GLOBAL TECHNOLOGY LAW CONFERENCE 2015

The Future of Money and Data

Editor-in-Chief
Justice Lee Seiu Kin

General Editor
Yeong Zee Kin

Singapore Academy of Law

Global Technology Law Conference 2015

GLOBAL TECHNOLOGY LAW CONFERENCE 2015

The Future of Money and Data

Editor-in-Chief

Justice Lee Seiu Kin

General Editor

Yeong Zee Kin

Academy Publishing

2016

Academy Publishing is a division of the Singapore Academy of Law.

The Singapore Academy of Law is the promotion and development agency for Singapore's legal industry. Its vision is to make Singapore the legal hub of Asia. It aims to drive legal excellence through developing thought leadership, world-class infrastructure and legal solutions. It does this by building up the intellectual capital of the legal profession by enhancing legal knowledge, raising the international profile of Singapore law, promoting Singapore as a centre for dispute resolution and improving the efficiency of legal practice through the use of technology. More information can be found at www.sal.org.sg.

Published by Academy Publishing

ISBN 978-981-09-8864-7

Contents

Foreword

The Global Technology Law Conference 2015, held over two days on 29 and 30 June 2015, is the second in our series of international conferences delving into the issues thrown up by the collision of law and disruptive technologies. In our first conference in 2011, we looked at the legal challenges and opportunities for cost effective case preparation that were presented by digital evidence within the context of civil litigation. The 2015 conference grappled with legal and regulatory issues in the wake of financial technologies, or Fintech, and the challenges to data protection and intellectual property law associated with big data.

Fintech is a word recently coined to refer to innovations in electronic payment methods. Although these methods are of relative antiquity (in the context of information communications technology), the advent of the World Wide Web has presented vast opportunities for online commerce. Electronic payment for goods, services and software has always been an area of disruptive innovation. In the past two decades, payment intermediaries like PayPal and credit card companies have carved out an important role within the e-commerce ecosystem. But technology never stands still and more recent innovations in the area of cryptocurrencies bring with them the promise of anonymity and irreversibility of payment transactions. This gained cryptocurrencies, Bitcoin in particular, attention and notoriety. The appeal of an electronic system that provided anonymous and yet irreversible transfers of value made it especially attractive to purveyors of merchandise who required non-traceability. Transactions that once took place in darkened street corners began to move to the Dark Web. However such enthusiasm was brought down to earth when investigators were able to take down the Silk Road. This was probably the most notorious DarkNet market, using the public ledger that provided the foundation of the blockchain database that powered Bitcoin. While Bitcoin may have lost some of its lustre, blockchain technology has gained in prominence and it is now a significant driver of Fintech innovations.

Another area that is recently gaining momentum is mobile payment systems, riding the crest of the proliferation of near field

communications ("NFC") technology which is embedded in many mobile phones. Credit and debit card information can be tokenised and stored on mobile phones, thereby presenting immense opportunity for payment intermediaries to offer converged payment services, both online and in the corner convenience store. The proliferation of NFC-enabled point-of-sale ("POS") terminals that can read NFC-enabled credit cards and mobile phones will encourage the adoption of mobile payment services. Mobile payments hold immense promise to finally enable payment transactions of relatively low values to be carried out in a cost effective way. There is another reason to be optimistic that mobile payment systems will not stumble. The tokenisation of credit card and other forms of electronic payment modes allows innovation to take place both at the POS terminal and in the mobile app. The day will soon come when your mobile phone is able to communicate with the POS terminal and then suggest to you the payment options that provide the best discount.

The next phase of innovation in information communications technology will be very much driven by and dependent on data. Today information is generated at increasing volume and speed. With the coming of age of the Internet of Things, data will be generated by an ever increasing variety and number of devices at ever increasing velocities and we will see data volume increasing exponentially. There will be an unceasing feed of data from all sorts of sensors to cloud-based services. Big data will provide immense opportunities for data-driven innovation in the design of services and public sector planning. To make sense of big data stores, we continue to develop ever sophisticated analytics engines. These same algorithms can also pull together the profile of an individual from multiple sources with uncanny ease. The challenges posed by big data are perhaps most keenly felt in the area of data protection legislation. Concepts of consent and purpose limitation took root in the decade before the proliferation of information communications technology. The assumption that consent may be meaningfully taken and the fiction that purpose may be comprehensively defined at the time of collection will continue to be challenged. Data-driven innovation pulls in diametrically opposite direction. One of the promises of big data is that with

sufficient volume and longitudinal data, one is better able to analyse the dataset in order to extract trends and discern behaviours. These may then be applied to, for example, offer better discounts on evenings during the week when online shopping is at its height; equally, data analytics may be used to identify groups whose lifestyle choices may predispose them to medical conditions, and to increase their insurance premiums. The challenge is to balance the benefits of data-driven innovation against undesirable or unethical application of data analytics.

Big data also poses challenges to intellectual property law. Traditional copyright principles that protect databases or compilations were articulated for a world where databases were best represented by directory and programme listings. Hence, the twin criteria of selection and arrangement of records as the touchstones for determining if there is compilation copyright. The limits are tested by electronic databases which exist in abstract tables within a database management system, where there is no meaningful arrangement to speak of, and where the selection of records to display on screen is often a function performed by the application layer, depending on the filters and other parameters supplied by the user. The seams that are stretched by electronic databases will be strained further when these traditional concepts are applied to big data. Whereas traditional electronic relational databases required structure, big data sources can remain as unstructured data. The analytics layer takes over to mine the data in order to provide a set of results. Machine learning technology allows the analytics to be fine-tuned and improved, depending on the user's interaction with the result. This is the genie in the bottle that allows social media services like Facebook to push increasingly accurate (and creepily so) news articles and friends' posts to you. With the analytics engine obviating the need for human intellectual effort, and the need for any form of creative spark, the protection of big data sources will once more test the suppleness of copyright law.

The publication that you hold in your hands collects a series of articles that deal with these topics in much greater depth. The views articulated at the 2015 conference form the bedrock of these articles. I am grateful to the authors for their masterful treatment

of these topics and for stitching together the different views and ideas ventilated during the conference into cogent treatises. I wish also to thank the chairpersons and members of the panels for their active participation, both in the lead up to and during the panel discussions, and also for providing comments on early drafts of the papers collected in this volume. It is my sincere wish that the ideas and views captured between these covers will contribute to the development of jurisprudence in this exciting and ever-changing area of law.

Lee Seiu Kin
Judge, Supreme Court of Singapore
Singapore

March 2016

A Smart Financial Centre: The Geeks shall Inherit the Earth

Finance and technology are integrating and this is in turn transforming the terrain which financial institutions operate in. The future promises, among other things, greater connectivity between customers and businesses, stronger cybersecurity and the ubiquitous availability of a massive storage of data. There are enormous benefits to be reaped as technological solutions enhance present financial services. But there are also new issues and challenges that arise with the adoption of new technologies. From the perspective of a regulatory authority, a balance needs to be struck between providing guidance and fostering innovation. A multi-faceted approach which range from providing financial support to collaborating with the industry players is being undertaken. To build a smart financial centre, not only will the infrastructure for financial services have to adapt, the regulatory framework will have to keep up to manage emerging risks at the appropriate level.

Ravi **MENON**
Managing Director, Monetary Authority of Singapore.

1 Technology is changing the way one lives, works and plays. Robots and unmanned drones are becoming more common. Robotic cleaners like iRobot have lightened the load of household chores. Pizza restaurants in cities ranging from Mumbai to Moscow have started to deliver pizzas using drones. Digital payment systems are taking off rapidly, especially in developing countries. Kenya launched, in 2007, M-PESA, a simple and low-cost service that allows users to deposit and transfer funds through short message service ("SMS") text messages.

2 A sector in which technology is going to be fundamentally transformative is financial services. In fact, there is a new buzzword: "FinTech" – financial technologies or the integration of finance and technology.

3 Two things are happening. First, non-financial players are using technology to offer innovative solutions that mirror the services traditionally offered by financial institutions ("FIs"):

(a) Payments: Apple, Google, Paypal, Amazon and Alibaba have payment solutions that replace physical wallets and credit cards.

(b) Lending: Zopa, Lending Club and Funding Circle offer peer-to-peer lending solutions that match lenders and borrowers on their online platforms.

(c) Investment: "Robo-advisers" like WealthFront use data analytics to dispense online personal financial advice and investment management services.

4 Indeed, these non-financial firms look set to disrupt the financial industry. As a senior banker in the US puts it: "people need banking, not banks".

5 The second thing that is happening is that FIs are fighting back. As disintermediation threatens FIs, they are pushed to rethink their business models. Rising costs, shrinking margins and the weight of new regulatory requirements are pressing FIs to look into more cost-efficient ways of running their businesses. They are increasingly turning towards innovation and technology for solutions. In an ironic way, the FinTech insurgency is forcing change amongst the incumbent FIs.

6 Leveraging on their size and networks, FIs are using technology much more intensely to enhance their product offerings and service delivery. For example, US insurance companies, Progressive and Allstate, are using telematics to develop usage-based motor insurance, also known as Pay-As-You-Drive (or Pay-How-You-Drive). Instead of rewarding past good driving behaviour, these insurers are able to price premiums contemporaneously with current driving habits.

7 What does all this mean? As a PowerPoint slide used by a FinTech company in Silicon Valley rather immodestly proclaims, "the geeks shall inherit the earth!" It is no doubt an exaggeration. But the message is clear – in the years ahead, countries, businesses and people who know how to use technology and innovate will have a keen competitive advantage.

WHY THIS TIME IS DIFFERENT

8 Has one not heard of this story before – that technology will transform banking and then nothing changed fundamentally? Indeed there have been false starts in the past. In the 1990s, everyone thought that electronic money would replace cash and cheques. That has not happened. In most parts of the world, including the US, Japan, Europe and Singapore, notes and coins in circulation outside banks have been increasing steadily every year. In 2000, some of us were quite sure that internet-only banks would eventually replace brick-and-mortar branches. This too has not happened.

9 The most obvious evidence that both beliefs were manifestly wrong occurs year after year, when lines of Singaporeans form at bank branches to obtain new notes for *ang pows*, to be given out during the Chinese New Year celebrations. But this year, however, "*e-ang pows*" were being given out for the first time. Could this be a sign of things to come?

10 Technology takes time to proliferate. More importantly, it is the interaction among related technologies that often creates transformation and that takes time. There is reason to believe that this time is different – that technology will indeed transform financial services in a way that has not happened before. It has much to do with the concept of mobility:

(a) **Mobility of technology.** Mobile devices, such as smartphones and tablets, have become commonplace. People do not just connect and surf from their home computers anymore. They also do so from their mobile devices, while on the go. This has profound implications for how financial services are offered and consumed.

(b) **Mobility of ideas.** Today, online platforms provide a variety of social networking and peer-to-peer services, and people are increasingly comfortable using these services. These services have compressed time and space. Interaction is real-time and information exchange transcends physical boundaries. They allow information, knowledge and ideas to be shared widely across communities and geographies.

(c) **Mobility of payments.** In the past, it used to take several days and cost quite a bit to pay someone in another country or currency. Today, online payment services have made it possible for people and businesses to transfer funds safely at very low cost. This has not only allowed e-commerce to flourish, but also enabled faster and more efficient cross-border financial services, like lending and borrowing.

11 We are looking at a financial services industry that will be increasingly driven and powered by technology.

THE BIG TRENDS IN TECHNOLOGY AFFECTING FINANCE

12 What are the big trends in technology affecting the financial industry? Six technologies appear potentially transformative:

(a) digital and mobile payments;

(b) authentication and biometrics;

(c) block chains and distributed ledgers;

(d) cloud computing;

(e) big data; and

(f) learning machines.

13 The six technologies outlined above (and discussed in detail below) have the potential to transform the financial industry globally. There could well be others that the author has not mentioned. The important thing for our FIs is to be alert to these and other technology trends, understand their possible implications, seize the opportunity to apply the relevant technologies safely and efficiently to boost productivity, gain competitive advantage, and serve consumers better.

Digital and mobile payments

14 Payment services are increasingly being enabled by mobile applications and near field communications ("NFC"). Gone are the days of the clunky cash register. Today, accepting payments can be as simple as attaching a simple dongle, no bigger than a matchbox,

to a tablet or smartphone. This is only the beginning. Payments at stores and restaurants may increasingly not even require physical touch points, and could take place entirely over the Internet, using the customer's smart device to effect payments. Further out, one can look to a future of seamless payments, where technology automatically recognises the customer, checks out the goods, and charges to the customer's account as he walks out of the store.

Authentication and biometrics

15 Authenticating one's identity is critical to gaining access to a variety of financial services and performing many financial transactions. As authentication technology progresses, one can look forward to more secure and efficient solutions to authenticate identity. Biometric authentication is making good advances. In the future, one may not have to remember complex passwords or worry about compromised password. Fingerprint, iris, facial, voice and even palm vein and heartbeat recognition systems are being explored for authentication purposes. Biometric automated teller machines have been deployed in several parts of the world, including the UK, Japan, China, Brazil and Poland. Banks in Singapore have launched mobile applications that utilise the TouchID function of the iPhone for fingerprint authentication. Some have also been exploring the use of voice biometrics in their phone banking and call centre services.

16 For users who are concerned about their privacy or have physical challenges, token-based authentication offers an alternative means of security. Tokens embedded within mobile devices, or perhaps on wearable technology, are viable options. Where stronger security is required, these could be used together with biometrics to provide multi-factor authentication.

Block chains and distributed ledgers

17 Digital currencies, like Bitcoins, have attracted much interest. Payments using Bitcoins are much faster and potentially cheaper than conventional bank transfers and, its advocates argue, just as safe. Whether digital currencies will take off in a big way remains

to be seen. It is a phenomenon that many central banks are watching closely, including the Monetary Authority of Singapore ("MAS"). If they do take off, one cannot rule out central banks themselves issuing digital currencies one day.

18 The bigger impact on financial services, and the broader economy, is likely to come from the technology behind Bitcoins – namely the block chain or, more generally, the distributed ledger system. A block chain is essentially a decentralised ownership record. It allows a document or asset to be codified into a digital record that is irrevocable once it has been committed into the system. The digital record can be accessed and verified by other parties in the system without going through a central authority. The potential benefits of such a distributed ledger system include:

(a) faster and more efficient processing;

(b) lower cost of operation; and

(c) greater resilience against system failure.

19 There are many potential applications of distributed ledger systems in the financial sector. Ripple, a company in the US, offers a solution based on distributed ledgers for real-time gross settlement, currency exchange and remittance. The same solution could potentially allow regulators to plug into the network to conduct surveillance of risks and to track transactions to detect money laundering or terrorist financing. In fact, distributed ledger systems could potentially be applied in any area which involves contracts or transactions that currently rely on trusted third parties for verification. Honduras is developing a land title registry system based on distributed ledgers. Other potential applications that are being discussed include registry of intellectual property rights, supply chain management, electronic voting systems and medical records.

Cloud computing

20 Cloud computing is an innovative service and delivery model that enables on-demand access to a shared pool of computing resources. It provides economies of scale, potential cost-savings, as

well as the flexibility to scale up or down computing resources as requirements change. There is a view among some quarters that "MAS does not like the cloud". This is an urban myth: it is simply not true. MAS did have concerns about cloud computing previously. This was because cloud services were at the time not sufficiently secure to safeguard the sensitive information that FIs held. Since then, cloud technology has evolved considerably and there are now solutions available to address these concerns.

21 For example, FIs can now implement strong authentication and data encryption to protect their data in the cloud. MAS has been in dialogue with both FIs and cloud service providers. Providers have now become more aware of our security considerations while individuals have gained a deeper understanding of the safeguards they have put in place. The author is pleased to share that several FIs in Singapore have successfully rolled out cloud solutions in the past two years.

Big data

22 The world is exploding with information. Data generated by online social networking and sensor networks, and data collected by governments and businesses amount to a universe of digital information that is growing at about 60% each year. There is also a global trend, including in Singapore, towards "open data" in which data are freely shared beyond their originating organisations. At the same time, the cost of storing and processing data has been falling dramatically. These trends have created the opportunity to use data to understand the world with a clarity and depth that was not possible before.

23 Some FIs are investing in and using this big data to derive useful and actionable insights. JPMorgan Chase and MasterCard, to cite two examples, are using big data techniques to derive insights from consumer spending patterns. Visa is using big data techniques to detect fraud in financial transactions.

Learning machines

24 This might well be the most impactful technological change of the future – computers that can "think". Traditional computing machines and algorithms are programmed to carry out specific tasks in response to defined circumstances according to the software program that is coded into them. As the world continues moving into the age of cognitive machines which are designed to learn from the data that they hold and be able to, in a sense, program themselves to perform new tasks. These machines continuously adapt to new data as well as feedback and input gathered from their experiences, including interactions with humans.

25 One can begin to see examples in the financial industry. In equity, commodity and FX markets, some traders are using self-learning algorithms. They not only analyse historical data, predict price movements and make trading decisions, but continually upgrade and adjust their trading strategies in light of new evidence and market reactions. In lending, learning machines have been used to construct models for consumer credit risk and improve the prediction of loan defaults. Legal minds might reflect on the legal liabilities arising from the actions, or inactions, of such learning machines.

