (unlike the Copyright Act, 1957) does not contain any provisions for secondary or contributory liability.

V. Conclusion and Steps Ahead

It is a tumultuous time for the Indian e-commerce industry. Although e-commerce platforms can breathe a sigh of relief after the clarifications issued in *Amazon Seller Services*,[82] there are still several ambiguities in the regime for intermediary liability in e-commerce that require more consideration. In this judgement as well, the court held that the intermediary status of an e-commerce marketplace will be determined after its role is ascertained at trial. This appears inconsistent with the IT Act, wherein an e-commerce marketplace is deemed to be an intermediary by definition. The purpose of a trial therefore should be to be establish whether the said intermediary is entitled to safe harbour or not. It may be adjudicated, after trial, that the intermediary was conspiring, aiding or abetting a crime, or that it failed to perform takedowns upon receiving actual knowledge of infringement in terms of Section 79(3), and accordingly, that it cannot avail safe harbour as provided in Section 79(1). Further, as discussed above, full-fledged trials in such cases are yet to be carried out and thus, there exists a lack of clarity as to the factual thresholds that a court may use to determine the intermediary status of an e-commerce marketplace.

While the crusade against counterfeiting is noble in origin, any law or policy drafted with respect to the same should be proportionate and must not come at the cost of choking a free market or the rights of small businessmen and entrepreneurs to carry on with their business. In light of this, the author proposes the following self-regulatory mechanism to effectively tackle counterfeiting on e-commerce marketplaces:

i. In the interests of a free market, no prior concurrence with brand owners should be required and e-commerce marketplaces as well as their sellers must be free to sell genuine products bearing any trademarks in line with the decision in *Amazon Seller Services*.[83]

[82] *Amazon Seller Services* (n 47).
[83] *Amazon Seller Services* (n 47).

ii. In order to retain the sanctity of the intermediary status of e-commerce marketplaces, they should not be mandated to pro-actively police their platforms for counterfeits, as the said due diligence must be carried out by brand owners. At the very least, compulsory deployment of technology-based automated tools to track counterfeits should be limited only to e-commerce companies above a certain net worth and size in a phased manner, so as to not act as an entry barrier for homegrown e-commerce companies. Further, the efficiency and accuracy of these automated tools must be ascertained in order to prevent a chilling effect on free trade.

iii. E-commerce marketplaces should obtain warranties and guarantees from their sellers that the products offered for sale are authentic.

iv. Since brand owners cannot reasonably be expected to go to court to procure orders for the takedown of each counterfeit product, e-commerce marketplaces should accept takedown notices from brand owners.

v. E-commerce marketplaces must takedown listings pointed out by brand owners without any evidentiary requirements in case of identical trademarks and copyright related matters, within 36 hours of intimation as prescribed under the Intermediaries Guidelines, provided that the brand owner undertakes that the takedown requests are bona fide and correct. This will ensure the expeditious takedowns of infringing listings without unduly expecting the brand owner to prove infringement at every instance in a tedious and time-consuming manner.

vi. Subsequent to takedowns, e-commerce marketplaces must intimate the seller that the listing has been taken down. After temporarily disabling access to the allegedly infringing product, notice must be given to the seller, along with a deadline to respond, so that the seller has an opportunity to prove its innocence. If the marketplace is satisfied with the explanation of the seller, the product may be reinstated with notice to the brand owner, providing reasons. An in-house appeal mechanism may also be instituted. This will ensure that the implementation of takedowns is balanced, and substantially reduce the probability of a takedown overdrive by intermediaries in order to avoid legal proceedings, the dangers of which have been discussed above.

vii. In case a brandowner is found to be repeatedly demanding takedowns of genuine products/parallel imports with the intent to create a trade

channel monopoly, the burden of proof may be shifted to the brand owner to prove that the listings pointed out are in fact, counterfeit. This will ensure that brand owners do not attempt to create a market monopoly by stopping lawful trade and maintain a free market in line with the principle of exhaustion as laid down in *Kapil Wadhwa*.[84]

viii. With respect to sellers, repeat offenders must be delisted or blocked from the platform entirely. In such cases, a 'three-strike policy' (for sellers who have been found guilty of selling counterfeits thrice) or similar mechanism may be instituted. By doing so, marketplaces will disincentivise the sale of counterfeit products on their platform and also ensure that infringing products are not repeatedly re-listed by the seller upon takedown.

ix. In case the allegations made by a brand owner are inconclusive and the intermediary is of the opinion that it is not a prima facie case of counterfeiting, it should be allowed to ask the brand owner to obtain an order from a court of law before delisting the product. In such cases which are not instances of blatant counterfeiting on bare comparison (as in the case of copyright concerning alleged fair use, design infringement, patent infringement, trade dress violations, refurbished goods, deceptively similar trademarks etc.), the marketplace should not be held liable for its failure to delist the product, even if the court subsequently determines that there is infringement. This will ensure that the marketplace does not assume an adjudicatory role in determining what constitutes infringement, in line with the dictum in *Shreya Singhal*.[85]

x. Consumer rights groups and government bodies should be encouraged to actively engage with e-commerce marketplaces to report counterfeit goods. In doing so, consumer interests will be protected even in cases where the brand owner fails to enforce its trademark or take steps to remove infringing products from the e-commerce marketplace.

[84] *Kapil Wadhwa* (n 48).
[85] *Shreya Singhal* (n 19).

The Conundrum of 'Relevant Market': Market Definition in India's Complex TV Distribution Business

Vibodh Parthasarathi[*]

Abstract *The universal problematic of market definition poses peculiar challenges in multi-lingual and fragmented media markets, like in India. This article engages with this problematic by taking up the case of the TV distribution market in India. Here, the rapidly expanding TV distribution business consists of two segments. The larger, wired Cable distribution segment, driven by over 1,000 large cable companies and over 50,000 last mile operators, accounts for 70 percent market share, or around 100 million TV homes. The rest 30 percent is occupied by the wireless segment, comprising 6 Direct to Home TV distributors. Amidst the heightened expansion of the TV distribution business during the last decade, we notice a series of cases at the Competition Commission of India (CCI) pertaining to 'relevant market'. This paper provides a critical appraisal of CCI's engagement with ideas of relevant geographical market and relevant product market during the first five years of such matters coming to it, i.e. between 2011 and 2015. Focussing on core concepts deployed in debating relevant markets, viz. substitutability and service area, the paper unravels conceptual and methodological challenges provoked by market definition in complex media landscapes such as India.*

[*] Associate Professor, Centre for Culture, Media and Governance, Jamia Millia Islamia, New Delhi. This paper emerged from research under my project 'Tracking Access under Digitalisation', supported by the Ford Foundation. For research assistance at various times, I am in gratitude to Shruti Ravi, Shradha Nigam, Mohit Kalawatia and, importantly for this version, Rajashri Seal. Thanks also to Maria Michalis for comments on an initial draft, and to the Institute for Communication Arts and Technology, Hallym University, Chuncheon (South Korea) for inviting me to present an earlier version. I appreciate comments by the two anonymous reviewers, and support from Nikhil Purohit in streamlining the references.

I. Introduction

In January 2019, the Competition Commission of India approved two subsidiaries of Reliance acquiring majority stake in two of the three largest Cable TV distributors, Hathway and DEN.[1] This spurred anxieties across both segments of the TV distribution business, viz. in the segment of 'wired' or Cable distribution and in the relatively smaller segment of 'wireless' or Direct to Home ('**DTH**') distribution. Their anxieties stemmed from the near-monopolistic situation arising from these giant acquisitions by Reliance in the overall TV distribution business--- that is, in the market for retailing TV channels. These anxieties were enhanced on count of Reliance, India's biggest industrial conglomerate, also controlling wide interests in the TV broadcast business--- that is, in the market for producing TV channels. However, the Competition Commission of India ('**CCI**') did not see Reliance's large inorganic expansion into the TV distribution business carrying risks of market dominance in that business. The crux of CCI's argument was that the businesses of Cable distribution and DTH distribution operate in the same 'relevant product' market[2]--- that is to say, they distribute substitutable products. CCI was suggesting that arguments of market dominance by an entity in India's TV distribution business must consider its share in both the Cable business and in the DTH business. It thus opined the market share of Reliance, despite acquiring two of the three biggest companies in the Cable segment, did not indicate its dominance in the 'relevant market' of TV distribution--- which it felt was an amalgamation of the Cable and the DTH segments.

Rather than further reasoning, or contesting, the wisdom of CCI's judgement, there is another purpose to invoke this case at the outset of this essay. The CCI's wisdom makes us ponder over two, often intertwined, problematics debated globally in media policy studies, competition law, and in media economics. The first is at the empirical level, about enumerating 'dominance' in a media market; and thus, whether the combined market share of the Reliance subsidiaries, if taken as one actor operating in the market, dominate the Cable business. The second problematic is at the conceptual level, and therefore more fundamental, about defining 'the market' where such

[1] Competition Commission of India (Combination Registration Nos. C-2018/10/609 and C-2018/10/610) 21 January 2019.
[2] ibid 7.

dominance is alleged. It raises the question whether the TV distribution business in India, comprising two different, technologically-defined segments, can be construed as one uniform and singular market. This essay delves into the second problematic, that of the very conception of market definition---commonly termed as the problematic of relevant market. The essay explores this in the context of the dynamic business of TV distribution in India.

II. The Context: The Business of TV Distribution

The TV landscape in India reflects the legacy of the country's mixed economy. On the one hand, the state continues its monopoly over broadcasting (TV channels) in the Terrestrial mode. Viewers do not pay to receive such TV channels, which is why terrestrial transmission of government-owned TV channels is referred to as 'free-to-air' broadcasting. On the other hand, viewers pay to receive private-owned TV channels transmitted in the Cable and Satellite mode. This business of Cable and Satellite TV ('**C&S TV**') comprises two sectors: one, the TV broadcast sector which consists of the market for producing and broadcasting TV channels; and secondly, the TV distribution sector which entails the market for distributing and retailing TV channels.

Two aspects of this commercially and technologically hybrid TV milieu are important to point out here, since they bear on conceptions of market definition.

One, TV distribution takes place through two technologically different ways: through wired networks, commonly referred to as Cable operations, and through wireless networks, widely termed as Direct-to-Home operations.[3] Thus, the TV distribution sector of the overall C&S TV business comprises two different segments, that of Cable and DTH. While Cable operations account for 58 percent share of the overall TV Distribution sector---around 103 million TV homes---the rest is occupied by DTH operations.[4] The Competition Commission of India was confronted to address whether these two technologically distinct segments of the TV distribution business signified two separate relevant markets, or represented one integrated market.

---

[3] The introduction of wireless distribution through DTH operations in 2006 expanded access to C&S TV in two significant ways. It enabled access in geographically remote areas, which wired Cable distributors were unable to service, as also to demographically sparse areas, which Cable distributors found cost ineffective to service.

[4] Telecom Regulatory Authority of India, 'Annual Report 2018-2019' (November 2019) 31.

Secondly, regulatory stipulations require TV distributors to carry, besides private C&S TV channels, a minimum number of government owned terrestrial TV channels. Consequently, there appear to be two audience markets in India's TV business--- audience receiving only government TV channels in the free to air terrestrial mode, and those receiving private C&S TV channels and government TV channels provided by the TV Distributor they subscribe to. This, in turn, seems to create two markets for advertising--- a contention the Competition Commission of India was obliged to grapple with.

Over the last 15 years, revenues in TV Distribution sector, realised from subscriptions by viewers, have expanded tremendously. Their growth has been steady and at higher rates than the growth of revenues in the TV Broadcasting sector, realised overwhelmingly from advertising. Yet, TV Distribution remains a far less studied area than TV Broadcasting. Very little is known about the workings of wholesale and retail markets in distribution, the impact of regulatory interventions on this sector of the TV business, evolving ownership patterns and market structure, and about interactions between the subscriber-audience and distributors.

In the value chain of C&S TV distribution, the principal entities are multi-system operators ('**MSOs**') which aggregate signals from numerous broadcasters and relay them across large areas. Although MSOs are licensed at the national level,[5] many are often called 'regional' since they operate either within a state or in contiguous states. A handful are referred to as 'national', like Hathway and DEN (now controlled by Reliance), since their operations spread across many, non-contiguous states. Below the MSOs in the value chain are small Cable distributors called last-mile operators ('**LMOs**'); they relay signals acquired from MSOs to the homes of subscribers of C&S TV. Typically, MSOs exercise market power in negotiations with the LMOs, on the one hand, and with the broadcasters on the other. They leverage their accumulated interests to bargain with broadcasters for content at a lower price, while also demanding higher carriage and placement fees to carry channels. Often leveraging this, MSOs are simultaneously able to offer better revenue share to LMOs, as also dangle incentives for LMOs to move away from smaller MSOs or large independent Cable distributors and align with larger MSOs.

[5] MSOs require a license whose criteria include, irrespective of their area of operation, the applicant entity having a minimum net worth; in contrast, the commercially far smaller and spatially localised LMOs have not attracted any licensing or financial stipulations, and are only required to register themselves at the nearest Post Office.

The mandatory digitalisation of Cable, introduced through legislation in 2011 and rolled out in 5 phases,[6] led to Cable operators being able to relay more channels, provide on-demand pay-per view programmes, and offer bi-directional services, such as broadband internet. Early evaluations reveal mandatory digital migration playing out unevenly across cities, and across social strata within a city.[7] While the move from analog to digital Cable in large (Tier 1) cities like Delhi, compared to say Tier-2 cities like Patna, began much before mandatory digitalisation was legislated, in both cases digital migration was slow among low income households.[8] Since digitalisation required incremental investments from MSOs and LMOs, many Cable operators who could not afford this exited, making this sector of the TV market less long tailed. As a result, today over 1000 MSOs exist--- down from over 5000 before mandatory digitalisation commenced. More significantly, 15 large MSOs control over 75 percent share of the Cable distribution market.[9] On its part, estimates on LMOs remain unclear since the Ministry of Information and Broadcasting ('**MIB**') has never released, perhaps never bothered to collect, a list of Cable operators registered at post offices across the country; all we have are 'industry estimates' that have for a decade been hovering around 50,000. But these numbers have reduced post mandatory digitalisation, since many LMOs sold out to, or became franchisees of, large MSOs in urban India.[10] At the same time, in some cities MSOs came to garner more than 80 percent of the Cable business; while in some states, a single entity came to acquire several MSOs and LMOs.[11]

Apart from Cable, the other segment of the TV distribution business consists of DTH operators who account for 72 million subscribers, or about 42 percent of the TV Distribution sector.[12] Being a wireless service, DTH operators are able to distribute TV signals all across the country, thus enabling them to have a national 'footprint', or area of operation. In sharp contrast to Cable, the public broadcaster had commenced its own DTH service; being rent-free is one reason why its users, initially limited to marginal social

---

6 The Cable Television Networks (Regulation) Amendment Act 2011.

7 Vibodh Parthasarathi, Arshad Amanullah, and Susan Koshy, 'Digitalization of TV Distribution: Some Findings on Affordability & Availability' (2016) 51(34) Economic and Political Weekly 20 August, 23-26.

8 ibid 25.

9 Telecom Regulatory Authority of India, 'White Paper on The Telecommunication (Broadcasting and Cable) Services: Benefits of 'New Framework' for Small MSOs' (23 April 2019) 12.

10 Vibodh Parthasarathi, Arshad Amanullah, and Susan Koshy, 'Digitalization as formalization: A view from below' (2016) 7(2) International Journal of Digital Television 155.

11 Telecom Regulatory Authority of India, 'Consultation Paper on Monopoly/Market Dominance in Cable TV Services' (3 June 2013).

12 TRAI (n 4) 31.

strata and geographically remote pockets, have been expanding over the past years.[13] Private DTH operators, unlike Cable operators, were obliged to seek a license. At its peak, there were 8 private DTH operators, which have since reduced to 5 due to consolidation. Like in Cable after mandatory digitalisation, different DTH operators have been using set top boxes of different technical specifications (compression and encryption)--- a regulatory lacunae which makes these competing wireless TV distribution services non-interoperable, a matter also noted by CCI and which we will return to.[14] This compels subscribers to bear migration costs to a rival DTH operator if services of the incumbent are found wanting.