SMART NATION NEEDS A SMART FINANCIAL CENTRE

26 At the national level, Singapore has set its sights on becoming a Smart Nation – one that embraces innovation and harnesses info-comm technology to increase productivity and improve the welfare of Singaporeans. The Smart Nation Programme under the Prime Minister's Office has brought together stakeholders from the government and the industry to identify issues and develop solutions with this objective in mind.

27 Government agencies have been rolling out a steady pipeline of Smart Nation initiatives. The Housing Development Board is carrying out a trial of a new system that utilises home sensors to monitor elderly folks who are staying alone and alert caregivers should an emergency arise. The Land Transport Authority is studying the use of autonomous vehicles that can self-drive with

the help of environmental sensors and navigation systems. The Urban Redevelopment Authority has been utilising geospatial information and data analytics for urban design and land-use planning.

28 A Smart Nation needs a Smart Financial Centre. Indeed, the financial sector is well placed to play a leading role given that financial services offer fertile ground for innovation and the application of technology. MAS will partner the industry to work towards the vision of a Smart Financial Centre, where innovation is pervasive and technology is used widely to increase efficiency, create new opportunities, manage risks better, and improve people's lives.

29 MAS will seek to achieve this vision together with the industry through two broad thrusts:

(a) a regulatory approach conducive to innovation while fostering safety and security; and

(b) development initiatives to create a vibrant ecosystem for innovation and the adoption of new technologies.

SMART REGULATION FOR A SMART FINANCIAL CENTRE

30 First and foremost, a Smart Financial Centre must be a safe financial centre. Technology can be a double-edged sword. If not managed well, it can potentially lead to a variety of risks in the financial industry:

(a) financial crime and illicit transactions;

(b) loss of data or compromise of confidentiality; or

(c) glitches that damage reputation, disrupt business, or worse, cause systemic crisis.

31 The first priority on our journey towards a Smart Financial Centre is therefore to continually strengthen the industry's cybersecurity. As more financial services are delivered over the Internet, the frequency, scale and complexity of cyberattacks on FIs have increased globally. Hackers and cybercriminals are constantly probing IT systems for weaknesses to exploit.

32 There are two reasons for concern. First, the level of connectivity among FIs mean that a serious cyber-breach in one institution can potentially escalate into a more systemic problem. Second, repeated cyber-breaches could diminish public confidence in online financial services and reduce people's willingness to use FinTech in general.

33 MAS and the financial industry in Singapore take cybersecurity seriously. FIs are expected to implement controls and measures to preserve the confidentiality of sensitive data, maintain the integrity and availability of their systems, and conduct regular vulnerability assessments and penetration tests to evaluate the robustness of their cyber-defences. MAS conducts regular onsite inspections of key FIs' technology risk management processes and controls to check that they meet these requirements. FIs have also established cybersecurity operations centres to enhance their cyber-surveillance and gather cyber-intelligence.

34 Cyberthreats will not go away. Like a cat and mouse game, both hackers and cyber-defenders have been enhancing their tools and techniques along with advances in technology, as well as in response to one another. As part of this evolution, a new wave of next-generation cybersecurity solutions is emerging, in areas such as trusted computing, security analytics, threat intelligence, active breach detection and intrusion deception. The financial industry needs to keep abreast of these developments.

35 While seeking to ensure cybersecurity, MAS's regulatory approach towards fostering innovation and the adoption of new technologies will take three forms.

36 First, *innovation owned by FIs*. In matters of innovation, time to market is critical. FIs are free to launch new ideas without first seeking MAS's endorsement, as long as they are satisfied with their own due diligence. A recent case that went on this approach was a mobile banking application that utilised fingerprint authentication for balance enquiries. The bank went ahead as it did not require MAS approval.

37 What does this approach entail? FIs' boards and management should take the responsibility to ensure that the risks of new innovative offerings are well identified and managed. The

compliance officers should ideally be involved early in the innovation process. However, they should avoid second-guessing MAS by taking an overly conservative stance that might nip innovation in the bud. If the FI encounters a specific issue on which it needs MAS's guidance, MAS will be happy to help. However, the FI must offer its own assessment of the risks in what it proposes to do and take ownership for its decisions. It cannot rely on MAS for its due diligence.

38 Second, *innovation in a "sandbox"*. Sometimes, it is less clear whether a particular innovation complies with regulatory requirements. In such cases, FIs could adopt a "sandbox" approach to launch their innovative products or services within controlled boundaries. The intention is to create a safe space for innovation, within which the consequences of failure can be contained. FIs can seek MAS's guidance and concurrence on the boundary conditions, for example, the time period, customer protection requirements and so on.

39 Third, *innovation through co-creation*. MAS has a long tradition of active consultation with industry on proposed new rules or initiatives. More recently, MAS has engaged industry players more directly to co-create new rules and guidance – in other words, to jointly come up with proposals. An example is the Private Banking Industry Code developed by industry practitioners in close consultation with MAS. Such co-creation is particularly relevant for developing rules or guidance on new technologies whose benefits and risks are not fully known and where a flexible approach may be desired.

40 A further possibility in co-creation might be MAS and the industry working together to develop common technology infrastructure that meets regulatory requirements. The aim is to clarify and address issues and uncertainties upfront during the course of development.

41 MAS is not seeking a zero-risk regime and MAS understands that failure is part of the learning process in innovation. If things do go wrong with an innovative product or service, and there will no doubt be some failures, the FI will need to review its implementation and draw its lessons. MAS will examine the facts to

assess if there is any systemic or deeper issue that needs to be addressed and determine if any action needs to be taken.

DEVELOPMENT INITIATIVES FOR A SMART FINANCIAL CENTRE

42 Apart from providing a conducive regulatory environment, MAS will work closely with the industry to chart strategies for a Smart Financial Centre. Some of the initiatives MAS has embarked on include:

(a) a Financial Sector Technology & Innovation ("FSTI") scheme to provide financial support;

(b) a multi-agency effort to guide the development of efficient digital payments systems;

(c) a technology-enabled regulatory reporting system and smart surveillance;

(d) supporting a FinTech ecosystem; and

(e) building skills and competencies in technology.

FSTI Schemes

43 The MAS will commit $225m over the next five years under the FSTI scheme to provide support for the creation of a vibrant ecosystem for innovation. FSTI funds can be used for three purposes:

(a) *innovation centres*: to attract FIs to set up their research and development and innovation labs in Singapore.

(b) *institution-level projects*: to catalyse the development by FIs of innovative solutions that have the potential to promote growth, efficiency, or competitiveness.

(c) *industry-wide projects*: to support the building of industry-wide technology infrastructure that is required for the delivery of new and integrated services.

44 Several FIs have already set up their innovation centres or labs in Singapore, some under the FSTI, as well as a couple of others

that are in the pipeline. Some examples of FSTI-supported institution-level projects that are ongoing include:

(a) a decentralised record-keeping system based on block chain technology to prevent duplicate invoicing in trade finance;

(b) a shared infrastructure for a know-your-client utility;

(c) a cyber-risk test bed; and

(d) a natural catastrophe data analytics exchange.

MAS looks forward to seeing more of such innovative projects coming on board.

Digital payments

45 Changes in the payments scene in Singapore have picked up pace in recent years. Our retail banks have released their own versions of the mobile wallet or mobile payment application: *DBS PayLah!*, *UOB Mobile Cash*, *OCBC Pay Anyone*, *Singtel–Standard Chartered Bank Dash Pay* and *Maybank Mobile Money*. With the launch of Fast and Secure Transfers ("FAST") in March 2014, now at one's disposal, a ready infrastructure that allows customers of the participating banks to make domestic fund transfers to one another almost instantaneously from their computers or mobile devices.

46 But there is a lot more needed on the digital payments front.

(a) **Payments at stores and restaurants**. This is almost a "Uniquely Singapore" phenomenon. Many of our stores and restaurants have multiple points of sale ("POS") at their payment counters. This not only clutters valuable real estate but also makes life difficult for customers and merchants. As more stores and restaurants introduce self-checkout facilities to improve productivity, what is required is a unified POS – a single terminal, preferably mobile – that will allow merchants to enhance efficiency by simplifying front-to-back integration of their operations and enhance the shopping or dining experience of customers.

(b) **Reduce the use of cash and cheques**. It costs as much as $1.50 to process each cheque. The cost of cash is less obvious but just as real – in transportation, collection, delivery and protection of cash. We need to promote greater adoption of new payment technologies, including electronic Direct Debit Authorisation and fund transfers using mobile numbers or social networks.

47 MAS and the Ministry of Finance have been co-leading a multi-agency effort to address these issues and guide the development of efficient digital and mobile payment systems. The aim is to make payments swift, simple and secure. The vision is less cash, less cheques and fewer cards.

Regulatory reporting and surveillance

48 As the financial system becomes increasingly complex and inter-connected, MAS needs to sharpen its surveillance of the system with more timely, comprehensive and accurate information to identify and mitigate emerging risks. The vision is an interactive, technology-enabled regulatory reporting framework which will reduce ongoing reporting costs through the use of common data standards and automation, and at the same time, enable the dissemination of anonymised information to industry analysts and academics for deeper analysis of the financial system and its risks. MAS is still in the early days on this initiative and will work with the industry on how best to take this forward.

Supporting a FinTech ecosystem

49 The effort to grow a Smart Financial Centre must go beyond the financial industry, to help nurture a wider FinTech ecosystem. The industry needs a strong FinTech community that can generate ideas and innovations that FIs could adopt in their businesses, and provide a platform for collaborations with the industry to produce innovative solutions for defined problems and needs.

50 For those unaware, there is a vibrant FinTech start-up community that is growing over at the "JTC LaunchPad @ one-north" in Ayer Rajah Industrial Estate. MAS looks forward to

engaging FinTech start-ups more actively to better understand emerging innovations, as well as to help them design their solutions bearing in mind the regulations and risk considerations that apply to the financial industry.

Building skills and competencies in technology

51 Technology will disintermediate and make obsolete many jobs in the financial sector, but it will also create new ones. Finance professionals will need new capabilities, and the industry will need skills and expertise from other disciplines not traditionally associated with finance.

52 MAS and the financial industry must work together to prepare for the changes ahead on the jobs and skills front. Building capabilities and opportunities in FinTech will be a key area of focus in the financial sector's SkillsFuture initiative. MAS will work with the financial industry, the Institute of Banking and Finance, training providers, and the universities and polytechnics to provide learning pathways relevant for a Smart Financial Centre. MAS will also provide funding to FIs and other support for training opportunities, to help Singaporeans acquire specialist capabilities in the relevant areas of FinTech.

CONCLUSION

53 Although much of the foregoing is about technology and FinTech, the larger picture is about promoting a culture of innovation in our financial industry. Such innovation is not always about high-tech. It is about designing better work processes and creating new business models that will deliver higher growth, more enriching jobs, and better services for the consumer. Technology is very likely to be a key enabler for all this, and individuals must make a concerted effort to understand it and use it effectively.

Regulatory Challenges of Electronic Payment Systems and Electronic Money

The exchange and transfer of value have underpinned commercial transactions for as long as commerce has been conducted by humans. From payments made with tangible commodities and specie money to fiat money and beyond, the evolution of payment systems has propelled and changed the face of commerce over the years. But the real game changing developments have mostly taken place over the last 65 years, fuelled largely by technological innovations and alternative mindsets. Resulting in a dynamic payment systems industry that continues to churn out non-traditional players and ever mutating electronic payment systems, these developments at the frontier challenge the very notion of money as well as its regulators seeking to energise, yet manage, economic growth through money regulation and who are also charged with other regulatory responsibilities. This article tracks these developments and speculates at the journey ahead.

Joyce A **TAN***
LLB (Hons) (National University of Singapore);
Managing Partner, Joyce A Tan & Partners.

INTRODUCTION

1 Electronic payment systems ("e-payment systems") and electronic money ("e-money") have seen tremendous changes in the past few years. Innovative payment services such as Paypal, Apple Pay and Bitcoin have transformed the payments industry and created new and unique challenges for regulators. This article commences with a survey of the key historical developments in e-payment systems and e-money, before proceeding to discuss the role and challenges of regulation in the payments industry.

* Some of the ideas put forth in this article were first discussed during the panel on "Regulatory Challenges of Electronic Money and Electronic Payment Systems" which the author chaired. The author acknowledges the contributions of her panellists Cietan Kitney, Larry Lim, Harish Natarajan & James G Robinson.

A BRIEF HISTORY OF MONEY

2 Money has been defined as a medium of exchange – that is, a set of assets in an economy which people regularly exchange for goods and services from others.[1] Commodities such as salt, cacao seeds, cows and precious metals were among the earliest examples of money, and were used to supplement barter trade. When merchants wished to trade goods of unequal value, they would use quantities of a commodity to round out the exchange.[2] Standardised coins of precious metals were subsequently invented for the sale and purchase of all types of goods and services. This form of money – specie money – enhanced and expanded trade and commerce around the world.[3] Gold and silver coins gave way to paper currency, which was cheaper to print and more convenient to use. Early paper currencies were backed by precious metals and holders could exchange their paper notes at banks for their equivalent value in precious metals.[4]

3 Commodity and specie money no longer dominate modern trade and commerce – that honour belongs to fiat money. Unlike commodity and specie money, fiat money has no intrinsic value; instead, its value originates from government decree, or fiat.[5] Following the permanent suspension of the US dollar's convertibility into gold and the resulting end of the Bretton Woods

1 B Z Yang, "What is (Not) Money? Medium of Exchange ≠ Means of Payment" (2007) 51 *The American Economist* 101.

2 J Weatherford, *The History of Money* (Crown, 1997) at pp 19–20.

3 The earliest form of specie money was invented in the kingdom of Lydia at around 640–630 BC. See J Weatherford, *The History of Money* (Crown, 1997) at pp 30–36.

4 Paper currency originated in China, which was also the birthplace of paper. See J Weatherford, *The History of Money* (Crown, 1997) at p 126.

5 Fiat money is currency designated as "legal tender" and persons are compelled by law to accept it for payment of debts. See G Shoup, *International Guide to Foreign Currency Management* (Routledge, 2013) at pp 18–19.

system,[6] fiat money has become the dominant form of money used today.[7]

4 The payments industry developed out of the need to transfer and move money. Inter-bank settlement systems have their origins in the payment services offered by early banks:[8] customers of the same bank could request for transfers of funds between their accounts. Such bank transfers were considerably safer and more convenient than physically handing over sums of money. Subsequently, banks began to accept claims on each other to enable customers of different banks to transfer funds. Banks would resolve their claims by calculating the amounts due to and from one another, which is, clearing and settling the resulting obligations. Inter-bank settlement systems, together with institutions such as clearing houses and central banks, were developed to enable banks to efficiently clear and settle claims among themselves.[9]

5 Remittance services came about to facilitate small-scale cross-border money transfers because such transfers were not adequately served by banks.[10] Remittance service providers, such as Western

6 The Bretton Woods system was created after World War II to facilitate post-war reconstruction and international trade by creating an international basis for exchanging national currencies. Forty-four countries agreed to fix their exchange rates by tying their currencies to the US dollar; in turn, the US dollar would be convertible to gold at a fixed rate. Unfortunately, there was a surplus of US dollars by the 1960s arising from foreign aid, military spending and foreign investment, such that the US did not have enough gold to back the total volume of US dollars in world circulation. The overvaluation of the US dollar led the US to suspend the US dollar's convertibility into gold in 1971. By 1973, many major world economies had abandoned the Bretton Woods system by allowing their currencies to float freely against the US dollar. See J Weatherford, *The History of Money* (Crown, 1997) at p 183; M J Stephey, "A Brief History of the Bretton Woods System", *Time* (21 October 2008); Office of the Historian, "Milestones: 1969–1971, Nixon and the End of the Bretton Woods System" (31 October 2013), US Department of State.

7 J Weatherford, *The History of Money* (Crown, 1997) at p 186.

8 Examples of early banks include late-medieval money changers in Continental Europe and 17th century goldsmiths in England.

9 B Norman, R Shaw & G Speight, *The History of Interbank Settlement Arrangements: Exploring Central Banks' Role in the Payment System* (Working Paper No 412, June 2011).

10 "Remittances: Over the Sea and Far Away" *The Economist* (19 May 2012).

Union, have historically served migrant workers sending funds back to their families in their home countries, a service which remains very much alive today.[11] Cross-border remittances between money agents around the world typically rely on inter-bank settlement systems, although the exact mechanism for such money transfers may differ depending on the countries and currencies involved.[12] Remittances have been a significant source of capital for developing countries, and continue to play an important role in their economic growth.[13]

DEVELOPMENT OF E-PAYMENT SYSTEMS AND E-MONEY

6 E-payment systems and e-money evolved as further innovations to facilitate payments and money transfers, and have rapidly advanced over the past 65 years. Early examples of e-payment systems include credit and debit card services offered by banks and credit card companies in the 1950s. Internet and mobile payment services followed in the 1990s,[14] and paved the way for the recent introduction of smartphone-based mobile payment services.[15]

7 The development of e-money as an electronic surrogate for coins and banknotes was a significant milestone in the evolution of e-payment systems.[16] Popular examples of e-money involving stored value instruments include the CashCard and EZ-Link card in Singapore. Interestingly, in one of its earliest incarnations in the 1990s, e-money bore significant similarities to cryptography-based virtual currencies, that is, cryptocurrencies. In particular, DigiCash, one of the earliest e-money issuers, allowed users to make

11 R Esteves & D Khoudour-Castéras, "Remittances, Capital Flows and Financial Development during the Mass Migration Period, 1870–1913" (2011) 15 *European Review of Economic History* 443.