This reminds us of the significant risks prevalent in TV Distribution in India.[15] In the context of this essay, four such risks are important to highlight. First, the regulatory cap of 20 percent vertical integration between an MSO/DTH operator and a C&S TV broadcaster has been widely circumvented by exploiting legal loop holes in the Companies Act, despite its revisions in 2013. This has resulted in leading TV distributors to cross-own and/or control TV Broadcasters (and vice versa) through subsidiaries, step-down subsidiaries, and group companies.[16] Second, LMOs had historically carved out their local areas of operation, leaving C&S TV homes no choice but to subscribe to Cable relays of the LMO ruling a particular locality[17]--- unless they chose to subscribe to DTH services. While one of the regulatory aims of mandatory digitalisation was to provide choices to subscribers of C&S TV, the effective monopoly of LMOs in the last-mile has curtailed subscribers to choose between Cable and DTH--- and not between competing Cable services. This brings us to the third risk, that arising out of the lack of inter-operability between set top boxes of competing DTH operators--- despite the sectoral regulator, TRAI, repeatedly emphasising DTH licensing conditions mandate such a provision.[18] Consequently, unless subscribers invest in set

---

[13] Aloke Thakore and Sevanti Ninan, 'When the Dish Knocked Down the Antenna', (2016) Working Papers id:10554 eSocialSciences <https://ideas.repec.org/p/ess/wpaper/id10554.html> accessed 13 June 2020.

[14] For a snapshot of different formats adopted by leading DTH vendors, *see* Vibodh Parthasarathi and others, *Mapping Digital Media: India* (The Open Society Foundations, London) 89, Table 16 <https://www.opensocietyfoundations.org/reports/mapping-digital-media-india> accessed 13 June 2020.

[15] These risks are important to recognise since the distribution sector is widely considered as '*the key locus of power and profit*' in content industries; Nicholas Garnham, *Capitalism and Communication: Global Culture and the Economics of Information* (Sage, 1990) 162 (original italics).

[16] Parthasarathi and others, 'Mapping Digital Media: India' (n 14) 8.

[17] Veena Naregal, 'Cable communications in Mumbai: Integrating corporate interests with local and media networks' (2000) 9(3) Contemporary South Asia 289.

[18] Telecom Regulatory Authority of India, 'Recommendations on Licensing Issues Related to DTH' (25 August 2006).

top boxes of competing DTH operators, they are locked-in with incumbent ones. This then makes the DTH segment bereft of perfect competition. This phenomenon, together with the effective monopoly of LMOs, conveys the nature of competition characterising TV distribution as a whole being rather alarming. The fourth risk is that of rampant political ownership in the Cable business. Since Cable relays entail the laying of wires across neighbourhoods and pockets of city, and engender local information environments, politicians have congenitally been drawn to this business--- as partners/investors in the business of LMOs/MSOs, or as Cable entrepreneurs themselves.[19] Political ownership/control of Cable operations has commonly led to the relay of particular TV channels/programs being blocked when the programmes they carry threaten or unmask the interests of concerned politicians or their political parties.[20] Elsewhere I have reasoned the persistence of such risks in terms of the 'considered silence' characterising TV regulation in India--- i.e. the wilful non intervention of the state despite the social risks evident in the behaviour of market and extra-market actors.[21]

Our overview of the core traits of the Cable and DTH segments hints at the many conflicts we may expect in the fast expanding but cut-throat distribution business. Equally, and often consequently, this would indicate the many reasons why engaging with the idea of relevant market could be determinate of the health of India's TV distribution business. While there have been periodic concerns about market power in this business, systematic examination of this methodologically necessitates grappling first with the conundrum of 'relevant market'. Last but not the very least, since digitalisation enables MSOs to additionally offer broadband services, debates on market definition in the TV distribution business are crucial to concerns in this segment of India's online economy--- a business which prior to mandatory digitalisation was effectively distinct from the TV Distribution business.

---

[19] Vibodh Parthasarathi, and Alam Srinivas, 'Problematic Ownership Patterns: The Evolution of the Television Distribution Networks in India' (2019) 54(12) Economic and Political Weekly 23 March 2019.

[20] For instance, *see* Padmaja Shaw, 'Public Sphere and the Telangana Movement', (2014) 152(1) Media International Australia 143; Maya Ranganathan, 'Television in Tamil Nadu Politics' (2006) 41(48) Economic and Political Weekly 2 December 2006.

[21] Vibodh Parthasarathi, 'Between Strategic Intent and Considered Silence: Regulatory Imprints in the TV Business' in Adrian Athique, Vibodh Parthasarathi and S.V. Srinivas (eds) *The Indian Media Economy* (vol 1, Oxford University Press, 2018).

III. The Setting: Institutional Contexts of Market Definition

The intriguing silence in India on regulatory protocols on market share and on an agreed understanding of 'market definition' has ignited a glut of disputes over abuse of competition and market power in the TV distribution sector. These disputes have involved all types of players in the TV distribution business viz. private and public DTH operators, LMOs of different sizes, and regional and national MSOs. Typical disputes coming to the Competition Commission of India (CCI) have been between MSOs and LMOs, between MSOs and DTH operators, between one or more MSO/DTH operator and one or more broadcasters. In adjudicating over these disputes, the CCI has had to repeatedly grapple with the conundrum of 'relevant market'--- the field where a situation for abuse of market power may occur, and which hence requires accurate conception before commencing to resolve disputes in the competitive milieu.

Market definition serves as an analytical tool to identify competitive constraints; clearly defining the relevant market helps identify products/services whose suppliers are capable of exerting effective competitive pressures and constraining each other's behaviour.[22] In short, market definition helps in assessing the competitive constraints a firm faces. This led policy scholars to see demand substitution being the single most important factor to define a market as a market in itself.[23] This is particularly important towards grappling with the dynamics of the TV broadcasting and distribution business in India since its market is demarcated as much by products---i.e. TV programmes in a *particular* language---as it is defined by geographical boundaries, i.e. based on the spatial operations of LMOs and MSOs but also of specific regional offerings by DTH operators. Consequently, in understanding conceptions and rationales of market definition this paper finds itself engaging with the key economic, organisational, and technological traits of the business of TV distribution in India.

In India, the concept of relevant market was defined in the Competition Act, 2002, which also established the Competition Commission of India in 2009. The CCI was set up as a quasi-judicial body with the purpose of preventing practices having an adverse effect on competition, promoting and

[22] European Commission, 'Market Definition in the Media Sector- Economic Issues: Report by Europe Economics for the European Commission, DG Competition' (Information, communication and multimedia Media and music publishing, November 2002).

[23] Jan van Cuilenburg, (2002) 'The media diversity concept and European perspectives', paper presented at the Media Economics, Content and Diversity Seminar, Finnish Academy of Sciences, Helsinki (16 December 2002).

sustaining competition in markets, protecting the interests of consumers and ensuring freedom of trade carried on by other participants in markets while sustaining economic development. The CCI took over from the erstwhile Monopolies and Restrictive Trade Practices ('**MRTP**') Commission that was the closest to an anti-trust body in independent India. Its legal instrument, the MRTP Act, was revoked since the government felt an 'incompatibility between the liberalized regime and previous policy instruments such as MRTP'.[24] For instance, the MRTP Act did not discuss predatory pricing, which demands a clear understanding of relevant market. Like the MRTP Commission, the CCI also has a multi-sectoral remit; it is mandated to promote and protect competition in all sectors by curbing business practices adversely affecting competition and protecting the interests of consumers. For the most, disputes adjudicated by the CCI have pertained to anti-competitive agreements and abuse of market power. Contesting parties aggrieved by a CCI judgement have the option of approaching its appellate arm, the Competition Appellate Tribunal ('**COMPAT**').

Apart from the Cable and DTH segments of TV distribution, the CCI has been adjudicating competition in a plethora of economic activities, from real estate to the stock market.[25] As per procedure, upon receiving a complaint by an informant party ('**IP**') under s. 19 of the Competition Act, the commission first considers whether there is a prima facie case and then investigates the matter under s. 26 (1) of the Act. The issue of abuse of dominant position and making anti-competitive agreements is determined after the investigations reveal the relevant market (s. 2 (r), (s), (t) of the Act) of the party concerned. This is the stage when market definition as an analytical tool comes into play.

Relevant markets or antitrust markets are defined in competition law to assess the likely effects of dominance in the competitive milieu. Thus, relevant markets are not defined for their own account, but as a tool to the effective execution of competition policy.[26] The purpose of defining a relevant market is to establish whether a firm or a group of firms has shown or can show market power. Defining the relevant market helps the CCI demarcate products/services whose suppliers are capable of exerting pressures on each other. Once demarcated, the CCI ascertains whether the supplier held a

---

[24] Thankom G. Arun, 'Regulation and Competition: Emerging Issues in an Indian Perspective' (2003) Working Paper Series No. 39, Centre on Regulation and Competition, University of Manchester (October), 8.

[25] For example, a heavy penalty of Rs 550 million was imposed on the National Stock Exchange and Rs 6300 million on DLF Ltd., a leading real estate firm, for abusing their dominant position in the stock exchange services and real estate sectors respectively.

[26] European Commission (n 22) 101.

dominant position in the concerned market and, if so, whether it is guilty for abusing its position. Such abuse of market power could be by predatory pricing, tie-in arrangements, exclusive supply agreements or other mechanisms declared to be anti-competitive under s. 3 of the Act. Along with s. 4 of the Act, relevant market is undoubtedly a fundamental issue in the adjudication of 'abuse of dominance'.

Establishing a robust argument for market power or abuse of dominance necessitates accurately identifying the product being sold and the territoriality of the market it spawns. A *Relevant Market* has been defined under the Act as the market, determined by the Commission, with reference to the relevant product market or the relevant geographic market, or with reference to both the markets.[27]

Relevant geographic market means a market comprising the area in which the conditions of competition, for supply or demand of goods or services, are homogenous and can be distinguished from the conditions prevailing in neighbouring areas.[28] In the context of the C&S TV business in India, this largely concerns competing distribution and relay of television signals within the physical territory served by a Cable operator and the footprint of a DTH service--- i.e. the service area of a TV distributor.

Relevant product market means a market comprising all those products or services regarded as interchangeable or substitutable by consumers, by reason of characteristics of the products or services, their prices, and intended use.[29] The TV business in India comprises two overlapping audience markets, one each on C&S TV and on free to air Terrestrial TV. Thus, in the case of C&S TV, it is fundamental to identify the particular product (TV channels) being distributed and the kinds of substitutability audience can avail, before defining a relevant product market. Simply viewing 'content' to be the generic product being distributed obfuscates differences between the types of commodities being distributed by Cable and DTH operators. For instance, TV programmes, advertisements, and on-demand movies convey different types of content. On their part rent free C&S TV channels and paid C&S channels also convey different types of 'products'--- something the European Commission has repeatedly held due to it differentiating between un-subscribed and subscribed content.[30]

---

[27] Competition Act 2002, s 2(r).
[28] Competition Act 2002, s 2(s).
[29] Competition Act 2002, s 2(t).
[30] Natascha Just, 'Measuring Media Concentration and Diversity: New Approaches and Instruments in Europe and the United States' (2008) TTLF Working Paper No. 2, Transatlantic Technology Law Forum, Stanford/Vienna, 8 <https://law.stanford.edu/

The paper provides a critical appraisal of CCI's engagement with conceptions of relevant geographical market and relevant product market in the TV distribution business. The corpus of cases considered are between 2011, when such matters first came to the CCI, and 2015, when the vast majority of Cable homes came to be mandatorily digitalised. In this period, we identify cases coming to the CCI pertaining to the Cable and DTH business to lay out the gamut of issues triggered around the problematic of relevant market. In doing so, the paper spotlights the conceptual challenges grappled by the CCI in understanding the relevant market in the wired and wireless segments of TV distribution.

Our narrative brings out why the CCI's adjudication necessarily depends on the specific nature of the product in question. For one, the cases bring out the pitfalls of viewing the programming offered by TV broadcasters ('content') to be the only product being distributed, since this obfuscates differences between the types of commodities constituting the business of commercial C&S TV--- which also include advertisements/airtime and on-demand programming. Secondly, the cases point at the role of language in defining the product/content distributed--- and hence the boundaries of a linguistic geography where a particular product would find its market. The presence of multiple, large, and often overlapping language markets in India is what imparts a complexity that sculpts the unique personality of its media economy as a whole.[31] These two factors, commodity-types and their language, ought to be brought together to evaluate whether the product distributed by Cable and DTH operators is substitutable or not.

But we also come across the problem of substitutability between Cable and DTH as distribution services. Cases analysed in this paper reveal geographical boundaries, and hence the market in question, being defined in different ways by Cable and by DTH. While the *area of operation* of a Cable operator is defined by the contiguous physical territory where its wired service can retail signals, that of the wireless TV distributor (DTH operator) is defined by the footprint of its signal--- which is effectively all across India. However, the market is defined not only by the area of operation alone; it is defined by the market for particular products within an area of operation. Thus, it is the aggregate and conditional outcome of all three factors together--i.e.

---

wp-content/uploads/sites/default/files/publication/205108/doc/slspublic/just_wp2.pdf> accessed 13 June 2020.

[31] Vibodh Parthasarathi, 'Market Dynamics of the Indian Media Economy' in Adrian Athique, Vibodh Parthasarathi, and S.V. Srinivas (eds), *The Indian Media Economy* (vol 2, Oxford University Press 2018) 1-22; Also *see* S.V. Srinivas, 'Region in Focus' (2015) 6(2) Bioscope: South Asian Screen Studies vii.

commodity, language, and technology--- rather than any one by itself, that needs to be nuanced before identifying the relevant market. Failing to place due weight on any one of these may lead to inaccurate adjudication; this could result in the CCI ignoring all these nuances, like it appears in the *Reliance* case evoked at the outset, or take some disputes for appeal at the COMPAT.

Discussions in the following section highlight the reasoning deployed by the CCI in variedly ascertaining the relevant geographic market to be a particular state/region within India, or a contiguous group of states/regions, or the entire country. The subsequent section delves into disputes squarely concerning relevant product market to show how/why the CCI argued the substitutability, or otherwise, of the two principal distribution platforms, viz. Cable and DTH. The paper then pulls together the conceptual and empirical challenges provoked by market definition in India's complex landscapes of TV distribution.

IV. The Territoriality of Distribution: Relevant Geographical Market

One of the first movers in the Cable business was the Sumangali Cable Vision whose affiliate companies included not only one of India's earliest multi-lingual broadcast network *(SUN TV)* but also a first mover in the DTH business, Sun Direct. Operating largely in southern India, Sun Direct was accused of employing anti-competitive practices in *Jak Communications* v. *Sun Direct* ('**Jak Communications**').[32]

The OP in this case, Sun Direct, introduced a package of channels, 'Tamil Freedom Package', for Rs. 440 for four months with a subscription fee of Rs. 99 per month. The informant, Jak Communications, a large MSO in South India, accused Sun Direct of attempting to eliminate all other players in its area of operation through predatory pricing by charging lower monthly rent (Rs. 99) than the then basic price (Rs. 156.55). It also accused Sun Direct of having an anti-competitive agreement with subscribers[33]--- a practice aided by Sun Direct's dominant position in the overall TV distribution market. By supplying set top boxes at highly reduced prices, Jak Communications alleged that Sun Direct was causing an appreciable adverse effect on competition in the southern states of India and was foreclosing competition in the

[32] *Jak Communications v Sun Direct*, Competition Commission of India Case No. 08/2009.
[33] Sun Direct was alleged to provide Set-Top Boxes, costing Rs 2,200, free to its subscribers.

arena. All in all, the practices of Sun Direct amounted to 'predatory pricing' and 'abuse of dominant position', under s. 3 (4) and s. 4 (2) (ii) respectively.

Since the informant argued that the OPs' dominant position was affecting competitors in the arena, it was necessary for the CCI to begin by identifying the relevant market. The CCI found the relevant geographical market of Sun Direct to be the entire territory of India since DTH services are agnostic to physical territory. This sharply contrasts the territorially defined nature of Cable distribution, such as that of Jak Communications which offer signals to subscribers only in parts of South India. Thus, CCI opined the DTH provider and the regional MSO operated in 'distinct and *distinguishable*' geographical markets. The CCI also saw the relevant product market of the two TV distributors in dispute to be different. Precisely because Sun Direct's services differed in product characteristics (i.e. channels in the packages it retailed), type of add-on services (like movies on demand) and interactive services (such as games and educational services), its offerings were not seen as substitutable to those of Jak Communications and other MSOs. Thus, CCI felt that the DTH distribution seemed to ostensibly cover many more products compared to those offered by the informant MSO, and thus, that Sun Direct was not vending interchangeable services. Within these definitions of the relevant markets, CCI reasoned Sun Direct could not abuse its dominant position because in the national market of DTH services, it was not the dominant or most dominant player, it being third in terms of subscriptions among six private DTH operators.

While the main order of *Jak Communications* found the DTH provider not guilty of contravening any sections of the Competition Act, 2000, the dissenting order illustrates why the issue of relevant market is more contentious than what immediately meets the eye.