12 The World Bank, Committee on Payment and Settlement Systems, "General principles for international remittance services" (March 2006).

13 "Remittance Corridors: New Rivers of Gold" *The Economist* (28 April 2012).

14 D Roth, "The Future of Money: It's Flexible, Frictionless and (Almost) Free" *Wired* (22 February 2010).

15 F Martins, "The History of the Mobile Payments Experience" *Winthecustomer!* (9 June 2015).

16 S Levy, "E-Money (That's What I Want)" *Wired* (1 December 1994).

untraceable and secure money transfer transactions over the World Wide Web using cryptographic protocols developed by its founder, Chaum. After low demand for DigiCash's services forced it to eventually shut down in 1999,[17] developers of payment systems shifted their attention to stored value instruments such as transit fare cards, which could electronically store and transmit monetary value.[18] This initial popularity of stored value instruments over virtual currencies meant that the recognition of e-money at a regulatory level was directed towards stored value instruments. The E-Money Directive[19] adopted by the European Union in 2000 defined "electronic money" as "monetary value as represented by a claim on the issuer which is: (i) stored on an electronic device; (ii) issued on receipt of funds of an amount not less in value than the monetary value issued; (iii) accepted as means of payment by undertakings other than the issuer".[20] This definition was refined in 2009 to "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".[21]

8 This early appropriation of the expression "e-money" to the narrow confines of electronic stored value instruments representing fiat money, was a source of anecdotal confusion over the scope of e-money when virtual currencies subsequently re-emerged in the late 2000s in forms which did not represent fiat money value but had currency in the electronic world. Prominent

17 J Pitta, "Requiem for a Bright Idea" *Forbes* (1 November 1999).

18 Committee on Payment and Settlement Systems, "Survey of developments in electronic money and internet and mobile payments" *Bank for International Settlements* (March 2004) <http://www.bis.org/cpmi/publ/d62.pdf> (accessed 27 August 2015).

19 Directive 2000/46/EC of the European Parliament and of the Council on the taking up, pursuit of and prudential supervision of the business of electronic money institutions (18 September 2000) ("Directive 2000/46/EC").

20 Directive 2000/46/EC, Art 1(3)(b).

21 Article 2(2) of the Directive 2009/110/EC of the European Parliament and of the Council 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 (16 September 2009) ("Directive 2009/110/EC").

examples of virtual currencies include in-game currencies issued by online games, such as EverQuest and World of Warcraft, and cryptocurrencies such as Bitcoin.[22] Against the backdrop of such developments, regulators put forward definitions of "virtual currency" apparently intended to distinguish it from the definition of e-money as a stored value of fiat money. For example, the European Central Bank initially defined virtual currencies in 2012 as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community".[23] This definition was updated in 2015 based on developments in the regulation and operation of virtual currencies, to "a digital representation of value, not issued by a central bank, credit institution or an e-money institution, which, in some circumstances, can be used as an alternative to money".[24] While virtual currencies are often thought of as cutting-edge innovations in financial technology, many of them have their roots in the cryptographic protocols established by DigiCash, one of the first e-money issuers. In this sense, virtual currencies are essentially a new variation of an old idea.[25]

DRIVING FORCES

9 The evolution of e-payment systems and e-money have been driven by commercial, technological and ideological considerations, which have played out in a highly fluid and interconnected way. Technological advancements, such as smart cards and the World Wide Web,[26] have simultaneously satisfied

22 J Dibbell, "The Decline and Fall of an Ultra Rich Online Gaming Empire" *Wired* (24 November 2008).

23 European Central Bank, "Virtual Currency Schemes" (October 2012).

24 European Central Bank, "Virtual Currency Schemes – A Further Analysis" (February 2015).

25 K Griffith, "A Quick History of Cryptocurrencies BBTC – Before Bitcoin" *Bitcoin Magazine* (16 April 2014).

26 The Internet is not, strictly speaking, synonymous with the World Wide Web. The Internet refers to the infrastructure that connects computer networks around the world, while the World Wide Web is an avenue for transmitting data over the Internet. See K Wagstaff, "The Internet and the World Wide Web Are Not the Same Thing" *NBC News* (12 March 2014).

and fuelled commercial demands for cheap, fast, secure and convenient payment services. Libertarian ideologies have spurred inventors to create new technologies that challenge and subvert the status quo. Together, these drivers have propelled competition and innovation in the rapidly-evolving global payments industry.

Commercial

10 Developments in e-payment systems and e-money have been driven by commercial considerations and concerns of service providers, consumers and merchants, generally revolving on the cost, convenience and security of payments.

Service providers

11 Competition among service providers has been a major driving force behind the growth of e-payment systems, especially in the early days of the credit card industry. The Diners Club card is commonly credited as the first modern credit card, and was introduced by the Diners Club in 1950.[27] The Diners Club card was initially made of cardboard, and allowed cardholders to buy meals at participating restaurants. Diners Club would reimburse the restaurant for the cardholder's purchase, and bill the cardholder at the end of the month. Diners Club profited from extending such unsecured loans to cardholders by charging participating restaurants a small fee for every purchase, and charging cardholders an interest every month.[28] The remarkable popularity of the Diners Club card spurred banks and businesses to issue credit cards which could be used at a variety of establishments. In 1958, American Express Company introduced the American Express

27 Some department stores and oil companies introduced credit payment schemes in the 1800s so that customers could make purchases and pay for them at the end of the month. However, unlike modern credit cards, cards issued under these schemes could only be used at a single establishment. See J S Olsen, *Historical Dictionary of the 1950s* (Greenwood Publishing Group, 2000) at pp 66–67.

28 J S Olsen, *Historical Dictionary of the 1950s* (Greenwood Publishing Group, 2000) at pp 66–67.

Personal Card, a credit card initially dedicated to the payment of travel and entertainment expenses,[29] and in 1959, Bank of America Corporation launched the first general-use credit card, the BankAmericard.[30] The Master Charge credit card was launched in 1969 by a group of American banks to compete with the BankAmericard.[31] About a decade later, the BankAmericard name was changed to Visa,[32] followed by the name change from Master Charge to MasterCard.[33] Together with technological advancements such as magnetic stripe cards and data networks, robust competition among credit card service providers fuelled the growth of the global credit card industry.

12 The first debit cards were introduced by banks in the late 1970s as a substitute for cheques. These cards enabled moneys to be deducted from the cardholder's bank account when the cardholder made a purchase, and were generally issued to bank customers with large savings accounts, such as business executives.[34] Debit card usage dramatically increased in the late 1990s for two main reasons. First, banks introduced debit cards which cardholders could use at automated teller machines ("ATMs") to withdraw cash

29 American Express, "Our Story" <https://secure.cmax.americanexpress.com/Internet/GlobalCareers/Staffing/Shared/Files/our_story_3.pdf> (accessed 13 August 2015); American Express, "Company History and Development" <https://www.americanexpress.com/china/en/aboutamex/corpinfo_history.shtml> (accessed 24 November 2015).

30 The BankAmericard was considered a general-use credit card because it could be used for any type of purchase at participating merchants. The BankAmericard was also the first credit card to offer revolving credit, which allowed customers to pay down their balances over time. See Bank of America, "Introducing the modern credit card" <http://about.bankofamerica.com/en-us/our-story/birth-of-modern-credit-card.html> (accessed 13 August 2015).

31 MasterCard, "Key Milestones" <https://www.mastercard.us/en-us/about-mastercard/who-we-are/history.html> (accessed 14 August 2015).

32 The BankAmericard name was changed to Visa in 1976. See Bank of America, "Introducing the Modern Credit Card" <http://about.bankofamerica.com/en-us/our-story/birth-of-modern-credit-card.html> (accessed 13 August 2015).

33 The Master Charge name was changed to MasterCard in 1979. See MasterCard, "Key Milestones" <https://www.mastercard.us/en-us/about-mastercard/who-we-are/history.html> (accessed 14 August 2015).

34 M Lambert, "The History of Debit Cards" *Bright Hub* (7 June 2011).

from their bank accounts.[35] Second, the banks who issued credit cards, such as Visa and MasterCard, began to open up their credit card infrastructure, including their extensive electronic network linking cardholders, merchants, card-issuing banks and merchant banks, for use in their debit card services. Debit cards are now a convenient alternative to credit cards, and a strong competitor.[36]

13 Besides debit cards and despite their status as industry veterans, traditional credit card companies also began to face stiff competition from Internet-based payment services. The introduction of the World Wide Web in the early 1990s facilitated the transfer of funds at a much lower cost than traditional money transfers.[37] Providers of Internet-based payment services began to spring up to take advantage of this new technology. Paypal, which was launched in 1998, allowed users to quickly and inexpensively transfer funds through its online platform and rapidly established itself as a dominant player in the payments industry.[38] Paypal's success demonstrated the utility of online payments, and rival online payment processors such as Stripe were quickly established in its wake.[39] Stripe offers simple software and services for online businesses to receive electronic payments,[40] and its current customers include industry leaders such as Kickstarter and

35 S E Weiner, "Electronic Payments in the US Economy: An Overview" *Federal Reserve Bank of Kansas City* (1999). The issuance of debit cards with ATM access in the late 1990s also boosted the general utility of ATMs. See F Hayashi *et al*, "A Guide to the ATM and Debit Card Industry" *Federal Reserve Bank of Kansas City* (2003). Also see para 25 below for further information on ATMs.

36 F Hayashi *et al*, "A Guide to the ATM and Debit Card Industry" *Federal Reserve Bank of Kansas City* (2003).

37 T Long, "Aug 7, 1991: Ladies and Gentlemen, the World Wide Web" *Wired* (7 August 2012). For further discussion on the World Wide Web, see n 26 above.

38 PayPal relies on existing credit card and bank services to make money transfers. See PayPal, "Learn How PayPal Works" <https://www.paypal.com/webapps/mpp/pay-online> (accessed 14 August 2015).

39 M Wohlsen, "The Internet Needs a Better Way to Handle Money. This Startup has the Key" *Wired* (23 July 2014).

40 M Isaac, "Stripe, Digital Payments Start-Up, Raises New Funding and Partners with Visa" *The New York Times* (28 July 2015).

Twitter.[41] By providing an inexpensive, convenient and secure avenue for money transfers, Internet-based payment services began to pose a major threat not only to credit card companies, but to banks as well.[42]

14 On the back of the Internet, mobile payment applications accessible through smartphones, such as Google Wallet, Android Pay, Apple Pay and CurrentC, were also developed as alternatives to credit card services. Google first introduced Google Wallet in 2011 as a mobile payment system that enabled users to store their debit, credit, gift and loyalty card information on their smartphones, and use such information in the smartphone to make online payments. A further variation enabled a Google Wallet user with a smartphone equipped with near field communication ("NFC") capabilities to pay for purchases by securely transmitting such information to a point-of-sale terminal.[43] However, Google Wallet saw tepid success following its launch, and met with stiff competition from the introduction of Apple Pay by Apple in October 2014.[44] Apple Pay is a mobile payment system which shares significant similarities with Google Wallet: it allows users to upload their credit and debit card information to their NFC-equipped smartphones and use such smartphones to pay for purchases.[45] Google responded by introducing Android Pay in May 2015[46] which built on technology from Google Wallet, to compete with Apple Pay.[47] In contrast, CurrentC is a mobile payment system introduced by a consortium of US retailers in 2014 with the aim of replacing credit cards altogether. CurrentC uses quick response ("QR") codes

41 S Perez, "Stripes New Product Helps Marketplaces Go Global More Quickly" *TechCrunch* (23 March 2015).

42 D Roth, "The Future of Money: It's Flexible, Frictionless and (Almost) Free" *Wired* (22 February 2010).

43 M Geuss, "How Apple Pay and Google Wallet actually work" *Ars Technica* (30 October 2014). For an explanation of NFC technology, see para 26 below.

44 Apple, "Apple Pay Set to Transform Mobile Payments Starting October 20" *Apple Press Info* (16 October 2014).

45 M Geuss, "Google Wallet use grows after Apple Pay launch" *Ars Technica* (5 November 2014).

46 P Bhat, "Pay Your Way with Android" *Android Official Blog* (28 May 2015).

47 M Geuss, "Android Pay is All about Tokenisation; Google Wallet Takes a Backseat" *Ars Technica* (29 May 2015).

displayed on a cashier's payment terminal and scanned by the customer's smartphone,[48] or *vice versa*, to initiate and verify purchases at participating retailers. This system is designed to automatically apply discounts, use loyalty programmes and charge the customer for purchases. Unlike Android Pay or Apple Pay, CurrentC directly debits funds from a user's bank account, allowing retailers to avoid costly credit card charges.[49] These diverse offerings demonstrate considerable competition among mobile payment service providers *inter se*, even as such services seek to compete with and *vis-à-vis* banks, credit card companies and Internet payment services.

15 Service providers have employed various strategies to maintain their profitability in the highly competitive payments industry. To reduce operating costs, e-payment service providers have devised ways to reduce their exposure to credit card companies and banks. For example, Paypal allows users to use existing funds in their Paypal account to make payments to other Paypal users, which enables Paypal to avoid paying credit card or bank transfer fees for such transactions. This allows Paypal to charge lower transaction fees than traditional credit card services, making it more competitive and attractive to consumers.[50]

16 High transaction volumes and cross-border transactions expose service providers to significant security risks,[51] and maintaining consumer data protection and payment security is a major challenge for service providers. Some service providers have mitigated such risks through innovative technologies. For example, concerns over credit card fraud led to the introduction of the EMV standard, a chip-based authentication system named after the three

48 QR codes are similar to barcodes; when a user scans a QR code with a smartphone, the information embedded in the code is transmitted to the smartphone. See R Swaby, "QR Code" *Wired* (16 April 2013).

49 J Constine, "CurrentC is the Big Retailers' Clunky Attempt to Kill Apple Pay and Credit Card Fees" *Techcrunch* (25 October 2014).

50 D Roth, "The Future of Money: It's Flexible, Frictionless and (Almost) Free" *Wired* (22 February 2010).

51 S Bodow, "The Money Shot" *Wired* (September 2001).

service providers that invented it – Europay, Mastercard and Visa.[52] However, recent customer data thefts from major service providers such as JPMorgan Chase[53] demonstrate that despite such technological advancements, safeguarding consumer data remains a pressing issue in the payments industry.[54]

Consumers

17 Consumer demand for services offered by e-payment systems and e-money has been driven by factors such as cost, variety, convenience, security and privacy.

18 Faced with rising credit card fees, many consumers have turned to payment services with lower transaction costs such as Paypal.[55] Convenience and user-friendliness have also been major drivers of consumer demand for mobile payment applications, such as Android Pay, which enable consumers to make contactless payments using their smartphones.[56]

19 The growth in e-payment systems and e-money has significantly increased consumer demand for a variety of payment options.[57] Studies have observed that many consumers use a wide range of payment methods depending on the type of payment, the amount of the payment, and other complex factors. For example, a consumer might purchase a $5 car-wash token with cash, but pay for a more costly plane ticket using a credit card.[58] Service

52 K Poulson, "Why the Heyday of Credit Card Fraud is Almost Over" *Wired* (25 September 2014).

53 "JPMorgan Hacked: 70 million Client Names and Personal Information Stolen in Major Data Breach" *The Independent* (3 October 2014).

54 B Hardekopf, "The Big Data Breaches of 2014" *Forbes* (13 January 2015).

55 E Adamowsky, "Bitcoin: The Pros and Cons for Consumers and Merchants" *Yahoo! Finance* (2 March 2014).

56 T Spataro, "Apple Pay, Samsung Pay, Android Pay: What This Means for Banks" *Bank Innovation* (3 August 2015).

57 KPMG Financial Services Regulatory Risk Practice and the Americas Financial Services Regulatory Center of Excellence, "Payment Systems: Regulatory Interest in Payment Processors, Faster Payments, and Related Consumer Protections" (July 2015).

58 S L Schreft, "How and When Do Consumers Choose Their Payment Methods?" *The Federal Reserve Bank of Kansas City* (April 2006); M Benton

(*continued on the next page*)

providers have responded to the varying needs of consumers by providing diverse payment solutions with different characteristics.[59]

20 Acceptance by merchants has been another driver of consumer demand, as new payment systems that are not supported by small merchants face consumer reluctance in adopting such systems. For new payment services to gain global acceptance, consumers need to be able to use them at local eateries, street vendors and stores.[60]

21 On the flip side, consumer demand has been tempered by security and privacy concerns, and consumer data thefts have cast a pall over the payments industry.[61] This has made payment services that restrict access to personal data more appealing to consumers, such as services which use Bitcoin as a means of anonymous payment.[62]

Merchants

22 Acceptance by merchants has been a critical factor in the development of e-payment systems and e-money. Merchants have generally been less willing to adopt new payment systems where the costs of implementing and using them are high.[63] Installing the required infrastructure (for example, contactless payment terminals) and training employees to use new payment

---

et al, "The Boston Fed Study of Consumer Behavior and Payment Choice: A Survey of Federal Reserve System Employees" *Federal Reserve Bank of Boston* (14 February 2007).

59 Federal Reserve Bank of Cleveland, "Our Payments System: Challenges and Opportunities" (31 December 1997).

60 Apple Pay was initially less popular among consumers despite its strong marketing campaign due to its limited acceptance by small merchants. See G Marks, "Why is Almost No One Using Apple Pay?" *Forbes* (1 June 2015).

61 B Hardekopf, "The Big Data Breaches of 2014" *Forbes* (13 January 2015).

62 Bitcoin users do not have to disclose personal information when making payments using Bitcoin. This provides protection against identity theft. See Bitcoin Foundation, "Frequently Asked Questions" <https://bitcoin.org/en/faq #what-are-the-advantages-of-bitcoin> (accessed 7 September 2015).

63 Bank for International Settlements, "Implications for Central Banks of the Development of Electronic Money" (October 1996).

technologies represent additional costs,[64] which are especially unpalatable to small merchants.[65] Service providers have responded by developing cheaper and more convenient alternatives to pricey point-of-sale terminals, such as tablet and smartphone applications.[66] Service providers have also significantly reduced transaction fees to incentivise merchants and compete with credit card companies, banks and other service providers.

23 Another incentive for merchants to support new payment technologies has been their "cool factor" – by supporting novel and trendy technologies, merchants have been able to distinguish themselves from their competitors and attract tech-savvy consumers.[67] These incentives have contributed greatly to the growing popularity of innovative payment services among merchants, as can be seen from the rise of new entrants such as Stripe.[68]

Technological

24 Technology has been a major driving force in the payments industry since the introduction of the credit card in the 1950s. While early credit cards such as the Diners Club card were initially made of cardboard[69] and later issued as embossed plastic cards, it was the invention of the magnetic stripe card in the 1960s that catalysed the establishment of the global credit card industry.

64 Payment terminals can be expensive, and represent a significant investment on the part of the merchant. See R Reader, "Forget about Payment Apps: The New Battle is around Payment Terminals" *Venture Beat* (29 October 2014).

65 G Marks, "Why is Almost No One Using Apple Pay?" *Forbes* (1 June 2015).

66 Services providers, such as PayPal and BitPay, allow merchants to accept payments using smartphone and tablet applications. See PayPal, "PayPal Here" <https://www.paypal.com/webapps/mpp/credit-card-reader> (accessed 7 September 2015); BitPay, "Bitcoin Checkout" <https://bitpay.com/bitcoin-for-retail> (accessed 7 September 2015).

67 M Sullivan, "Here's how Apply Pay will Win with Small Merchants" *Venture Beat* (17 April 2015).

68 M Wohlsen, "Stripe Leads the Race to the $1 Trillion Future of Mobile Payments" *Wired* (30 September 2014).

69 American Express, "Our Story" <https://secure.cmax.americanexpress.com/Internet/GlobalCareers/Staffing/Shared/Files/our_story_3.pdf> (accessed 13 August 2015).

Together with point-of-sale devices, data networks and computers, magnetic stripe cards enabled credit card information to be transmitted efficiently, accurately and securely.[70]

25 ATMs were introduced in the late 1960s, and required users to have a personal identification number and a special paper voucher, which could be inserted into the machine in return for paper currency.[71] ATMs were subsequently modified to accept magnetic stripe cards and smart cards instead of paper vouchers, which greatly improved the security of ATM transactions.[72]

26 The introduction of smart card technology in the 1970s enabled plastic cards to be outfitted with microprocessors,[73] and allowed credit cards with enhanced capabilities to be issued. Although the ATM was invented earlier than and independently of smart card technology, ATMs came to embrace smart card technology. Smart card technology also paved the way for credit and debit cards to be outfitted with the EMV chip-authentication system which provided greater protection against fraud.[74] Credit cards with additional NFC capabilities[75] have also enabled consumers to make convenient and secure payments by tapping their card against a point-of-sale terminal.[76] These technological advancements contributed towards the popularity of credit cards and the overall growth of the payments industry.

---

70 The magnetic stripe card was invented by IBM engineer Forrest Parry: see IBM, "Magnetic Stripe Technology" <http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/magnetic> (accessed 13 August 2015).

71 "Enfield's Cash Gift to the World" *BBC* (27 June 2007).

72 "All ATM Cards to have Secure Smart Chips Installed by 2014" *AsiaOne* (21 January 2012).

73 R Moreno obtained the first patent for smart cards in 1974: see P Davidson, "Roland Moreno: Inventor who Missed Out on Global Recognition for his Computer Chip Smart Card" *The Independent* (4 May 2012).

74 O Kharif & E Dexheimer, "Credit and Debit Cards Lag on Upgrades" *Bloomberg Businessweek* (2 October 2015).

75 NFC technology evolved from radio frequency identification technology, and allows data to be transmitted over short distances (*eg*, 4cm). See C Foresman, "Near Field Communications: A Technology Primer" *Ars Technica* (9 February 2011).

76 C Faulkner, "What is NFC? Everything you Need to Know" *Techradar* (20 April 2015).

27 Smart card technology facilitated the development of e-money in the form of stored value cards.[77] Stored value cards were first used in France for public phone networks in the 1980s,[78] and the ease and convenience they offered for payment systems made them particularly useful for transit fare payments. By the early 2000s, stored value cards were used in public transportation networks around the world. Examples of such applications include the Octopus card in Hong Kong, and the EZ-Link card in Singapore. Stored value cards are now one of the most popular forms of e-money and are used in countries all over the world.[79]

28 The single greatest game changer to the payments industry has arguably been the World Wide Web. Before the World Wide Web was introduced in the 1990s,[80] payment networks were dependent on expensive infrastructure maintained and monopolised by banks and credit card companies. The World Wide Web provided an inexpensive, accessible and superior alternative to such infrastructure, which opened up the payments industry to new players, such as technologists and entrepreneurs.[81] The World Wide Web also facilitated convergence between mobile and computer devices, telecommunication networks and various computing platforms.

29 This convergence accelerated technological developments in the payments industry, leading to the invention of virtual currencies and smartphone-based mobile payment systems. Interestingly, the first mobile payment service was offered by Coca-Cola in 1997, when it allowed a user to purchase drinks from any designated vending machine by sending a mobile text message to

77 Committee on Payment and Settlement Systems, "Survey of Developments in Electronic Money and Internet and Mobile Payments" *Bank for International Settlements* (March 2004).

78 A M Al-Khouri, *Critical Insights from Government Projects* (Chartridge Books Oxford, 2013) at p 147.

79 Committee on Payment and Settlement Systems, "Survey of Developments in Electronic Money and Internet and Mobile Payments" *Bank for International Settlements* (March 2004).

80 For further discussion on the World Wide Web, see n 26 above.

81 D Roth, "The Future of Money: It's Flexible, Frictionless and (Almost) Free" *Wired* (22 February 2010).

that vending machine.[82] Since then, innovations in mobile technology, especially the introduction of smartphones with NFC capabilities, have driven similarly ground-breaking developments in mobile payments, culminating in the introduction of Android Pay, Apple Pay and CurrentC.[83] Arguably, these mobile payment services are the next wave in the evolution of payment services. Consumers have been the ultimate beneficiaries of these new technologies, because they now have access to a wider array of payment services at lower costs.[84]

Ideological

30 Libertarian ideals have been influential in the development of e-money, and have inspired the creation of virtual currencies which did not need to be sustained by financial institutions, central banks or governments.

31 Many early e-money businesses were inspired by libertarian ideals. For example, Chaum founded DigiCash,[85] which issued anonymous and untraceable e-money, to help individuals prevent overzealous governments from monitoring or blocking their transactions.[86] Another e-money business founded on a similar libertarian outlook was E-Gold, an electronic currency backed by gold and other precious metals. E-Gold was established by Douglas Jackson in 1996 as a private currency that would circulate independently of government controls. E-Gold users were allowed to anonymously open online accounts and make fund transfers; unfortunately, this anonymity also allowed criminal organisations to use E-Gold to covertly transmit funds. By 2009, E-Gold had been effectively shut down by the US authorities for engaging in money

82 F Martins, "The History of the Mobile Payments Experience" *Winthecustomer!* (9 June 2015).

83 M Geuss, "Google Wallet use grows after Apple Pay launch" *Ars Technica* (5 November 2014); M Geuss, "Android Pay is All about Tokenisation; Google Wallet Takes a Backseat" *Ars Technica* (29 May 2015).

84 J Greenberg, "Tech Upended Banks and Stock Trading. Insurance is Next" *Wired* (1 July 2015).

85 For further discussion on DigiCash, see para 7 above.

86 S Levy, "E-Money (That's What I Want)" *Wired* (December 1994).

laundering and operating as an unlicensed money transmission business.[87]

32 Failed e-money businesses such as DigiCash and E-Gold evidently shared a common exposure: they relied on a central operator that could be shut down by government authorities or simply go out of business. When Bitcoin was introduced in 2009 by Nakamoto,[88] this exposure was addressed by its decentralised peer-to-peer network that obviated the need for a central operator.[89] Bitcoin uses cryptographic technologies and a shared public ledger called the "blockchain" to track, confirm and secure transactions. Like Chaum's DigiCash and Jackson's E-Gold, Nakamoto's Bitcoin has been designed in the belief that to protect individual autonomy, government oversight over monetary systems and individual citizens should be minimal at best.[90]

33 Libertarians and privacy enthusiasts were early users of Bitcoin because it allowed them to make secure and potentially untraceable payments without relying on centralised banking institutions.[91] Following its rapid rise in popularity in 2013, Bitcoin became a target for speculative investments, making its exchange rates with various fiat currencies increasingly volatile.[92] The absence of a central regulator has made Bitcoin's users vulnerable to scams and thefts.[93] Despite these issues, many Bitcoin businesses, ranging from Bitcoin exchanges[94] to electronic wallet

87 K Zetter, "Bullion and Bandits: The Improbable Rise and Fall of E-Gold" *Wired* (9 June 2009).

88 To date, the identity of "Satoshi Nakamoto" remains a mystery. See M O'Leary, "The Mysterious Disappearance of Satoshi Nakamoto, Founder & Creator of Bitcoin" *Huffington Post* (11 May 2015).

89 M Venezky, "The Rise and Fall of Bitcoin" *Wired* (23 November 2011).

90 S Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" *Bitcoin*; R Reitman, "Bitcoin – A Step Towards Censorship-Resistant Digital Currency" *Electronic Frontier Foundation* (20 January 2011).

91 A Lowrey, "My Money is Cooler Than Yours" *Slate* (18 May 2011).

92 J Light, "Should You Invest in Bitcoin?" *The Wall Street Journal* (23 November 2013).

93 HM Treasury, "Digital Currencies: Response to the Call for Information" (March 2015).

94 Bitcoin Foundation, "How to Buy Bitcoins" <http://howtobuybitcoins.info/#!/> (accessed 1 September 2015).

providers[95] and even remittance service providers,[96] have sprung up in the past few years. Financial institutions, such as Barclays and Credit Suisse, are also investigating potential uses of the blockchain for financial market technology platforms.[97] While there may be doubts if Bitcoin can transcend its libertarian origins and become a globally accepted mainstream currency,[98] its future does not appear to be without promise.[99]

REGULATION OF PAYMENT SYSTEMS

Objectives

34 Payment system regulations around the world have generally been implemented to address the broad policy objectives of safety and efficiency.[100] Safety refers to the resilience, security and stability of payment systems, whereas efficiency is achieved when payments can be made quickly, cheaply and effectively. Safe and efficient payment systems facilitate the use of money as an effective means of payment, engender public confidence in electronic transactions, enable the smooth functioning of financial markets and promote economic growth.[101]

95 Bitcoin Foundation, "Choose your Bitcoin Wallet" <https://bitcoin.org/en/choose-your-wallet> (accessed 1 September 2015).

96 F Graillot, "Bitcoin Might Be the Next Big Thing in the Remittance Market" *TechCrunch* (25 May 2015).

97 C Khaw, "Nine Major Banks Working on Bitcoin-like Block Chain Tech for Market Trading" *Ars Technica* (17 September 2015).

98 PricewaterhouseCoopers, "Virtual Currencies: Out of the Deep Web, Into the Light" (March 2014).

99 D Wolman, "Bitcoin's Radical Days are Over. Here's How to Take it Mainstream" *Wired* (30 October 2013).

100 Monetary Authority of Singapore, "Consultation Paper: Payment Systems Oversight Act" (April 2003); Bank for International Settlements, Committee on Payment and Settlement Systems, "Central Bank Oversight of Payment and Settlement Systems" (May 2005).

101 Bank of Canada and the Department of Finance, "The Canadian Payments System: Public Policy Objectives and Approaches" *Bank of Canada* (May 1997).

Safety

35 Safe payment systems are stable and secure, and facilitate the effective functioning of financial markets and economies.[102] Safety in payment systems can be enhanced by protecting payment systems from credit, liquidity and settlement risks, and by ensuring that transactions which have been effected by such systems are final and irrevocable.[103] To achieve these objectives, the Payment and Settlement Systems (Finality and Netting) Act[104] ("PSSA") was introduced in Singapore in 2002 to provide the broad legal foundations for the operation of stable payment and settlement systems so as to reduce the risk of systemic disruptions to Singapore's financial system.[105] The PSSA empowers the Monetary Authority of Singapore ("MAS") to designate payment and settlement systems, which are exempt from the application of specific legal rules, including the rule in insolvency law for the unwinding of specific type of transactions. In determining whether to designate a system, MAS will consider the systemic risks associated with that system.[106] Payment systems that have been designated under the PSSA include (i) the MAS Electronic Payment System, the real-time gross settlement system operated by MAS for the settlement of funds between banks,[107] and (ii) the Continuous Linked Settlement system, a global payment and settlement system that aims to eliminate foreign exchange settlement risk due to time

102 Bank of Canada and the Department of Finance, "The Canadian Payments System: Public Policy Objectives and Approaches" *Bank of Canada* (May 1997).

103 The Monetary Authority of Singapore & The Attorney-General's Chambers of Singapore, "Legal Protection for Financial Payment Systems" (15 August 2002).

104 Cap 231, 2003 Rev Ed.

105 *Singapore Parliamentary Debates, Official Report* (25 November 2002), vol 75 at cols 1539–1542 (Lee Hsien Loong, Deputy Prime Minister and Minister for Finance).

106 Payment and Settlement System (Finality and Netting) Act (Cap 223, 2003 Rev Ed) s 3; *Singapore Parliamentary Debates, Official Report* (25 November 2002), vol 75 at cols 1539–1542 (Lee Hsien Loong, Deputy Prime Minister and Minister for Finance).

107 Monetary Authority of Singapore, "MAS Electronic Payment System (MEPS+)" (21 June 2014).

zone differences among international banks.[108] Thus, the PSSA provides an omnibus solution to the risks that would otherwise surround the operation of payment and settlement systems by according legal protection to, and thereby preserving the integrity and finality of transactions processed under, systems designated by MAS.[109]

36 Safe payment systems are also necessary to combat criminal activity, especially money laundering and terrorism financing.[110] As such, MAS has implemented anti-money laundering and countering the financing of terrorism ("AML/CFT") regulations to protect the integrity of Singapore's financial system from illegal activities and flows of illicit funds. E-money issuers,[111] money changing and remittance businesses[112] and other financial institutions are therefore required to put in place appropriate controls to detect and deter the flow of illicit funds through the financial system in Singapore. Such controls include customer due diligence checks, regular account reviews and monitoring and reporting of suspicious transactions.[113]

108 Monetary Authority of Singapore, "Continuous Linked Settlement System" (21 June 2014).

109 *Singapore Parliamentary Debates, Official Report* (25 November 2002), vol 75 at cols 1539–1542 (Lee Hsien Loong, Deputy Prime Minister and Minister for Finance).

110 Department of Finance Canada, "Balancing Oversight and Innovation in the Ways We Pay: A Consultation Paper" (13 April 2015).

111 MAS has issued AML/CFT measures applying to entities which issue stored value facilities. See MAS Notice PSOA-N02: Notice to Holders of Stored Value Facilities on Prevention of Money Laundering and Countering the Financing of Terrorism (5 November 2007) <http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Anti_Money%20Laundering_Countering%20the%20Financing%20of%20Terrorism/PSOAN02%20Revised%20Notice%20to%20Holders%20of%20SVF.pdf> (accessed 12 October 2015).