The dissent averred that in defining the demarcations between geographical markets, it had not been considered that DTH services often customise their channel packages differently in different territories--- like Sun Direct did with its 'South India' and 'Rest of India' packages. Such grouping of channels is based on the popular language in the territory of sale, enabling DTH operators, while having a pan-India footprint, to cater to particular linguistic communities within a region of India. Even competing DTH distributors like Airtel Digital TV and Tata Sky retailed regional packages specific to TV homes in South India. The dissent recalled that s. 19 (5), (6), and (7) of the Competition Act require the Commission to give due regard to *local specification requirement*, consumer preferences, language, price of service, and existence of specialised producers, which in this case was the

'Tamil Freedom Package' offered by Sun Direct--- hence deemed to be considered interchangeable with regional MSOs' product offerings in the area where the dispute emerged. Consequently, the four states of South India were seen to be the market for the 'South India' package of Sun Direct. Doing so, the dissent inferred, would lead to Sun Direct revealing a dominant position in the service area that was being abused by way of unexplained low rates per channel.

Thus, the main order of *Jak Communications* found the relevant market to be the whole of India, and DTH services said to be in its own exclusive terrain.[34] The dissenting order problematised relevant market by pointing to the determining importance of language in constituting it, as also the ability of DTH operators to offer different language packages (i.e. different products retailed) in different regions of India. The dissent reasoned that since viewers in Indian states would be inclined to watch channels in their own regional languages, it was untenable to consider the geographic market being the country--- and therefore only the four states of South India could be seen as the relevant market.

The very next year, the CCI maintained in another case that the country was the relevant geographical market for DTH services, albeit on a different reasoning. In *Big CBS Networks & Anr* v. *Tata Sky Ltd* ('**BIG CBS**'),[35] the petitioner distributed a host of entertainment channels, while the OP was the DTH operator, Tata Sky Ltd., whose co-owner was a broadcaster competing with those of Informant broadcaster in some language segments.

Big CBS Networks had filed a case under s. 19 (a) of the Competition Act alleging abuse of dominant position by Tata Sky in contravention of s. 4 of the Act. It asserted that the DTH operator was charging it an exorbitant (five times over) carriage fee to transmit its channels. It submitted the relevant product market to be the 'service of broadcasting channels through DTH platform'. It further submitted that its channels catered to the English speaking urban population and therefore the *relevant geographical market* was 'service of broadcasting channels (including through DTH operators) in large urban market i.e. Delhi, Mumbai, Chennai, Hyderabad, Kolkatta, Bangalore and other important cities like Chandigarh, Kochi, Goa, Pune, Mangalore and state of Sikkim'.[36] According to BIG CBS, Tata Sky was having dominance in this market since it was the most widely used DTH

[34] Which is to say that the market for DTH services (to which Sun belongs) is different from the market of Cable provider (to which informant belongs).

[35] *BIG CBS Networks v Tata Sky Ltd*., Competition Commission of India Case No. 36/2012. (BIG CBS Networks)

[36] *BIG CBS Networks*.

platform in metropolitan and other big cities where viewership of English channels was concentrated.[37]

The CCI opined that the relevant geographic market was the 'provision service of broadcasting of channels through DTH' i.e. the entire country. The plea of BIG CBS was rejected because it failed to submit cogent evidence to show that English channels were not telecast in other areas, or were not watched by non-urban populations. Consequently, the case for the dominant position, and therefore the possibility of its abuse, by the DTH operator across India was found untenable.

The issue of relevant market came up yet again in *Makkal Tholai Thodarpu Kuzhumam Ltd.* v. *Tamil Nadu Arasu Cable TV Corpn. Ltd.*[38] The Informant was the Tamil-language broadcaster, Makkal TV, whereas the OP was an MSO in Tamil Nadu, Arasu Cable, that was fully owned by the state government--- a unique case in India's TV distribution business. Thus, both parties were wholly operating in the same language market. Arasu Cable was carrying Makkal TV since September 2011, free of cost and in its S-band in 'S-4' channel. However, in 2015, to enhance revenues it decided to collect carriage fee from (free-to-air) broadcasters. Since this fee was very high for Mid and Hyper bands for free-to-air channels including Makkal TV, Arasu Cable was accused to have indulged in unfair and discriminatory practice through an abuse of its dominant position.

Although Makkal TV could be viewed by households subscribing to either DTH or Cable, CCI felt these two platforms could not be treated as being similar, or substitutable. Hence, it identified relevant product market to be that involved in the 'retransmission of channels through Cable TV Networks'--- i.e. channels distributed through Cable. As a corollary, the CCI further observed that the relevant geographic market was the territory where Cable distributors relayed Makkal TV--- which was the state of Tamil Nadu.[39] Combining both observations, the CCI ultimately held that the relevant market in the present case would be Cable distribution in state of Tamil Nadu.

Taken together, what do the three cases reflect on the problem of defining relevant geographical market?

---

[37] ibid 2.

[38] *Makkal Tholai Thodarpu Kuzhumam Ltd. v Tamil Nadu Arasu Cable TV Corpn. Ltd.*, 2015 SCC OnLine CCI 162.

[39] Except Chennai, which was at that time covered under a different regulatory framework.

Ascertaining a relevant geographical market proved to be highly dependent on the types of distributors and types of products in specific areas. In the first dispute, the CCI judgement found the relevant geographical market to be the entire country--- despite the area of operation of the Cable distributor involved being only regional. From this stemmed CCI's further view that the distribution services of the DTH provider and regional MSO operated in separate product markets. The dissent rightly reasoned that it was untenable to view the entire country as the geographic market since the products offered by both, in the area of dispute, were likely to be interchangeable. In the second dispute, the CCI held the relevant geographic market to be the entire country. However, this was because the informants led by a multi-lingual broadcaster were unable to provide evidence on why English channels, such as its own, would not have viewers in regions of India outside metropolitan cities where the contesting DTH distributor operated. In the third dispute, between a regional Cable distributor and a smaller, single-language broadcaster, the relevant geographical market was effectively held by CCI to be the state of Tamil Nadu.

The circumstances of these three cases reflect the peculiarities of the TV landscape in India. The first case arose due to the capacity of *different TV distribution technologies*, despite having different physical boundaries of their service areas, to offer substitutable products. Along with the dissent, it thus illustrated how product and technology come together to shape the Indian TV landscape. This was to some extent also visible in the second case involving broadcasters and a DTH distributor, since it arose due to the characteristic fragmentation of TV broadcast markets overlapping with *geographical separation of their audiences*--- despite the ability of the concerned TV distributor to technologically integrate them. This is where the paucity of data necessary to thickly enumerate the market becomes crucial, as admitted in the judgement of *BIG CBS*. In comparison to the first two cases, the circumstances of the third case were less challenging to comprehend since it involved one broadcaster and one distributor operating in one well-defined linguistic and physical territory.

What these cases also suggest is that ascertaining relevant geographical market is contingent on accurately understanding the nature of the specific products in question. In this light, what unifies the circumstances of these cases, ostensibly about considerations of service area in market definition, is the role of language as a trait of the product being broadcast and distributed. In these three cases, this has varied from being Tamil, which has a regional, geographically-specific audience market, to English, whose audience is diffused across the country. The role of language emerges as central not only

on the demand side--- i.e. what the audience prefers in linguistically and geographically bound, or separated, territories--- but also on the supply side, i.e. how distributing technology agnostic to geography enables curating product for specific linguistic audiences within this geography. Only the dissent in *Jak Communications* found these dynamics relevant to unpack. We are thus curious about the CCI's experiences in explicitly identifying the relevant product market, given India's multi-lingual broadcasting and multi-technology distribution environments.

V. The Substitutability of Distribution Services: Relevant Product Market

The relevant product market has been defined to consist of all those products or services that are regarded as interchangeable or substitutable by the consumer owing to the nature of the products or services, their prices and intended use.[40] This approach of the CCI seems to stem directly from an early definition of relevant product market in the European Union.[41]

Dish TV v. *Prasar Bharti* ('**Dish TV**')[42] involved Dish TV, India's first private DTH distributor, also having an affiliate in the Cable business (SITI Cable) and affiliates in broadcasting through a large number of news and entertainment channels (Zee News and Zee TV respectively) in several languages. The OP, Prasar Bharti, is the national public broadcaster providing TV channels through its Doordarshan network on the terrestrial and Cable & satellite modes. Doordarshan also provides a rent free DTH service. Consequently, the DTH distribution service and the Cable & Satellite broadcasts of Prasar Bharti competed respectively with Dish TV and its broadcast affiliates.

Dish TV approached CCI after Prasar Bharti refused to telecast its advertisements on Doordarshan National, a terrestrial channel, on a commercial basis. Neither did any of the other private DTH distributors refuse telecasting advertisements of Dish TV, despite being its competitor, nor was there

---

[40] *Atos Worldline India (P) Ltd. v Verifone India Sales (P) Ltd.*, 2015 SCC OnLine CCI 57 .