112 Money-Changing and Remittance Businesses Act (Cap 187, 2008 Rev Ed).

113 Monetary Authority of Singapore, "Anti-Money Laundering/Countering the Financing of Terrorism" (4 May 2015).

Efficiency

37 Efficient payment systems operate with reasonable costs and timely and simple processes, thereby providing cheap and convenient payment services for users. The Payment Systems (Oversight) Act ("PSOA") was promulgated in 2006 to promote the efficiency and safety of "stored value facilities" ("SVFs") and institutions which issue such SVFs.[114] An SVF is effectively e-money,[115] being a facility that represents monetary value and is used for the payment of goods and services up to that stored value, and which can be in various forms, such as magnetic stripe cards, smart cards and Internet accounts.[116] The PSOA distinguishes between a widely accepted SVF and a non-widely accepted SVF. An SVF is deemed a widely accepted SVF where its aggregate stored value exceeds $30m, which must be guaranteed by an approved bank and the holder of which must be approved by MAS.[117] In contrast, an SVF with an aggregate stored value not exceeding $30m is regarded as a non-widely accepted SVF and does not need to be guaranteed by any bank nor the specific approval of MAS, although it is still subject to stipulated conditions and requirements under the PSOA.[118] By such distinction, the PSOA reflects a regulatory approach that operates on the basis that the prescribed amount of $30m is a "proxy indicator for how widely used and accepted"[119] an SVF is, and that some SVFs which are less widely accepted have a "lower level of funds-at-risk"[120] than those which are more widely accepted.[121] In doing so, the PSOA seeks to strike a balance between addressing the safety of widely accepted SVFs and preserving the

114 Payment Systems (Oversight) Act (Cap 222A, 2007 Rev Ed) s 4.

115 For a detailed explanation on e-money, see paras 6–8 above.

116 Monetary Authority of Singapore "Stored Value Facility Guidelines" (1 June 2006).

117 Payment Systems (Oversight) Act (Cap 222A, 2007 Rev Ed) ss 35–36.

118 Payment Systems (Oversight) Act (Cap 222A, 2007 Rev Ed) ss 29–32.

119 Monetary Authority of Singapore, "Draft Payment Systems (Oversight) Bill" (December 2004).

120 Monetary Authority of Singapore, "Draft Payment Systems (Oversight) Bill" (December 2004).

121 J A Tan & D Seng, "A Review of IT Law Developments in Singapore" in *Singapore Academy of Law Conference 2006 – Developments in Singapore Law between 2001 and 2005* (K S Teo gen ed) (Singapore Academy of Law, 2006).

efficiency, innovation and competition for smaller-scale SVF schemes, that is, non-widely accepted SVFs.[122]

Oversight

38 As the central bank of Singapore, MAS's mission is to promote sustained non-inflationary economic growth through appropriate monetary policy formulation and close macroeconomic surveillance of emerging trends and potential vulnerabilities.[123] To this end, MAS conducts integrated supervision of the financial services sector and oversees payment systems in Singapore.[124]

39 To support the oversight and policy-making functions of MAS, the PSOA confers on MAS the power to gather information from all relevant parties in any payment system in Singapore,[125] including details on the operation of, and the pricing of services offered by such payment systems.[126] Such information may be used by MAS to monitor trends and developments in the payments industry, and fine-tune its oversight framework for payment systems where appropriate.[127]

40 Beyond such specific regulations, MAS is also vested with the general power to "require any financial institution or class or classes of financial institutions whose operations are considered by [MAS] to affect (a) monetary stability and credit and exchange

122 Tharman Shanmugaratnam, "The Payment Systems (Oversight) Bill: Second Reading Speech by Mr Tharman Shanmugaratnam, Minister for Education and Deputy Chairman, Monetary Authority of Singapore" *Monetary Authority of Singapore* (16 January 2006).

123 Monetary Authority of Singapore, "About MAS" (14 July 2014).

124 Monetary Authority of Singapore, "Annual Report 2012/2013" *Parliament of Singapore*.

125 Tharman Shanmugaratnam, "The Payment Systems (Oversight) Bill: Second Reading Speech by Mr Tharman Shanmugaratnam, Minister for Education and Deputy Chairman, Monetary Authority of Singapore" *Monetary Authority of Singapore* (16 January 2006).

126 Payment Systems (Oversight) Act (Cap 222A, 2007 Rev Ed) s 6.

127 Tharman Shanmugaratnam, "The Payment Systems (Oversight) Bill: Second Reading Speech by Mr Tharman Shanmugaratnam, Minister for Education and Deputy Chairman, Monetary Authority of Singapore" *Monetary Authority of Singapore* (16 January 2006).

conditions in Singapore; (b) the development of Singapore as a financial centre; or (c) the financial situation of Singapore generally, to be approved by [MAS] for the purpose of carrying on business in Singapore".[128] This overarching power allows MAS to regulate such institutions without necessarily having to pass further statutory legislation.

Challenges and considerations

41 In the constantly-evolving payments industry where the identities of service providers and the shape of frontier technology are ever dynamic, regulators are challenged by the inherent trade-offs that result from deciding one way or the other, on the nature, scope and extent of regulation for e-payment systems and e-money. A light-touch regulatory regime with minimal restrictions may encourage innovation, but fail to provide legal clarity, certainty and safety. Strict and comprehensive regulations may enhance consumer protection and reduce financial crime, but also create high compliance costs for businesses and hinder industry growth. A proportionate regulatory response to innovative payment businesses and technologies is necessary to promote industry growth while safeguarding societal and economic interests.[129]

Control and supervision

42 Payments regulators around the world have traditionally addressed policy objectives such as crime control, consumer protection and monetary stability through regulatory control and supervision, which have become increasingly complex and challenging in light of recent innovations and developments in the payment industry.[130]

128 Monetary Authority of Singapore Act (Cap 185, 1999 Rev Ed) s 28(1).

129 H McKenzie, "The Long Arm of the Law" *Banking Technology* (30 September 2014).

130 K A Dolan, "M-Pesa and GCash: Can 'Lean Regulation' Be a Gamechanger for Financial Innovation?" *Forbes* (3 October 2013); A Neumann, "Fostering Payments Innovations" *Chicago Fed Letter* (2015).

Criminal activities

43 As payment systems may be used to facilitate criminal activities, especially money laundering and terrorism financing,[131] regulators around the world have been led to impose AML/CFT safeguards on e-payment systems and e-money including those that require identity verification of customers. However, such safeguards have created challenges for payment service providers serving low-income customers, such as mobile payment systems or remittance businesses operating in developing countries. These service providers may find it difficult to comply with customer verification requirements, as low-income people often lack formal identification documentation, and developing countries may lack independently verified sources of data that could identify and verify customers, such as voter registration records and national identification cards.[132]

44 Innovative e-payment systems that do not need to rely on centralised banking institutions, and yet enable effective and anonymous payment transactions, such as Bitcoin, have also proven to be particularly useful to criminal activities[133] such as money laundering[134] and illegal drug purchases.[135] The absence of a central issuer or regulator who can be held accountable for the illicit activities has posed a problem for government authorities. Such authorities have faced significant difficulties in applying AML/CFT laws to anonymous transactions conducted using virtual

131 Financial Action Task Force, "Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services" *Financial Action Task Force* (June 2013); Financial Action Task Force, "Virtual Currencies: Key Definition and Potential AML/CFT Risks" *Financial Action Task Force* (June 2014).

132 T Abell & V Tsianaxis, "AML/CFT: Balancing Regulation with Innovation" *Consultative Group to Assist the Poor* (23 January 2015).

133 Z Kleinman, "Bitcoin Island: Cleaning Up the Crypto Currency" *BBC News* (24 April 2015).

134 A Greenberg, "'Dark Wallet' is About to Make Bitcoin Money Laundering Easier than Ever" *Wired* (29 April 2014).

135 A Greenberg, "Crackdowns Haven't Stopped the Dark Web's $100m Yearly Drug Sales" *Wired* (12 August 2015).

currencies, including Bitcoin.[136] Despite these challenges, AML/CFT regulations remain in place over such payment systems. For example, in the US, Bitcoin exchanges are subject to anti-money laundering regulations, and are required to register with the federal government, collect customer information and report suspicious activities.[137] Notably, compliance costs have forced some smaller Bitcoin exchanges to exit the market.[138] MAS announced in 2014 that it will impose AML/CFT regulations on Bitcoin exchanges similar to those imposed on money changers and remittance businesses who undertake cash transactions.[139] However, it is unclear if such regulations can be effectively adapted to address the unique characteristics of Bitcoin, especially its operation as a decentralised virtual currency.[140]

Consumer protection

45 Consumer protection has also been a key concern for regulators.[141] Many countries have instituted e-money regulations, such as the PSOA in Singapore,[142] and the E-Money Directive in the European Union,[143] to ensure that e-money issuers provide effective

136 Financial Action Task Force, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks" *Financial Action Task Force* (June 2014).

137 In 2013, the Financial Crimes Enforcement Network issued new guidelines expressly addressing regulatory requirements for "de-centralized virtual currencies": see Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (18 March 2013); T B Lee, "US Regulator: Bitcoin Exchanges must Comply with Money-laundering Laws" *Ars Technica* (20 March 2013).

138 HM Treasury, "Digital Currencies: Response to the Call for Information" (March 2015).

139 Monetary Authority of Singapore, "MAS to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks" (13 March 2014).

140 A Loke, "Virtual Currency Regulation in Singapore" (2015) 1(2) *Journal of Financial Regulation* 290.

141 Group of Ten, "Electronic Money: Consumer Protection, Law Enforcement, Supervisory and Cross Border Issues" *Bank of International Settlements* (April 1997).

142 Payment Systems (Oversight) Act (Cap 222A, 2007 Rev Ed).

143 Directive 2009/110/EC of the European Parliament and of the Council 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

(*continued on the next page*)

protection for consumers. E-money issuers may also be obliged to protect personal data of consumers under existing data protection regulations,[144] and are also subject to supervision and oversight of government authorities.[145] Broadly speaking, countries that monitor compliance and enforce consumer protection regulations discourage abusive service providers from entering or remaining in the payments industry. Such regulations help to instill trust in legitimate payment services, and are important enablers for the uptake of such services.[146]

Monetary stability

46 The proliferation of e-money in the different forms and forums held and used by consumers could potentially affect the behaviour of monetary aggregates,[147] which is an important factor to be considered in the work of a financial regulator.[148] To monitor

repealing Directive 2000/46/EC (16 September 2009) ("Directive 2009/110/EC").

144 For example, e-money issuers would be obliged to protect their users' personal data which they handle or gain access to, under legislation such as the Personal Data Protection Act 2012 (Act 26 of 2012) in Singapore and European Union Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (24 October 1995).

145 For example, the Financial Conduct Authority regulates the issuance of e-money in the UK, and the Monetary Authority of Singapore regulates the issuance of stored value facilities in Singapore. See Financial Conduct Authority, "Electronic Money Institution" <https://small-firms.fca.org.uk/firms-sectors/electronic-money-institution> (accessed 11 September 2015); and Monetary Authority of Singapore, "Stored Value Facilities Guidelines" <http://www.mas.gov.sg/regulations-and-financial-stability/regulations-guidance-and-licensing/payment-and-settlement-systems/guidelines/payment-systems-oversight-act-2006/2006/stored-value-facility-guidelines.aspx> (accessed 23 February 2016).

146 R Grady, "'Model Law for Best Practice in Financial Consumer Protection': An Important Driver for Universal Financial Access" *World Bank* (7 February 2015); K Prochaska, "What's the Linkage between Consumer Protection and Financial Access?" *Alliance for Financial Inclusion* (17 August 2015).

147 Monetary aggregates measure the amount of money circulating in an economy. See the Organisation for Economic Co-operation and Development, "Glossary of Statistical Terms: Monetary Aggregates" (23 October 2012).

148 Board of Governors of the Federal Reserve System, "Current FAQs" (24 January 2014).

such monetary aggregates, central banks may require information on the outstanding amounts of e-money from issuers, and on e-money usage in general.[149] The broad information gathering powers conferred by the PSOA grants MAS the ability to adjust to significant changes in the popularity of e-money, and to fine-tune its policies where necessary.[150]

47 Similarly, the widespread adoption of virtual currencies as an alternative to fiat currency may have an effect on the money supply in an economy.[151] However, due to the current relative low use of virtual currencies, regulators such as the Bank of England and the European Central Bank have concluded that virtual currencies do not presently pose a material risk to monetary stability in their respective countries.[152] MAS has indicated that it will continue to monitor developments in this area and consider implementing regulations to address the risks posed by virtual currencies.[153]

"Wait-and-see" approach

48 Regulators have generally exercised control and supervision over e-payment systems and e-money through legislation and various regulatory bodies. However, new developments in the payments industry, such as mobile payment systems which cater to low-income customers and innovative payment services such as Bitcoin, pose challenges to these tried-and-tested regulatory mechanisms. In response, some regulators have favoured adapting,

149 US Department of the Treasury, "An Introduction to Electronic Money Issues" (20 September 2015).

150 Tharman Shanmugaratnam, "The Payment Systems (Oversight) Bill: Second Reading Speech by Mr Tharman Shanmugaratnam, Minister for Education and Deputy Chairman, Monetary Authority of Singapore" *Monetary Authority of Singapore* (16 January 2006). For further discussion on the Monetary Authority of Singapore's information gathering powers, see para 39 above.

151 R Ali *et al*, "The Economics of Digital Currencies" (2014) 54(3) *Bank of England Quarterly Bulletin* 276.

152 R Ali *et al*, "The Economics of Digital Currencies" (2014) 54(3) *Bank of England Quarterly Bulletin* 276; European Central Bank, "Virtual Currency Schemes – A Further Analysis" (February 2015).

153 Monetary Authority of Singapore, "MAS to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks" (13 March 2014).

using or extending existing regulations as a short term measure, and adopting a "wait-and-see" approach towards establishing bespoke regulatory regimes. Regulators have also been more reluctant to completely ban new payment services, as doing so might reduce the visibility of transactions and encourage the illegitimate use of such services.[154]

Facilitation and collaboration

49 Without a robust regulatory framework, it may be difficult for new and innovative payment services to gain and maintain credibility and legitimacy within the payments industry. However, complex regulations may create high compliance costs and stifle businesses. Conversely, a consistent and proportionate regulatory approach would reduce the cost and complexity of compliance, thereby encouraging innovation and facilitating competition among new and established industry players.[155]

50 Creating an attractive and supportive environment for service providers is likely to encourage innovation and growth in the payment industry, and the development of efficient payment services. Beyond financial incentives, regulators may even create initiatives to promote best practices, standardisation and interoperability between service providers, merchants and other industry players.[156] Financing research grants to academic institutions, banks and businesses can enable regulators to facilitate research into new financial technologies. Regulators may also collaborate with industry players to institute regulations that encourage legitimate uses of payment services while clamping down on criminal activity.[157]

154 HM Treasury, "Digital Currencies: Response to the Call for Information" (March 2015).

155 HM Treasury, "Digital Currencies: Response to the Call for Information" (March 2015).

156 B Fung *et al*, "Electronic Money and Payments: Recent Developments and Issues" *Bank of Canada* (April 2014).

157 HM Treasury, "Digital Currencies: Response to the Call for Information" (March 2015).

51 Industry collaboration facilitates flexible, realistic and proportionate regulation, as industry players engaging in legitimate business activities have an interest in quashing criminal activity, so as to maintain consumer trust and confidence. For example, regulators at the Central Bank of Kenya collaborated with the operators of M-Pesa, a mobile payment platform in Kenya, to create a regulatory framework that mitigates systemic risks while providing the M-Pesa operators room to innovate and grow.[158] Spurred by this regulatory support, M-Pesa has become one of the most successful mobile payments platforms in the world.[159]

52 The case for industry self-regulation as a viable, if not preferable, option is founded on the motivation of industry players to protect their investments and promote their business interests,[160] and the apprehension that prescriptive regulation may inhibit industry players from devising flexible solutions and best practices to address illegitimate activities. Such flexible solutions have been pursued by virtual currency businesses, which have used creative technological solutions like multi-signature authentication and escrow accounting to enhance consumer protection and thereby gain acceptance of the solutions offered. Open-source technologies, such as the Bitcoin blockchain, have also helped industry players to independently monitor and regulate payment transactions.[161]

53 The availability and flexibility of these internal regulatory mechanisms have made self-regulation a realistic alternative to top-down, government-driven and prescriptive regulations. The UK government has decided to collaborate with the virtual currency industry to develop voluntary standards for consumer protection. By creating a regulatory framework based on industry best practice standards, the UK government aims to address crime and

158 K A Dolan, "M-Pesa and GCash: Can 'Lean Regulation' Be a Gamechanger for Financial Innovation?" *Forbes* (3 October 2013).

159 T S, "Why does Kenya Lead the World in Mobile Money?" *The Economist* (27 May 2013).

160 PayPal, "Payments Regulation for Asia Pacific: A Model for Innovation & Growth" (October 2013).

161 HM Treasury, "Digital Currencies: Response to the Call for Information" (March 2015).

consumer protection risks without imposing a disproportionate regulatory burden on the industry.[162] However, virtual currency users and businesses with libertarian ideologies may be unwilling to support any form of government regulation, and attempts to collaborate or negotiate with such industry players may be unduly difficult.[163]

54 Given the rise of cross-border and Internet-based transactions, there is a growing need for international cooperation in regulation. A consistent international regulatory framework for the payments industry would greatly reduce the cost and complexity of compliance for industry players. Countries could consider developing such a regulatory framework based on existing cross-border regulations, including European Union legislation and international AML/CFT measures.[164] Close international co-operation will also be crucial for the enforcement of such regulations, and for addressing cross-border criminal activities in general.[165]

CONCLUSION

55 Regulating the dynamic and ever-changing payments industry is far from an easy task. Payments regulators face the compelling need to develop sophisticated measures that balance a wide range of policy goals, including crime control, consumer protection and monetary stability, while stimulating innovation and competition in the payments industry. International harmonisation of payments regulations has also become a key concern due to the popularity of cross-border and Internet-based transactions. Given the complexity of the challenges and considerations faced by payments regulators,

162 HM Treasury, "Digital Currencies: Response to the Call for Information" (March 2015).

163 D Roberts, "Yes, Regulation is Coming to Bitcoin" *Fortune* (24 March 2015).

164 HM Treasury, "Digital Currencies: Response to the Call for Information" (March 2015).

165 S Knight, "Japan Says Any Bitcoin Regulation Should Be International" *Reuters* (27 February 2014); European Central Bank, "Virtual Currency Schemes – A Further Analysis" (February 2015).

industry collaboration may play a critical role in the development of innovative and effective regulatory regimes.

Mobile Payment Systems: A Maze of Legal Issues and Laws

Although mobile payment systems may be considered a subset of electronic payments systems, the fact that the interface is through a mobile device may attract wholly unique legal problems and challenges. Crucially, they arise from the collapse of the boundaries between the financial and telecommunications sectors. Rules which commonly apply to electronic payment systems may not carry over well to mobile payment systems, not least without substantial adjustments. The consequences of mobile payment systems also reach diverse areas of the law, from personal data protection to patent, adding a further layer of complexity.

LIM Siew Mei Regina*
LLB, BAcc (Singapore Management University).

INTRODUCTION

1 The first mobile payment system in the world rolled out in the Philippines. The year was 2000. A wireless service provider, Smart Communications, Inc, had partnered with MasterCard to produce a never-before-seen electronic cash card that was linked to a mobile phone. The system called "SMART Money", provided users with the unique convenience of holding a store of value in a SMART Money card that could then be used to pay for various goods and services or transferred to another SMART Money card via Short Message Service ("SMS").[1] Today, there are more than 150 other mobile

---

* Some of the ideas in this article springboard from discussions of the panel on "Practical Legal Challenges with Electronic and Mobile Payment Solutions" chaired by Rajesh Sreenivasan with members: Ashish Kulpati, Roy Teo, Greg Unsworth and Michael Tan.

1 S Smith, "What Works: Smart Communications – Expanding Networks, Expanding Profits" *World Resources Institute* (September 2014) at p 1.

payment systems.[2] At the end of 2013, they drew about 245 million users. By 2017, the numbers are predicted to almost double.[3]

2 With the marketplace of mobile payment expanding and being contested by an increasingly diverse group, which range from the obvious (for example, American Express) to the somewhat unexpected (for example, Jawbone),[4] it has become an area primed, first, for regulation and, secondly, for litigation.

REVISITING THE FAMILIAR LANDSCAPE OF ELECTRONIC PAYMENT SYSTEMS

3 The fact that a mobile payment system is, first and foremost, about *payments* through *electronic means* signals that legal issues are aplenty. It is relevant here to make a brief foray into the analysis of some of the issues peculiar to payments that are effected electronically, for they also arise in the narrower field of mobile payment. The focus is invariably on blame: who bears the liability in the event of an unfortunate happenstance.

4 For fraudulent misuse of a payment device, the answer could depend on whether the payment device was obtained with the device holder's consent as well as the terms of use of the payment device. The case of *Bank of Montreal v Demakos* demonstrates that a credit cardholder could be held liable for the fraud perpetuated on the bank by a subsidiary cardholder under the same account with the bank.[5] The fraud involved the subsidiary cardholder depositing forged cheques to the bank, which put the account into an apparent credit position and which therefore enabled the subsidiary cardholder to incur debts beyond the credit limit. Given that the credit cardholder authorised the issuance of subsidiary card and the card agreement stipulated for his joint and several

2 Ernst & Young, *Mobile Banking: Financial Services Meet the Electronic Wallet* (Knowledge@Wharton, 2013) at ch 1.

3 E Thompson, "Omlis Global Mobile Payment Snapshot 2014" *Omlis* (5 August 2014).

4 Jawbone has partnered with American Express to add mobile payment capabilities to its upcoming fitness tracker: B Geier, "AmEx is bringing mobile payments to fitness trackers" *Fortune* (15 April 2015).

5 (1996) 31 OR (3d) 757.

liability for any indebtedness incurred through use of the subsidiary card, he was held to be liable.

5 Independent of this case, a similar position is reached under UK legislation. Section 84(2) of the UK Consumer Credit Act 1974 essentially provides that a device holder has unlimited liability with respect to the misuse of the device by "a person who acquired possession of it with [his] consent".[6] The wording of the provision is thought to be wide enough to cover even the situation where custody of the payment device was consented to be held by a person for the limited purposes of safekeeping.[7]

6 But where the payment device was not obtained with consent (for example, it was stolen, lost, or copied), the device holder may nevertheless have to bear liability. The usual circumstance for pinning liability without limit on the device holder is, in the language of the recommendations issued by the European Commission, "extreme negligence".[8] An example of this may be the recording of a personal identification number ("PIN") in an easily recognisable form, such as to enable the fraudster to make use of

6 c 39.

7 C Wild, "Payment Cards and the Internet" in *Electronic and Mobile Commerce Law: An Analysis of Trade, Finance, Media and Cybercrime in the Digital Age* (University of Hertfordshire Press, 2011) at ch 9, p 240.

8 See Annex 8.3 of Directive 88/590/EEC: Commission Recommendation concerning payment systems, and in particular the relationship between cardholder and card issuer (17 November 1988), which provides: "The contracting holder shall bear the loss sustained, up to the time of notification, in consequence of the loss, theft or copying of the payment device, but only up to the equivalent of 150 ecus for each event, except where he acted with extreme negligence or fraudulently." See also Art 6.1 of Directive 97/489/EC: Commission Recommendation concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder (30 July 1997), which maintains that standard: "Up to the time of notification, the holder bears the loss sustained in consequence of the loss or theft of the electronic payment instrument up to a limit, which may not exceed ECU 150, except where he/she acted with extreme negligence, in contravention of relevant provisions under Article 5(a), (b) or (c), or fraudulently, in which case such a limit does not apply." Understandably, the entity which maintains the electronic payment system will not be keen to accept the losses flowing from device holder's extreme negligence, even if it would otherwise cap the device holder's liability for unauthorised use.

the payment device.[9] This roughly parallels the concept of "gross negligence" in the old cases of bailment, which is what a bailor would have to prove in order to claim for compensation from a gratuitous bailee. Gross negligence in those cases entails the bailee taking less care of the bailor's goods than he did of his own property.[10]

7 On the other hand, if an unauthorised debit was made from the device holder's account while he retains the payment device, the outcome of the litigation between the device issuer and the device holder could hinge upon the evidence available, particularly, the evidence relating to the purported reliability of the computer system. This is perfectly illustrated by the contrasting cases of *Job v Halifax Plc*[11] ("*Job*") and *Judd v Citibank*[12] ("*Judd*"). In both cases, the consumer contested certain automated teller machine ("ATM") withdrawals. Their payment devices were not lost or stolen. An important difference between them is that in *Job*, there was no history of successful fraudulent attacks on online chip and PIN transactions and no evidence of systems failure, whereas in *Judd*, the bank's own witness testified to the physical malfunctions of the computer system.[13] Unsurprisingly, the consumer in *Job* lost his case, while the consumer in *Judd* succeeded. It is understandable why such evidence could be significant. The courts were essentially choosing between the consumer's testimony (that he had not authorised a transaction) and the bank's computer records (showing that a transaction was initiated by means of the

9 S M Rahman & M S Raisinghani, *Electronic Commerce: Opportunity and Challenges* (Idea Group Publishing, 2000) at p 396.

10 C Reed, "Consumer Electronic Banking" in *Cross-Border Electronic Banking: Challenges and Opportunities* (J J Norton, C Reed & I Walden eds) (Lloyd's of London Press Ltd, 1995) at ch 4, p 92.

11 29 May 2009 (unreported).

12 435 NYS 2d 210 (Civ Ct 1980).

13 It should be noted that other circumstantial evidence in *Job* also suggest that the transactions were made by the consumer, by someone authorised by him, or by gross negligence in that he had enabled someone else to use the card and have knowledge of the PIN: (a) the transactions were all cash withdrawals from ATM machines; (b) the withdrawals were all recorded as having been made at ATM machines near his home; (c) the withdrawals stopped without the card being captured or rejected before police report was made; and (d) the sums withdrawn were relatively small.

consumer's payment device and so was possibly authorised by him). Any evidence weakening or strengthening the consumer's testimony and the bank's computer records were highly relevant. If there was evidence showing system malfunction, the bank's general claims about the infallibility of its system could not be sustained. Correspondingly, it would suggest that the consumer's testimony was to be preferred. A review of the case law in the US in the 1980s in fact indicate a trend of consumers consistently overcoming computer records where there is evidence of system malfunction or other evidence corroborating their testimony.[14]

8 In another situation where there is a failure in one of the legs of what appears to be a simple purchase of goods, the question turns to whether payment by use of the device absolutely or conditionally discharges all of the device holder's obligations. There would be a number of contracts formed between the various parties for the proper functioning of an electronic payment system. In the context of a credit card payment, there would have been three separate bilateral contracts each time a payment is made: a contract of supply between the merchant and the cardholder; a contract between the merchant and the card issuer, which undertakes to pay the merchant; and a contract between the card issuer and the cardholder to reimburse the card issuer for liabilities incurred as a result of the use of the card. As succinctly observed by Millett J in *Re Charge Card Services Ltd*[15] ("*Charge Card*"), they are each a party to two of the three contracts but neither party nor privy to the third. If there is a breach in one of these contracts because of non-payment, it would be advantageous to the creditor that a non-party is bound impliedly to make good the debt in the debtor's stead. Of course, the features of the payment system would be critical to the analysis. So in *Charge Card*, a case concerning the claim of the merchant for payment from the cardholder when the card issuer became insolvent, Millett J took into account the fact that the machinery of the payment did not

14 B Geva, "Unauthorized Electronic Funds Transfers – Comparative Aspects" in *New Developments in International Commercial and Consumer Law* (J S Ziegel ed) (Hart Publishing, 1998) at ch 5, pp 124–125.

15 *Re Charge Card Services Ltd* [1987] Ch 150 at 158.

facilitate disclosure to the merchant of the details of the cardholder such that the merchant might later trace him without the cooperation of the card issuer. He also took into account a difference in the terms on which the supplier was entitled to payment from the card issuer and those on which the card issuer was entitled to payment from the cardholder, that is, the card issuer had to pay very shortly after the sale but might deduct its commission, while the cardholder had to pay the full value but was entitled to much longer credit. Those features in fact supported a *presumption* that payment by use of credit card by the cardholder absolutely discharged the cardholder's obligation to the merchant.[16] Taken together, Millett J held that the loss lay where it fell, that is, on the merchant. On appeal, the decision was upheld for "broadly for the same reasons".[17]

9 The experience with other electronic payment systems highlight the kind of issues that would permeate the use of mobile payment systems because many (though not all) mobile payment systems build upon existing credit card and debit card networks. A user of Apple Pay, for example, could pay using a credit card, which he has added to his Passbook app.[18] If he should challenge an Apple Pay transaction for being unauthorised, the same issues of whether he has consented to the use of his mobile phone by a third party, whether he was extremely or grossly negligent with the security of his mobile phone or the authorisation data, or whether there was a system failure or fraud would likely arise. If instead an intermediary should become insolvent, factual issues about the arrangement for delivering goods and services, on the one hand, and processing payments, on the other, would likely be raised in order to shed light on the legal issue of how the risk of that insolvency was intended to be borne. In short, the legal landscape of electronic payment systems, with its fair share of challenges, would resemble to some degree that of mobile payment systems.

16 *Re Charge Card Services Ltd* [1987] Ch 150 at 168–169.

17 *Re Charge Card Services Ltd* [1989] Ch 497 at 517.

18 See "Overview" <http://www.apple.com/apple-pay/> (accessed 6 November 2015).

CHARTING THE NEW TERRITORIES OF MOBILE PAYMENT SYSTEMS

10 It is worth emphasising that differences do exist between mobile payment systems and other electronic payment systems. These differences create new twists and turns in one's navigation through the legal landscape of mobile payment systems, which will doubtlessly deviate from the well-trodden path carved through the legal landscape of electronic payment systems. They add to the legal complexities that one would encounter with mobile payment systems.

11 For one, the interposition of a mobile network operator between a payer and the payee means that there could be errors in the course of processing payment instructions solely attributable to the mobile network operator. This is an issue unique to mobile payment systems. Its resolution too depends on the unique circumstances of mobile payment systems. It has been suggested, in the context of a South Korean legislation,[19] that although the mobile network operator ought to be liable for the damage caused by the errors, it may be desirable to make the financial institution compensate the customer first and seek indemnification from the mobile network operate later because it is almost impossible for the customers to clarify whether the errors were caused by financial institution or mobile network operator.[20]

12 Secondly, the capability of the mobile phone to authenticate a transaction means that if there is a vulnerability in the mobile payment system which has been exploited, the fault could be as much the app developer's, the handset manufacturer's, the bank's or the merchant's, so it could be difficult to discern how the

19 Article 12(1) of the Electronic Financial Transaction Act (Act No 7929 of 2006) (South Korea): "Any financial institution or electronic financial business operator shall ensure the payment is made by transmitting the amount requested by a payer or payee on a transaction request to the payee or his/her financial institution or electronic financial business operator, pursuant to an agreement made with the payer or payee to facilitate electronic payment transactions."

20 Chung CH, "Legal Issues Arising from the Use of Mobile Devices in Electronic Commerce" delivered at UNCITRAL Colloquium on Electronic Commerce (14–16 February 2011), New York.

liability should be shifted or shared accordingly. Take, for example, the wave of fraudulent transactions which hit Apple Pay in the first quarter of 2015. While the costs of fraud were ultimately borne by the banks on the basis that it was responsible for verifying cardholder identity and had failed to do so,[21] there is commentary to the effect that Apple Inc is not entirely blame-free; it could have increased security in the verification process, which it had not done in favour of making the app more convenient to users.[22] This presents a further dimension to the blame game.

13 Thirdly, the increased number of participants in mobile payment systems could exacerbate the contractual issues about the enforceability of the more draconian, anti-consumer and non-negotiated terms of service. A common term in a contract between a card issuer and a cardholder provides that the card issuer is not liable for a failure to carry out a transaction as a result of mechanical failures or transmission problems. Assuming that the card issuer is the *sole* entity in charge of processing a transaction and it has failed to do so because of a technical problem, such an exclusion clause is arguably unreasonable and therefore unenforceable, if the technical problem arose because of the card issuer's own negligence.[23] The unreasonableness of the exclusion clause stems, in part, from the attempt to exclude liability for negligence and, in part, on the fact that the cardholder does not possess the knowledge to challenge the claim by the card issuer that it suffered from technical problems as it claimed (unless the cardholder commences discovery proceedings). Turning to the context of a mobile payment system involving numerous participants, it is imagined that the chances of succeeding with this argument must be higher, given that it is even more difficult to find out which of the participants collectively operating the mobile payment systems was at fault for failing to carry out the transaction and therefore whether a particular participant has incorrectly invoked the exclusion clause. Given also that "contract law is the

21 R Sidel & D Wakabayashi, "Apple Pay Stung by Low-Tech Fraudsters" *The Wall Street Journal* (5 March 2015).

22 C Thompson, "Who's at Fault in Apple Pay Fraud, Apple or Banks?" *CNBC* (4 March 2015).

23 J O'Donovan, *Lender Liability* (Sweet & Maxwell, 2005) at ch 4, pp 199–200.

dominant form of organizing these digital spaces",[24] these contractual issues may arise rather frequently.