[41] In the European Union, a relevant product market is defined as follows: 'A relevant product market comprises of all those products and/or services which are regarded as interchangeable or substitutable by the consumer, by reasons of the products' characteristics, their prices and their intended audiences; Commission of the European Communities, 'Commission Notice on the Definition of the Relevant Market for the Purposes of Community Competition Law' (1997) Official Journal of the European Union, OJ C 372, 9 December 1997, 5.

[42] *Dish TV v Prasar Bharti*, Competition Commission of India Case No. 44/2010.

anything in Doordarshan's Advertisement Code to stop such advertisements being telecast on Doordarshan National.

The CCI felt Dish TV had conceived of the relevant market as the viewership of the terrestrial broadcasts of Doordarshan National. However, CCI argued that in this instance the product in question was advertisement airtime, not the viewers of a particular channel. This suggests CCI's sensitivity towards recognising commercial TV entailing a 'dual product' market.

In traditional models of publicly or license-fee funded television, the product was media content, while the viewers were the consumers. This reflected traits of a single product market, akin to that of other standard economic products. However, advertising-driven commercial television (like that by private C&S TV broadcasters in India) operates in a dual product market: i.e. on the one hand, it entails a market for viewers, where the product is the content (i.e. programmes, news stories etc.), like in traditional public television; but simultaneously, there also exists a market for advertisements or airtime, wherein the product is the audience who are sold to advertisers (to provide revenues to produce the content).[43] In short, private C&S TV in India entails one market where content is sold to audiences, and another where audiences are sold to advertisers. Significantly, the dynamics of a dual product market could well create situations where an entity dominates one part of the product, audience share in the C&S TV market, and not the other part of the product, i.e. airtime share.

Thus, in this case, the CCI grappled with the consequences of the phenomenon of dual product market. Recognising the markets for audiences and airtime being related businesses, Dish TV claimed Prasar Bharti, the government-owned terrestrial broadcaster, leveraged its dominance in one market, that of audiences, to attain dominance in the other market, that of airtime. However, Dish TV was unable to present evidence to establish Prasar Bharti's dominant position in the relevant product market--- i.e. in the market for airtime. The CCI observed that while Doordarshan may be considered to dominate the market for content (i.e. programming) among terrestrial audiences, it did not dominate the market for airtime sales across both terrestrial (free-to-air) and C&S (subscription-based) broadcasting. Distinctions in the latter remind us of the reasoning behind the European Commission differentiating between pay-TV and free-to-air TV.[44]

---

[43] Robert G. Picard, *Media Economics: Concepts and Issues* (Sage Publications, 1989) 17-19. For an early exposition of how media products differ from other goods, *see* Richard Collins, Nicholas Garnham, and Gareth Locksley, *The economics of television: The UK case* (Sage Publications, 1988).

[44] Just (n 30).

When the product gets identified correctly in disputes, then the other big factor comes into play: the substitutability of products. In *Yogesh Ganeshlaji Somani* v. *Zee Turner Ltd. Star* (**'Shri Yogesh Ganeshlaji'**)[45] both the OPs were content aggregators; that is, they were wholesaling channels for one or more broadcasters, as bundles or otherwise, by negotiating on their behalf with MSOs and DTH distributors. The complainant argued that the planned joint venture by the two aggregators---where each involved a Cable distributor directly or via its affiliate---would lead to a trickle down, control effect. Since both the partnering entities had interests in the MSO segment, the fear was these aggregators would gradually bypass MSOs other than those associated with them, leading to eliminating LMOs other than the ones their MSOs preferred---and finally culminating in a restrictive, narrow choice of distribution networks for subscribing households.

The CCI held the businesses of aggregating and of distributing TV channels not being substitutes since they pertained to respectively the wholesale and retail markets of TV distribution. Consequently, the relevant product market in question here was that of 'aggregators and distributors of Cable and DTH' in India. The CCI felt this market was different from that of Cable and DTH services which it saw to be interchangeable and substitutable from the consumer side--- since they could switch between these different services.[46] Further, the use of 'India' as the geographical market was justified because the license provided to the aggregators was that of 'India' and their operations are not restricted to any state. Thus, the CCI saw the OP not capable of adversely affecting competition in the relevant market identified. The case of Shri Yogesh Ganeshlaji thus helps us to make a larger point about the CCI recognising the relevant market for aggregators and for distributors being different, despite both dealing in the same 'product'.

In *Consumer Online Foundation* v. *Tata Sky Limited, Dish TV India Limited, Reliance Big TV Ltd. and Sun Direct TV Pvt Ltd.* (**'Consumer Online Foundation'**),[47] the CCI held that DTH operators had deliberately developed a business model wherein customers had to buy the necessary DTH hardware from the operators. While this suggests that the CCI saw even rival DTH services not being perfect substitutes, for now our focus is on this judgement exemplifying different distribution technologies conveying different product markets.

---

[45] *Yogesh Ganeshlaji Somani v Zee Turner Ltd.*, 2013 SCC OnLine CCI 26 : (2013) 115 CLA 78. (Shri Yogesh Ganeshlaji).

[46] *Shri Yogesh Ganeshlaji*, para 3.8.

[47] *Consumer Online Foundation v Tata Sky Limited, Dish TV India Limited, Reliance Big TV Ltd. and Sun Direct TV Pvt Ltd.*, 2011 SCC OnLine CCI 12 : [2011] CCI 11.

In this dispute, the three DTH operators comprising the OP argued that Cable T.V., IPTV, and DTH services were the same product market as they could be substituted or interchanged. However, the CCI negated this view on substitutability by distinguishing between the three modes of transmission and holding them to be very different. While IPTV came through wires but on the internet, Cable TV was transmitted through wires and the services of MSOs, and DTH signals were received directly from the satellite and no other intermediate medium. Although the intended use of all the services were the same, the CCI noted that the prices of the three services were different; while DTH was costlier than IPTV and Cable, the technological character of all three are different since IPTV and Cable TV could not be seen in places without adequate broadband or cables. Moving to the demand side, CCI found Cable inspiring to lesser consumer satisfaction as limited number of channels were available, while vast number of channels could be viewed on DTH which also had better image quality. Thus, CCI held that customers too regarded DTH as a service that was distinct from IPTV and Cable TV.

With this in mind, the CCI reiterated that under s. 2(t), it was for the consumer to realise that the services are substitutable or interchangeable. Given all these points of difference and the letter of the Act, the CCI held that DTH constitutes a significantly different market and therefore a *separate* relevant product market vis-à-vis IPTV and Cable. While this part of the judgement was in public interest, it maintained the CCI's orthodox and un-nuanced view of the relevant geographical market of DTH being the whole of India--- as per *Jak Communications*, *Shri Yogesh Ganeshlaji*, and *Big CBS Networks*.

Looking back at the cases discussed, two grey areas seem to exist in market definition, viz. identifying the relevant product, and determining the substitutability of products.

In *Dish TV*, we see recognition of TV signals being distributed to consist of many different products but also see complications arising from the two different types of broadcast markets, terrestrial TV and C&S TV, operating in parallel in India--- which makes pinpointing the relevant product market a delicate proposition. This reminds us of the holding in another case where the CCI's judgement was not so delicate. In *Co-ordination Committee of Artist and Technicians of West Bengal Film and Television Industry* v. *Sajjan Kumar Khaitan*,[48] the majority judgement opined the relevant product

[48] *Co-ordination Committee of Artist and Technicians of West Bengal Film and Television Industry v Sajjan Kumar Khaitan,* 2014 SCC OnLine Comp AT 4 : 2014 Comp LR 329 (CompAT). The Co-ordination Committee was a joint platform of Federation of Cine

market to be the 'whole Film and TV Industry of West Bengal'. As opposed to this vague conception, the minority judgment saw the relevant market being that only of 'broadcast of TV serials'--- i.e. a particular subset of the former. When the matter went to COMPAT, it agreed with the minority judgment, squashing the rather broad definition of relevant product market in CCI's judgment.

In upholding the substitutability of Cable and DTH in *Shri Yogesh Ganeshlaji*, the CCI failed to recognise that DTH and Cable differ in product characteristics--- as per *Jak Communications*; it also failed to nuance that consumers' ability to switch between them was not a case of perfect substitution since they had to incur fresh and additional costs to invest in hardware (set top box) while replacing one with the other. The differing product types indicated by Cable and DTH were elaborated in *CCI* v. *Zero Coupon Optionally Convertible Debentures*.[49] In a case principally about the anti-competitive implications of a broadcast network being acquired by Reliance, CCI's judgement implicitly considered the two distribution technologies to be non-substitutable because Cable offered a smaller number of channels and lacked clarity on the actual subscriber base.