14 But the biggest differences emerge in respect of mobile payment systems which link to a prepaid phone deposit or a phone bill (as opposed to a credit card, a debit card, a prepaid card, or a bank account).[25] Mobile payment systems in this category involve a convergence between the traditionally distinct telecommunications and financial sectors. For this reason, they throw up issues which are quite unlike any in the realm of payment systems relying on traditional intrabank or interbank payment networks.[26]

15 Perhaps the most famous example of such mobile payment systems is M-PESA. It is an SMS-based money transfer system launched in Kenya in 2007 by Safaricom. It is operable from a mobile phone: individuals may deposit, send and withdraw funds using their mobile phones, so long as they have an M-PESA account. Registration for an M-PESA account can be done with any authorised M-PESA agents, which range from banks to small mobile phone retailers.[27] The one feature which distinguishes it from its bank-based counterparts is its issuance of electronic value for cash.[28]

16 This ensnares a mobile payment system like M-PESA in legal uncertainty because it blurs the lines between financial services and telecommunications services. In the years since the launch of M-PESA, the Central Bank of Kenya has had to, among other things, set out a *Guideline on Agent Banking*[29] and propose

24 Ernst & Young, *Mobile Banking: Financial Services Meet the Electronic Wallet* (Knowledge@Wharton, 2013) at ch 5.

25 See the Statement of Suzanne Martindale, Staff Attorney, Consumers Union of US, Inc in *The Future of Money: How Mobile Payments Could Change Financial Services* (22 March 2012) at p 12.

26 See T Khiaonarong, "Oversight Issues in Mobile Payments" *IMF Working Paper* (July 2014) at p 8.

27 "What is M-Pesa?" <http://www.vodafone.com/content/index/what/m-pesa.html> (accessed 19 February 2016).

28 M W Buku & M W Meredith, "Safaricom and M-PESA in Kenya: Financial Inclusion and Financial Integrity" (2013) 8 *Washington Journal of Law, Technology & Arts* 375 at 378–379.

29 CBK/PG/15 of 2010.

regulations on e-money and electronic retail transfers.[30] Still, these regulatory efforts would not have drawn complete boundary lines on what is to be regulated or address the risk of coordination failure between the financial sector regulator and the telecommunications sector regulator. In time, as mobile payment systems evolve and as tie-ups form between mobile network operators and banks to develop more sophisticated mobile banking products, the confusion may increase. What used to fit within the definition of "banking business" in the Kenyan Banking Act[31] may fall outside its scope and vice versa.

17 Precisely because a non-bank entity (for example, the mobile network operator) is involved in taking deposits from customers and issuing electronic money in return, fund safeguarding measures may also be triggered. The Kenyan draft regulations mentioned above, for example, make it a requirement of authorisation for an e-money issuer to maintain an unencumbered core capital of at least KSh60m (about US$580,000);[32] and for a payment service provider, which is not a licensed bank, a licensed financial institution or an authorised e-money issuer, to otherwise maintain a core capital of at least KSh10m (about US$98,000).[33] Elsewhere, in Indonesia, non-bank issuers are required to place 100% float in a commercial bank and only allowed to use the float

30 J K Nyaga, "Mobile Banking Services in the East African Community (EAC): Challenges to the Existing Legislative and Regulatory Frameworks" (2014) 4 *Journal of Information Policy* 270 at 280–281; see also "Draft NPS Regulations and Guidelines – Invitation for Comments" <https://centralbank.go.ke/index.php/news/286-draft-nps-regulations-and-guidelines-invitation-for-comments> (accessed 6 November 2015).

31 Cap 488, 2014 Rev Ed.

32 Clause 5.2 of the draft E-Money Regulation provides that: "The Bank shall not authorize a person as an e-money issuer unless the person complies with the following requirements: … (d) The person has minimum unencumbered core capital of Sixty Million Shillings or such other amount as may be required by the Bank".

33 Clause 6.1 of the draft Regulation for the Provision of Electronic Retail Transfers provides that: "A payment service provider, other than a bank or financial institution licensed under the Banking Act or a Deposit Taking Microfinance business licensed under the Microfinance Act and an authorized e-money issuer, shall, at the time of authorization, hold a core capital of not less than Ten Million Shillings."

funds to fulfil the issuer's obligations to customers and agents.[34] These measures are likely alien to the non-bank entities. But they are necessary in order to ensure that electronic value issued by these non-bank entities can be redeemed at all times, and that the customer funds held by these non-bank entities are traceable, insulated from the claims of other creditors in the event of insolvency, and not commingled with operating or third party's funds.

18 And it is not just fund safeguarding measures, commonplace in the financial sector, which should be extended to the telecommunications sector, where appropriate. In theory, all banking laws and regulations should be applied to a non-bank entity if it passes the litmus test of being materially similar to a bank. This would include entities which activities mimic banking functions, which products are functional equivalents of banking accounts, or which process financial and transactional data once only held by banks and transaction processors. If they are not subject to the same statutory restrictions, conceivably, they would introduce vulnerability into the financial system.[35] This is especially so if subscription to the mobile payment system in question is considerable and the value placed with the non-bank entity is significant.

19 The devil is in the details. If the approach is simply to transplant existing legal solutions to the mobile payment space, that may itself create further issues. Because non-bank entities, as the label suggests, have hitherto very disparate businesses from the

34 Paragraph VII.H of Circular Letter No 11/11/DASP provides as follows:

1. In case the Issuer is an Institution Other Than Bank, managed Float Funds must be placed with a Commercial Bank in the form of a deposit account consisting of savings account, current account, and/or time deposit account.
2. Float Funds placed at a Commercial Bank ... total 100% from Float Funds derived from sales proceeds of Electronic Money that still represent the Issuer's liability towards Holders and Traders.
3. ... Issuer can only utilize Float Funds in the interest of liability fulfillment for Holders and Traders.

35 C Merritt, "Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person" (2011) 5(2) *Journal of Payments Strategy & Systems* 143 at 157.

banks, it is possible that they lack the capacity or will not practice the same level of care to comply with the usual banking laws and regulations. A study observed, for instance, that the mobile network operators tended to be less vigilant about enforcing Know Your Customer ("KYC") procedures. The business model of the mobile network operators, it was stated, did not provide them with the sufficient incentive to enforce KYC procedures for the prepaid customers because there was no exposure risk from these customers.[36]

20 The initial approach that India took was to rule out altogether mobile payment systems which disintermediates banks. In 2008, the Reserve Bank of India decided that "[o]nly banks which are licensed and supervised in India and have a physical presence in India will be permitted to offer mobile banking services".[37] The rationale was straightforward: mobile transactions carried out through the conventional banking systems are assuredly within the control of the regulators, whereas the same may not be said of non-bank entities.[38] However, this restriction has since been relaxed in order to broaden financial inclusion.[39] In November 2014, the Reserve Bank of India issued Guidelines for Licensing of Payments Banks which will allow "entities to carry on the business of banking and other businesses in which banking companies may engage".[40] Amongst the entities which have already been granted licences are major mobile operators such as Vodafone and Airtel.[41]

---

36 S P Ketkar, R Shankar & D K Banwet, "Telecom KYC and Mobile Banking Regulation: An Exploratory Study" (2014) 15(2) *Journal of Banking Regulation* 117.

37 Paragraph 2.1 of Mobile Banking Transactions in India – Operative Guidelines for Banks Issued by the Reserve Bank of India under s 18 of the Payment and Settlement Systems Act (Act 51 of 2007).

38 Ernst & Young, *Mobile Banking: Financial Services Meet the Electronic Wallet* (Knowledge@Wharton, 2013) at ch 2.

39 I Allison, "Why some Banks and Governments still Stifling the Mobile Money Inclusion Miracle" *International Business Times* (14 September 2015).

40 "Guidelines for Licensing of Payments Banks" <https://rbi.org.in/scripts/bs_viewcontent.aspx?Id=2900> (accessed 19 February 2016).

41 "RBI grants "In-principle" Approval to 11 Applicants for Payments Banks" (19 August 2015) <https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=34754> (accessed 19 February 2016).

21 It leaves for India therefore to implement an effective legal framework, which would have to overcome the aforementioned issues pertaining to not only mobile payment systems in general but also the non-bank-based type of mobile payment systems.

A HODGEPODGE OF RULES

22 As alluded, the laws and regulatory controls applicable to mobile payment systems are diverse. The diversity is a reflection of the enormous reach they possess, the intricate tie-ups that underlie their operation, and their intrusiveness into the private lives of the users. It is a formidable task to govern each aspect of mobile payment systems: personal data protection, competition, anti-money laundering, patent, *etc*. So far, therefore, there is no comprehensive regulatory regime for mobile payment systems. It does not seem possible to conceive of one anyway. That requires a very thorough insight into the ever-developing technology that forms any mobile payment system and the attendant effects. Governments have had to content themselves with collecting information as best as they can and empowering their central banks to have greater control over designated payment systems in order to plug the gaps in regulation.[42] Australia and Singapore are cases in point. The Payment Systems (Regulation) Act 1998[43] in Australia and the Payment Systems (Oversight) Act[44] in Singapore,[45] entrust the Reserve Bank of Australia and the Monetary Authority of Singapore, respectively, with broad powers to gather information about any payment system as well as designate any payment system to be subject to stricter regulations. As recognised in the Singapore Parliament, the information gathering powers are necessary "to monitor trends and developments in the payment industry, and fine-tune [the central

42 See S E Weiner, "The Federal Reserve's Role in Retail Payments: Adapting to a New Environment" (2008) 93(4) *Economic Review* 35 at 47–50.

43 Act No 58 of 1998.

44 Cap 222A, 2007 Rev Ed.

45 In fact, the Singapore legislation is, to a large degree, based on the Australian legislation.

bank's] oversight policy for payment systems over time".[46] The idea is that, by keeping abreast of changes, the central bank can at least adapt to, if it cannot pre-empt, the demands of new technology.

23 To paint a general picture of the mobile payment space in legal and regulatory terms, it would be a web of laws and regulations interlinked, intertwined and intersecting in the same space. And this is not a static web: outdated strands of law and regulation are and will continue to be adjusted, while new strands of law and regulation are and will also continue to be added.

24 Personal data protection, for example, is one such strand. Indeed, it is a prominent strand because data collection is rife in mobile payment systems. It could be lucrative for the providers of mobile payment services because they could sell the data which they collect from the users to merchants who would want to understand customers' preferences, to target the right customers or to make individually tailored offers to them.[47] It could also be a way mobile payment service providers give free access to their mobile payment services, if the income from the sale of data could sustain the business. Alternatively, it could be necessary or useful for improving the mobile payment services. Whatever the reasons for collecting and sharing personal data, though, there has been a push back from the users. So there is a palpable tension between the users and the service providers and their competing rights to information and privacy. Whether and to what extent must mobile payment service providers respect the users' privacy surely is an issue which will arise in many situations. No doubt lawsuits commenced by the users, such as *Svenson v Google Inc*[48] ("*Svenson*"), will test the limits of the parties' positions. In

46 *Singapore Parliamentary Debates, Official Report* (16 January 2006), vol 80 at col 2090 (Tharman Shanmugaratnam, Minister for Education).

47 Ernst & Young, "Mobile Money: An Overview For Global Telecommunications Operators" at p 12, cites "[i]ncreased amount of customer data for marketing" as a compelling reason for merchants to invest in mobile money. The same report at p 32 also states that the telecom operators are comparatively in a stronger position to mine data. Presumably, it is usually the mobile network operators which will be in a position to capture customer data and sell it on to the merchants.

48 Case No 5:13-cv-04080.

Svenson,[49] the complaint is that Google Inc had impermissibly shared the personal information of users of Google Wallet with third-party app developers. Five claims were brought by the users; two were dismissed *in limine* under rule 12(b)(6) of the Federal Rule of Civil Procedure for failure to state a claim, but three remain and they assert (a) a breach of users' contracts (that is, the written privacy policies governing Google Wallet), (b) a breach of the implied covenant of good faith and fair dealing; and (c) a violation of California Business & Professions Code § 17200, a consumer protection law. Although the substantive decision has not yet been rendered, the lawsuit already has some practical effect in that it has prompted Google Inc to cease its practice of sharing information.[50]

25 Competition is another strand in the web.[51] A few mobile payment systems tend to dominate the market. In Japan, Edy and Mobile Suica are "[p]articularly widely diffused".[52] In Bangladash, bKash alone takes up 50% of the market share.[53] It does not help that alliances, joint ventures and other forms of partnerships are frequently formed amongst big industry players for the provision of mobile payment services. Retailers in the US, for example, have teamed up to adopt CurrentC, to avoid paying credit card processing fees. In a show of unity, retailers apparently bound themselves to a three-year mobile payment app exclusivity deal. This was speculated to be the reason why certain retailers pulled unofficial support for Apple Pay.[54] Separately, in the UK, Everything Everywhere, O2 and Vodafone entered into a joint venture, code-named Project Oscar, to develop a mobile payment system. Their

49 This is a class action brought by Alice Svenson, the lead plaintiff, in the United States District Court for the Northern District of California.

50 J Stempel, "Google Fails to Dismiss Privacy Lawsuit Over Google Wallet" *Reuters* (2 April 2015).

51 G Ivatury & I Mas, "The Early Experience with Branchless Banking" Consultative Group to Assist the Poor (1 April 2008).

52 M Kakihara, "Japan: The Leading Mobile Market at the Crossroad" in *Trends in Mobile Technology and Business in the Asia-Pacific Region* (Y Yoo, J-N Lee & C Rowley eds) (Elsevier, 2008) at p 103.

53 "Most Mobile Payment Agents Profitable: Study" *The Daily Star* (11 November 2014).

54 J Constine, "CurrentC is the Big Retailers' Clunky Attempt to Kill Apple Pay and Credit Card Fees" *TechCrunch* (25 October 2014).

rival, Three, was quick to accuse the joint venture of being anti-competitive and it filed a challenge with the European Commission, pointing out that the three shareholders hold 90% of the UK mobile network operator market.[55] But the European Commission gave the green light to the joint venture, opining that it "will not likely have the technical or commercial ability, nor the incentive, to substantially foreclose entry, or hinder expansion by competitors in relation to wholesale or retail mobile wallet platform services, advertising services or data analytics".[56] This elegantly summarises the core of competition concerns: the raising of barriers to entry in a way which stifles innovation. In the mobile payment space, some of the factors which would smack of anti-competitive practice are: (a) controlling technical standards and hence obstructing interoperability between various mobile payment systems; (b) levying predatory fees; (c) leveraging one's strong market position in a related market by tying products; (d) denying the use of another's payment cards in one's mobile payment system; (e) forbidding the use of one's payment cards in another's mobile payment system; and (f) curbing the freedom of partners from participating in other mobile payment systems.[57]

26 A third important strand in the web is anti-money laundering. As with any other electronic payment system, mobile payment systems are susceptible to the risks of money laundering, especially if there are insufficient safeguards to verify the identity of the payee and recipient. Customer due diligence and KYC procedures have therefore served as the cornerstone of anti-money laundering measures. However, they vary from jurisdiction to jurisdiction, in reflection of the particular circumstances and risks in the jurisdiction. South Africa, for example, dispenses with certain

55 "Rivals' Mobile Wallet is Anti-competitive, says Mobile Network Three" *Out-Law.com* (9 September 2011) <http://www.out-law.com/en/articles/2011/september/rivals-mobile-wallet-is-anti-competitive-says-mobile-network-three/> (accessed 6 November 2015).

56 Case No COMP/M.6314 – Telefónica UK/Vodafone UK/Everything Everywhere/JV (4 September 2012) at p 131, para 594.

57 M Mohan, "Mobile Payments Systems: Potential Competition Concerns" *Mondaq* (10 April 2014) <http://www.mondaq.com/x/306028/Antitrust+Competition/Mobile+Payments+Systems+Potential+Competition+Concerns> (accessed 6 November 2015).

identification and verification requirements pertaining to a customer if the bank account which is sought to be opened is restricted one: the balance is capped at R25,000; the right to transfer, withdraw and pay funds out of the account is limited to R5,000 per day and R25,000 per month; an international transfer of funds may not be effected, except as a result of a point-of-sale payment or as withdrawal in a country in the Rand Common Monetary Area, *etc*.[58] This acknowledges the very real situation in South Africa that at least one-third of the households lack official documents or other information that can be used to verify their informal residential addresses.[59] So to reduce the regulatory burden, yet adequately address money laundering risks, the solution is to place restrictions on the type and value of the transactions that can be performed with the bank account. By contrast, in Hong Kong, the situation is clearly different and so are its regulations: records are required to be maintained on all wire transfers equal to or exceeding HK$8,000.[60] As a matter of practice, a more stringent approach is in fact taken because transactions below this figure in mobile payment systems are also recorded.[61]

27 A last example of a strand in the mobile payment web is patent. Mobile payment systems are no stranger to wars on patent infringement and invalidation. After all, these issues could determine the fate of a mobile payment system. Its existence could depend on whether it can fend off an injunction, and its profitability, on whether it would be burdened with the payment of licensing fees to a third party. Major lawsuits, like the ones brought by Maxim Integrated Products, Inc against Starbucks Corporation,

58 Exemption 17 of the Financial Intelligence Centre Act (Act 38 of 2001).

59 L D Koker, "Money Laundering Control and Suppression of Financing of Terrorism" (2006) 13(1) *Journal of Financial Crime* 26 at 42.

60 See Guideline on Anti-Money Laundering and Counter-Terrorist Financing (Revised March 2015) issued by the Hong Kong Monetary Authority under s 7 of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap 615).

61 "Mobile Financial Services Risk Matrix", Kenya School of Monetary Studies and United States Agency for International Development (23 July 2010) at p 143.