In Consumer Online Foundation, the CCI went into the technological and price attributes of DTH, Cable, and IPTV, to bring home the point about the competing but non substitutable nature of products/services in the TV distribution business. Further, and rather importantly, it spotlighted a crucial aspect of the Act--- that it was for the subscriber/audience to realise that the services are substitutable. One important distinction subscribers keep in mind, omitted in all judgements, is the mobility offered by DTH connection when subscribers move to a new address.[50] While this drives further the case for the non substitutability of Cable and DTH, it recalls the importance of debates in other media businesses on competing but non-substitutable products.

One such example would be the substitutability between fixedline (wired) and mobile (wireless) services in a comparable sector--- such as in the broadband business. In the broadband business, differences in price, speed, and reliability between fixedline/wired and mobile/wireless services can rightly reason these two being considered as competing but non-substitutable products. However, as differences in these attributes diminish over time, there

---

Technicians and the West Bengal Motion Pictures Artists Forum. The EIMPA was a regional association of film producers, distributors, and exhibitors from West Bengal.

[49] *CCI v Zero Coupon Optionally Convertible Debentures*, 2012 SCC OnLine CCI 76.

[50] Interviews conducted in Delhi and Patna under fieldwork directed by the author and Arshad Amanullah.

emerges an argument for such wired and wireless services to access the internet being considered substitutable, since users and potential subscribers see them at par, as research in Turkey reveals.[51] In contrast, the prices of wired (Cable) and wireless (DTH) services to access C&S TV India have remained noticeably different, and hence continue to be a factor in TV subscribers refusing to see them as substitutes. The case of broadband access also reveals the importance of time--- both technological change and market maturity---in imparting the expected consistency in jurisprudence on market definition.

To accurately decipher the relevant product market, competition regulators must carefully delve into the attributes of seemingly similar, and therefore apparently substitutable, products. The CCI reflected such a nuance in its judgements concerning another media business, that of cinema exhibition. In *Film & Television Producers Guild of India* v. *Multiplex Assn. of India* the CCI construed (and I would agree) single-screen theatres operating in a different product market than multiplex theatres--- where several movies are exhibited at the same time and whose tickets are many times higher than those at the former.[52] This then aptly echoes CCI's reasoning in Consumer Online Foundation where it successfully grasped the complexities of competing but non-substitutable services in defining relevant product markets.

VI. Market Definition in a Complex Milieu: Conceptual and other Conundrums

Case law of the CCI vividly demonstrates that determining the *relevant market* in TV distribution in India is a slippery slope. This in itself is not very unique given that the early decades of anti-trust jurisprudence in Cable distribution in other countries has also reflected this, such as in the USA.[53] What is rather special to India is the *co-determination of market definition* by the interplay between the circumstances of a case, and an accurate reading of the characteristics of the technology and service area.

Our meandering narrative of cases on relevant market in India's complex C&S TV landscape offers insights at two levels: conceptual and empirical.

---

[51] Fuat Oğuz, K. Ali Akkemik, and Koray Göksal, 'Toward a wider market definition in broadband: The case of Turkey' (2015) 37 Utilities Policy 111.

[52] *See Film & Television Producers Guild of India v Multiplex Assn. of India.*, 2013 SCC OnLine CCI 89 : 2013 Comp LR 19 (CCI).

[53] *See* Michael Botein, 'Cable Television Franchising and the Antitrust Laws: A Preliminary Analysis of Substantive Standards' (1984) 36(3) Federal Communications Law Journal 253.

Foremost, it brings to light some conceptual hiccups in construing and adjudicating definitions of relevant market in TV distribution.

We recognise that the twin segments of DTH and Cable illustrates a case of inter-related markets occurring between the demand and supply side of TV signals. The TV distribution business reflects competition among various Cable operators and DTH operators as also, *often simultaneously*, between these two technological platforms, i.e. wired and wireless TV distributors. This echoes the market dynamics of the records industry during the 1900s and the video cassette business during the 1980s where rivalry between individual companies simultaneously marked a competition between rival technological formats.[54] Furthermore, in TV distribution, this competition unfolds at two levels. On the one hand, Cable and DTH firms compete, like in any wholesale market, to attract TV channels of broadcasters; on the other, they vie for households, akin to in any retail market, to buy C&S TV signals. Competition between firms at both levels unfolds in a manner such that their success in the first (wholesale) market tempers their operations in the second (retail) market---and therefore their margins harvested in both.

Successful and accurate competition adjudication tends to share two traits: a precise identification of the product likely to be relevant, and a clear assessment of the workings of the substitutability between *seemingly competing* distribution services. Our narrative has highlighted problems in identifying markets in the supply of specified products---as illustrated by the case of *Dish TV* over relevant market in advertising airtime in the market for terrestrial TV. Equally, we spotlighted problems arising from a partial understanding of the similarities/differences between competing technologies of distributing television signals, best indicated in *Jak Communications*. Taken together, perhaps both these boil down to a fundamental conundrum: are Cable and DTH perfect substitutes in India's TV distribution market, and if so under what competitive circumstances and in which areas of operation?

This leads us to ponder over the impediments in transporting orthodox conceptions of market definition to complex television markets like India. Thus, in dealing with market definition, we stumble upon the peculiar contexts and characteristics of TV distribution in India that give rise to such conceptual challenges.

---

[54] *See* Vibodh Parthasarathi, 'The Evolution of an Early Media Enterprise: The Gramophone Company in India, 1898-1912' in Ravi Sundaram (ed) *No Limits: Media Studies from India* (Oxford University Press, 2013); and, Michael A. Cusumano, Yiorgos Mylonadis, and Richard S. Rosenbloom, 'Strategic Maneuvering and Mass-Market Dynamics: The Triumph of VHS over Beta' (1992) 66(1) The Business History Review 51.

What upsets the neatness of the economic premise upon which policy frameworks and regulatory adjudication are based, is the fact that the *retail market of TV distribution in India is not characterised by perfect competition,* as commonly assumed in textbooks.[55] Textbook renditions of competition demands that C&S TV subscribers within a geography are able to compare offerings by rival Cable distributors as also rival DTH distributors. However, in India there is no real choice for potential subscribers within an area between rival providers of Cable signals, as each residential locality (be it in cities or rural areas) is effectively catered to by one LMO. Intriguingly, this phenomenon was evident in the early years of the Cable business[56] but remains so 20 years later--- and despite the much talked about goal of mandatory digitalisation to usher in choice for TV audience.[57] In short, at the last mile of TV distribution in India, all retail boroughs effectively consist of one Cable distributor, or a 'natural' monopoly.

On its part, DTH distribution also reflects a lack of perfect competition, but for another reason--- the lack of enforcement of interoperability amongst competitors. While the CCI's judgements are rarely informed by this, in the odd case where they are, it finds the absence of interoperability due to DTH operators' deliberately seeking to lock-in their subscribers--- thereby making subscribers' migration between competing operators an expensive proposition, as well articulated in Consumer Online Foundation. The unwillingness of DTH distributors to comply with interoperability protocols, and the silence of the government to enforce such protocols, nullify the empirical assumptions underlying the concept of substitutability. Of course this adversely effects competition in this important consumer-facing business, as the CCI's investigation itself confirmed.

What thus becomes blatant is that the Cable and DTH segments of the retail market in TV distribution display imperfect competition, albeit constituted in different manners. This makes the endurance of arguments about the substitutability of Cable and DTH, in the CCI judgements and assumptions by policymakers alike, even more surprising.

The scenario cultivated by the absence of perfect competition and of the conditions enabling substitutability gets further complicated when we look at other traits of the TV distribution business. Primary here are the existence of *multiple and overlapping distribution markets* within the country based

---

[55] For instance, Jeffrey C. Ulin, 'Television Distribution', *The Business of Media Distribution: Monetizing Film, TV and Video Content in an Online World* (Focal Press, 2010).

[56] Naregal (n 17).

[57] Parthasarathi, Amanullah, and Koshy (n 10).

on language, geography, and technology. The first factor reflects, language, the 'embeddeness', to evoke Polanyi,[58] of the business of TV distribution in Indian society--- i.e. the extent to which distribution markets are constrained by non-economic institutions, as underscored for media markets more generally in India.[59]

Markets for TV Distribution in India are simultaneously defined by the media products retailed---itself determined by language---and the geography of retail, i.e. the spatial operations of LMOs, MSOs, and DTH providers. Thus, within a particular area of operation, distributors may not necessarily compete to retail uniform products; they may well have different or customised linguistic offerings of TV signals, which could be dependent on the technology used by competing distributors. These overlapping dynamics, in turn, have contributed to congenitally *fragmenting the TV distribution market along multiple axes*. Such fragmentation invites quibbles with orthodox conceptions of market definition--- an invitation which only the dissent in *Jak Communications* accepted to take on. It is however heartening that the logic of the dissent, i.e. the need for the so called 'national' market to be segregated, was echoed by the CCI in another case, albeit not pertaining to distribution.[60] There the competition regulator astutely argued for disagregating the so called 'national' market for broadcasting, since the consumption of the product in question (i.e. advertisements) was based on evidence (i.e. viewership surveys) that excluded rural areas and small towns.

What our analyses of the corpus of cases has also managed to achieve is to tease out the methodological challenges of market definition instigated by the media milieu of India.

Of principal import is the challenge arising from the *complex overlap of the linguistic, geographical, and technological dynamics of TV distribution in India*--- and the resultant multiple fragmentations of distribution markets. These features were most readily visible in the circumstances of *Big CBS* and *Dish TV*. They make the legal and economic perceptions of the TV distribution market extremely fuzzy, since they require consideration of competing constraints within and across a series of overlapping and layered markets.

We have additionally learnt how the veracity of market definition could be undermined by rapid technological changes. What is relevant here is not only

---

[58] Karl Polanyi, *The Great Transformation: Political and Economic Origins of Our Time* (2nd edn, Beacon Press 2001).

[59] *See* Parthasarathi (n 31).

[60] See, *Prasar Bharati v TAM Media Research (P) Ltd*., 2016 SCC OnLine CCI 15.

the proliferation of new forms of production organisation---such as geographically agnostic, wireless distribution platforms like DTH---but changes entailing their business organisation, in response to the peculiar landscape in India. In short, considerations on market definition must be agile to strategic initiatives by distributors catalysed by the possibilities offered by new(er) distribution technologies. The judgement in *Jak Communication* seemed oblivious to how a 'national' DTH operator could distribute customised packages of TV signals for specific linguistic regions, as duly pointed out by the dissent.

This suggests conceptions of market definition in TV distribution in India are confronted with not only methodological challenges but those concerning the enumeration of the field of distribution, as discussed above. Revisualising textbooks conceptions of market definition will have to consider, rather centrally, the peculiar dynamics of the TV distribution business in India. Such considerations could benefit from recent scholarship visualising the media economy as a broad epistemic construct, which in reality contains a variety of distinct markets or/and sub-markets.[61]

VII. Conclusion

Following a decade of incremental demonopolisation and deregulation during the 1990s, the CCI was envisaged as a quasi-judicial body to curb the negative fallouts of competition across diverse sectors. This demanded competencies in, inter alia, market definition that are not only interdisciplinary but also informed about the peculiarity of products and commercial geographies pertaining to a raft of businesses.

In competition-oriented economic systems, antitrust protocols have traditionally operated alongside coherent statutory protocols. But in the media business of India, these protocols are invariably weak in their conception and design, and uneven in their implementation. Moreover, regulatory protocols are often marked by an incomplete appreciation of the complexity of India's media milieu, and therefore that of the social risks imparted by the unorthodox market behaviour of media companies.

While some cases in the corpus analysed stemmed from disputes arising from shallow compliance with existing regulatory protocols, few others arose due to the abject absence of such protocols. On their part, the trajectory of CCI's adjudication reflects the desire to redress such regulatory

[61] Vibodh Parthasarathi and Adrian Athique, 'Market matters: Interdependencies in the Indian Media Economy' (2020) 42 (3) Media, Culture & Society 431.

loopholes. In doing so, however, the competition regulator often confronts the peculiarities of the distribution business, which in some instances it is unable to comprehensively appreciate. In such scenarios, the CCI's remit of *ex post* regulation risks enhancing not only regulatory costs but also costs borne by the subscriber-audience. Whether this calls for sectoral regulators to robustly consider, and be empowered to enact, *ex ante* regulation is a conundrum as globally debated as that of market definition.

Information About the Journal

The *Indian Journal of Law and Technology* (ISSN 0973-0362) is an academic journal, edited and published annually by students of the National Law School of India University, Bangalore, India. All content carried by the Journal is peer-reviewed except for special comments and editorial notes. The Journal comprises:

- the Board of Advisory Editors, consisting of professionals and academicians pre-eminent in the field of law and technology, which provides strategic guidance to the Journal;
- the Article Review Board, a panel of external peer-reviewers;
- the Editorial Board, consisting of students of the National Law School of India University, which is responsible for selecting and editing all content as well as contributing occasional editorial notes;

OPEN ACCESS POLICY

The *Indian Journal of Law and Technology* is a completely open access academic journal.

- Archives of the journal, including the current issue are available online with full access to abstracts and articles at no cost.
- Please visit the website of the Indian Journal of Law and Technology at "http://www.ijlt.in" to get additional information and to access the archives of previous volumes.

INFORMATION FOR CONTRIBUTORS

The Indian Journal of Law and Technology seeks to publish articles, book reviews, comments and essays on topics relating to the interface of law and technology, particularly those with a developing world perspective.

MODE OF SUBMISSION

Submissions can be in electronic form or in hard copy form. However, submissions in electronic form are strongly encouraged in order to expedite the submission review process. Please address submissions in electronic form to the Chief Editor of the Indian Journal of Law and Technology at "ijltedit@gmail.com".

REGULAR SUBMISSION REVIEW

The Journal shall communicate an acknowledgement to all authors shortly after the receipt of their submissions. The preliminary review of

the submissions shall be completed within four weeks of receipt in usual circumstances. The submissions that are initially accepted shall be blind-refereed by the Article Review Board. The Journal shall make due efforts to complete the entire peer-review process within a reasonable time frame. The Journal shall notify the authors about the exact status of the peer-review process as required.

EXPEDITED SUBMISSION REVIEW

This option is available to those authors who have received an offer of publication from another journal for their submissions. The authors may request an expedited submission review. However, the decision to grant an expedited submission review shall remain at the discretion of the Editorial Board. Please note that requests for an expedited submission review can only be made in relation to submissions in electronic form. All such requests must be accompanied by the following details:

- Name(s) of the author(s) and contact details;
- Title of the submission;
- Details about the journal(s) which has/have offered to publish the submission;
- Whether the offer is conditional or unconditional and, if the offer is conditional, then what conditions are required to be met for final acceptance;
- The date(s) on which the offer(s) expire(s).

The Journal shall make due efforts to accommodate the existing offer(s) and applicable deadline(s). However, upon an oiler of publication pursuant to the expedited submission review, the authors shall have to communicate their decision within five calendar days of the notification or the offer. If there is no response, then the journal shall have the discretion to withdraw the offer.

SUBMISSION REQUIREMENTS

- All submissions must be accompanied by:
  (1) a covering letter mentioning the name(s) of the author(s), the title of the submission and appropriate contact details.
  (2) the résumé(s)/curriculum vitae(s) of the author(s).
  (3) an abstract of not more than 200 words describing the submission.
- All submissions in electronic form should be made in the Microsoft Word file format (.doc or .docx) or in the OpenDocument Text file format (.odt).

- All text and citations must conform to a comprehensive and uniform system of citation. The journal employs footnotes as the method of citation.
- No biographical information or references, including the name(s) of the author(s), affiliation(s) and acknowledgements should be included in the text of the submission, the file name or the document properties. All such information can be provided in the covering letter.
- The Journal encourages the use of gender-neutral language in submissions.
- The Journal shall be edited and published according to the orthographical and grammatical rules of Indian English that is based on British English. Therefore, submissions in American English shall be modified accordingly. The Journal encourages authors to use British English in their submissions in order to expedite the editing process.
- The authors are required to obtain written permission for the use of any copyrighted material in the submission and communicate the same to the Journal. The copyrighted material could include tables, charts, graphs, illustrations, photographs, etc. according to applicable laws.

COPYRIGHT

DISCLAIMER

PERMISSIONS

ORDERING COPIES

Price Subscription (inclusive of shipping) of the IJLT is as follows:

Hard Copy for 2019	Rs. 900
Hard Copy for 2018	Rs. 900
Hard Copy for 2017	Rs. 900
Hard Copy for 2016	Rs. 800

Order online: www.ebcwebstore.com

Order by post: send a cheque/draft of the requisite amount in favour of 'Eastern Book Company' payable at Lucknow, to:

Eastern Book Company,

34, Lalbagh, Lucknow-226001, India

Tel.: +91 9935096000, +91 522 4033600 (30 lines)