Expedia, Inc, Capital One Financial Corp and Bank of the West[62] for infringement of four of its patents relating to secure data transfers for payment processing, would possibly even have an effect beyond the defendants' mobile payment systems, given that the patents at the heart of the lawsuits are "written too broadly" and could be easily turned on other mobile payment systems once a legal victory or settlement is secured with these initial defendants.[63] It is noteworthy that the majority of patent filing activity in recent years has occurred in technologies relating to payment architecture and access security,[64] so these are likely to be the areas where mobile payment service providers will clash.

CONCLUSION

28 Suffice to say, these are interesting times in the mobile payment space. It is rife with issues that await to be unravelled. They arise from divergent fields of law and regulation, some dating from the advent of electronic payment systems, while others are newly generated by the design of mobile payment systems. To this mix of issues, further issues on conflicts of law will be added. Mobile payment systems are global in their operation, but laws are local in their enactment. So until there is a harmonised standard or a supra-national framework that is applied to all the jurisdictions

62 The cases are *Maxim Integrated Products, Inc v Starbucks Corporation* Case No 4:12-cv-00005; *Maxim Integrated Products, Inc v Capital One Financial Corporation* Case No 4:12-cv-00006; *Maxim Integrated Products, Inc v Expedia, Inc* Case No 4:12-cv-00007; and *Maxim Integrated Products, Inc v Bank of the West* Case No 4:12-cv-00010. All are brought in United States District Court for the Eastern District of Texas: D Wilson, "Bank of the West, Others Face IP Suits over Mobile Apps" *Law360* (9 January 2012) <http://www.law360.com/articles/298213/bank-of-the-west-others-face-ip-suits-over-mobile-apps> (accessed 6 November 2015).

63 C Tode, "Starbucks, Expedia, Capital One Sued over Mobile Payments Patent Infringement" *Mobile Commerce Daily* (12 January 2012) <http://www.mobilecommercedaily.com/starbucks-expedia-capital-one-sued-over-mobile-payments-patent-infringement> (accessed 6 November 2015).

64 LexInnova Technologies LLC, "War of the Wallets: Patent Landscape Analysis" (2015) <http://www.wipo.int/export/sites/www/patentscope/en/programs/patent_landscapes/documents/war_of_wallets.pdf> (accessed 6 November 2015).

which a mobile payment system operates in, there are bound to be disputes about which law is effective and enforceable.

29 In the future, as mobile payment systems develop, probably so in leaps and bounds as is the case presently, the law will have to catch up. This poses yet more challenges in the law-making department because one would need not just a penetrating foresight of what is to come, but also a healthy dose of caution and care to avoid over-regulation which suppresses innovation. As one writer puts it:[65]

> To this day, we see all around us the Promethean drive to *omnipotence through technology* and to *omniscience through science*. The effecting of all things possible and the knowledge of all causes are the respective primary imperatives of technology and of science. But the motivating imperative of society continues to be the very different one of its physical and spiritual survival. It is now far less obvious than it was in Francis Bacon's world how to bring the three imperatives into harmony, and how to bring all three together to bear on problems where they superpose. [emphasis in original]

---

65 G Holton, *The Advancement of Science, and Its Burdens: The Jefferson Lecture and Other Essays* (Cambridge University Press, 1986) at ch 9, p 183.

Virtual Currencies: The Future of Money or Just Another Passing Fad?

As with any novel technology, virtual currency possesses the potential to spur utility gains for society and to drive further innovation. However, the disruptive nature of virtual currencies such as Bitcoin – countenancing as they do decentralised and self-regulating currency systems that fall outside the traditional frameworks of most central banks – is also a source of confusion and, significantly, opportunity for technology-savvy criminals. This article first introduces and examines the phenomenon of Bitcoin, before turning to shine the spotlight on some of the challenges in the way of its use and adoption. It concludes with both a positive and normative consideration of alternative regulatory approaches to virtual currencies.

TAN Sze Yao*
BA Law (Cantab), LLM (Columbia University), LLM (Kyushu University);
Deputy Senior State Counsel, Attorney-General's Chambers.

> The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes … [i]f a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains … we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power.
>
> Satoshi Nakamoto, creator of Bitcoin[1]

* The author expresses his deepest appreciation to Professor Alexander Loke and Yeong Zee Kin for their comments to an earlier draft of this article. Some of the ideas in this article springboard from discussions of the panel on "Virtual Currencies: The Future of Money or Just Another Passing Fad?" chaired by Steven Liew with members: Foo Chek-Tchung, Ko Hanamizu, Professor Alexander Loke and Gene Truono.

1 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (31 October 2008).

INTRODUCTION

1 Virtual currency has been defined to be a digital representation of value that functions as (1) a medium of exchange (to make payments); (2) a unit of account (to measure the value of any particular item for sale); and (3) a store of value (to transfer purchasing power from today to some future date).[2] These traditional functions of currency are fulfilled by virtual currency not through issuance or guarantee by any government, but rather through agreement within the community of users of the virtual currency.[3] Accordingly, virtual currency does not have legal tender status in any jurisdiction, unlike traditional fiat or national currency.[4] Virtual currency can also be distinguished from e-money, which is basically a digital representation of fiat currency used to transfer value denominated in fiat currency.

2 Two distinct varieties of virtual currency may be discerned. *Centralised virtual currencies*, such as Linden dollars in the online game "Second Life", are administered by a single authority. This authority issues the currency and establishes rules for its use, and also has the power to withdraw the currency from circulation. The exchange rate for such centralised virtual currencies may be determined by market supply and demand (floating), or it may be fixed by the authority at a set value measured in fiat currency (pegged).

3 In contrast, *decentralised virtual currencies* such as Bitcoin are not governed by any central administrative authority. They operate instead under a peer-to-peer paradigm on an open-source platform. Without any authority to provide oversight of transactions entered into with decentralised virtual currencies, these transactions are

2 R Ali *et al*, "The Economics of Digital Currencies" (2014) 54(3) *Bank of England Quarterly Bulletin* 276. Whether the "store of value" function is sufficiently fulfilled by virtual currencies such as Bitcoin, however, is subject to some debate: see paras 34–66 below for further discussion.

3 Financial Action Task Force Report, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks" *Financial Action Task Force* (June 2014) at p 5.

4 Fiat currency is currency that derives its value from government regulation or law. It can be contrasted with commodity money, which is created from a good (often a precious metal such as gold or silver) which has uses other than as a medium of exchange.

instead validated by a distributed proof-of-work system. Specifically, each transaction is distributed among a network of participants who devote computer resources to run algorithms validating the transaction.

4 The most common form of decentralised virtual currency is the *cryptocurrency*. Cryptocurrencies utilise principles of cryptography to implement a distributed and decentralised framework for the digital exchange of value. In the case of the world's leading cryptocurrency, Bitcoin, cryptography is employed by a global public ledger known as the "blockchain" to validate transactions. Each time value is transferred via Bitcoin, the transaction must be cryptographically signed and added to the global blockchain through the use of public and private keys. This process requires computing power, which is in turn provided by a network of users called "miners". These miners donate their computer power to help validate transactions in exchange for the (randomised) opportunity to gain or "mine" additional bitcoins.[5]

5 The Bitcoin ecosystem is broadly comprised of three groups of stakeholders. First, there are the Bitcoin miners, who (as just discussed) collectively perform the role of validating transactions that are then recorded on the blockchain. Second, there are Bitcoin exchanges – online marketplaces where bitcoins are bought and sold in exchange for (a) fiat currency or (b) other assets with real-world value. Finally, there are also merchants (such as Overstock.com) who accept bitcoins as payment for goods and services.

6 The remainder of this article focuses on the challenges and benefits that cleave to Bitcoin and other virtual currencies, as well as the various approaches that have been taken or are being contemplated by national regulators in this regard. As with any novel technology, Bitcoin possesses the potential to spur utility gains for society and to drive further innovation. However, the

5 There is, however, a fixed supply of 21 million bitcoins that will be gradually released over time at a publicised rate. Accordingly, the rate of supply diminishes over time in a predictable fashion. It should be noted, however, that individual bitcoins can be divided into smaller fractions.

disruptive nature of Bitcoin – countenancing as it does a decentralised and self-regulating currency system that falls outside the traditional frameworks of most central banks – is also a source of confusion and, significantly, opportunity for technology-savvy criminals.

BENEFITS OF VIRTUAL CURRENCIES

Low-cost, high-speed

7 Bitcoin offers many advantages over traditional forms of fiat currency. The first and most obvious of these is that Bitcoin transactions are fast and cheap. The lack of any need for a central authority under the Bitcoin framework means that transaction costs are reduced through direct peer-to-peer transfers of value. For example, a Bitcoin payment sent by an individual in Sydney to anywhere in the world would be processed within seconds, and verified within an hour.[6]

8 In contrast, traditional payment systems, for example, online payments via credit card and PayPal, require an intermediary to carry out validation procedures. These procedures would necessitate both time and money (in the form of transaction fees), as well as actual accounts on both ends of the transaction.[7]

Security and transparency

9 Bitcoin is also secure,[8] not in spite of its openness but *because* of it: every transaction is validated with cryptography by a network of miners worldwide and publicly recorded on the blockchain, which effectively acts as a globally-accessible timestamp and transaction log denoting the true path of each bitcoin in existence.

---

6 R Bollen, "The Legal Status of Online Currencies: Are Bitcoins the Future?" (2013) 24(4) *Journal of Banking and Finance Law and Practice* 272 at 277.

7 A L Tyree & J Sheehan SC, "Banking Law and Banking Practice: Bitcoin" (2012) 23 *Journal of Banking and Finance Law and Practice* 139 at 140.

8 This is relative to other forms of online payment such as credit cards (the details of which can be bought and sold on the Internet). As will be seen at paras 19–33 below, however, Bitcoin is also susceptible to some technical risks.

10 Due to the architecture of the blockchain, Bitcoin is able to avoid the "double spending" problem that is associated with distributed e-money and other digital cash transactions. Since electronic files can be duplicated and the act of spending a digital unit of value does not remove its data from the ownership of the original holder (unlike physical money), it becomes possible for a person to send a single digital unit of value to two different recipients. Bitcoin averts this problem through its proof-of-work system and the publicly-verifiable blockchain,[9] which acts as a register of transactions.

Self-sustainability

11 Another unique benefit of Bitcoin is that it is self-sustainable. Bitcoin uses its own product – bitcoins – to reward miners who are providing computing resources to power the global Bitcoin validation system. Accordingly, Bitcoin automatically regulates its own money supply rate without the need for any monetary policy, avoiding any overhead costs that might attach to traditional payment systems.[10] Indeed, compared with centralised currency systems that require ever more resources to handle an increasing user base, the Bitcoin ecosystem functions more efficiently as more participate in it.[11]

9 Double-spending is theoretically still possible with Bitcoin. A person could pre-mine one transaction into a block and spend the same bitcoins before releasing the block to invalidate that same transaction. However, this method is highly technical and extremely difficult for the average Bitcoin user to implement.

10 T Wan & M Hoblitzell, *Bitcoin: Fact. Fiction. Future.* (Deloitte University Press, 2014) at p 5.

11 There is, however, a finite supply of bitcoins, and there remains a question mark over how miners (or, by then, "transaction validating computer resource owners") will continue to be incentivised once the 21 million bitcoin threshold is reached. Suggested solutions have ranged from increasing the supply cap to a redistributive "tax" to allocate bitcoins from persons who provide computer resources to those who choose not to (or from those who provide more resources to those who provide less).

Privacy

12 There are various legitimate reasons why individuals might seek privacy in their financial transactions. Some persons might wish to receive controversial health treatments without having to explain themselves to their family, friends or employers. Others might wish to conceal their transactions (and wealth) from the watchful eye of despots running the country. Through its pseudonymous nature,[12] Bitcoin is able to offer some of the privacy that cash traditionally offers, except with the added convenience of digital transfer.[13]

13 However, precisely because its users are pseudonymous, Bitcoin is often the currency of choice for illegal transactions. In October 2013, for example, the US Federal Bureau of Investigation shut down the notorious Silk Road website ("Silk Road"), an online marketplace for drugs, stolen credit card numbers, hacking tools and fake identity documents.[14] Investigations revealed that payments for illegal goods and services on Silk Road had been greatly facilitated by the use of the relatively anonymous Bitcoin. The discussion will be continued below on the risks concomitant with the privacy offered by virtual currencies such as Bitcoin.[15]

Innovation

14 The successful mainstream adoption of Bitcoin will give credibility to the underlying technology of the blockchain, a technology that has myriad uses beyond currency. The blockchain – a global peer-to-peer register that is publicly

12 Users can send and receive bitcoins without providing personally identifying information, allowing them to remain relatively anonymous. However, since every Bitcoin transaction is publicly logged on the blockchain, complete anonymity under the Bitcoin framework is difficult. If any of the addresses in a transaction can be tied to an actual identity, for instance through network analysis or surveillance of third party transactions, it is possible to work from that point to decipher the parties that own all the other addresses.

13 J Brito & A Castillo, *Bitcoin: A Primer for Policymakers* (Mercatus Center, George Mason University, 2013) at p 15.

14 *United States v Ross William Ulbricht* 14 Cr 68 (KBF).

15 See paras 19–29 below.

validated – could potentially be employed to verify the purchases of big-ticket items such as property (checking of existing encumbrances *etc*) and cars (due diligence *vis-à-vis* prior accidents and inspections *etc*). It could also form the basis of new types of contract and financial instruments – for example, an option contract could be written as code and registered with the blockchain, to execute only upon the triggering of an event such as where the strike price is reached.[16] This would permit regulators to reliably monitor, at a very detailed level through the blockchain, activity in the market.

15 The applications of blockchain technology to identity management are also obvious – with the verification of identity keys via a decentralised, peer-to-peer ledger, forgery of identity documents will become a thing of the past. Such a system of identification would increase not just security but also mobility –

16 The community-driven project Ethereum, aims to "decentralize the internet" by providing a "platform for building and running applications which do not need to rely on trust and cannot be controlled by any central authority", is developing a framework that allows the conditions of a contract to be automatically executed – *ie*, smart contracts – through rules that are verifiable by others connected within the community (in a fashion similar to the blockchain for Bitcoin) <http://www.ethereum.org> (accessed 12 July 2015). Similarly, Colored Coins, which are created by attaching metadata to a fraction of a bitcoin in a transaction, are used to represent the real world value of an asset in its digital form. Being digital assets with various capabilities (specific time limitation, access controls, permissions for issuance of more of the same colored coin *etc*), insofar as the user community is prepared to recognise the asset *backing* each colored coin, they can be used to issue shares, prove ownership of property, store records and create smart contracts <http://www.coloredcoins.org> (accessed 12 July 2015). For example, User A could mark some of his bitcoins as colored coins representing 100 Microsoft shares. These colored coins may then be sold to User B for normal bitcoins, with the rights in the underlying 100 Microsoft shares deemed to be transferred together with the transfer of the colored coins. With this process, the need for a third party stock exchange is dispensed with – the 100 Microsoft shares are effectively sold from User A to User B via the exchange of bitcoins. Other examples of such decentralised digital asset registers may be found at http://gendal.me/2013/11/10/decentralised-digital-asset-registers-concepts/ (accessed 12 July 2015).

individuals will no longer have to carry paper identification documents with them on their travels, but only their Bitcoin key.[17]

Accessibility

16 The final and perhaps most important benefit of Bitcoin is its accessibility. Anybody in the world with a working Internet connection can potentially carry out Bitcoin transactions. Ernie Allen, the President and CEO of the International Centre of Missing and Exploited Children, has noted that virtual currencies such as Bitcoin can "achieve social good by bringing financial inclusion for the 2.5 billion adults today without access to banks, credits and the mainstream banking system".[18]

17 The true potential of Bitcoin, therefore, may be unlocked in developing parts of the world where Internet literacy and access is increasing, but billions of people live day to day without access to affordable banking services. In particular, in regions where a government-issued fiat currency is unstable due to frequent regime changes, heavy capital controls or uncontrolled inflation, bitcoins present itself as an extremely attractive alternative.[19]

18 Already, Bitcoin microfinancing – where Bitcoin is used as a medium to transfer small loan amounts from lenders to borrowers – is achieving success in countries such as Kenya, Tanzania and Afghanistan.[20] Since microfinance deals with small amounts of money, traditional bank transaction fees can be high relative to the amount of the loan. By transferring funds in

17 While some private keys are stored on physical tokens, other online services (*eg*, StrongCoin, an online Bitcoin wallet) allow for the recall of private keys through encrypted web-based interfaces.

18 B P Eha, "Why Regulate Bitcoin?" *The New Yorker* (18 November 2013).

19 J B Turpin, "Bitcoin: The Economic Case for a Global Virtual Currency Operating in an Unexplored Legal Framework" (2014) 21(1) *Indiana Journal of Global Legal Studies* 335 at 348.

20 J Fong, "How Bitcoin Could Help the World's Poorest People" PolicyMic (14 May 2013) at http://mic.com/articles/41561/bitcoin-price-2013-how-bitcoin-could-help-the-world-s-poorest-people (accessed 12 July 2015).

Bitcoin,[21] these costs can be reduced and the savings passed on to borrowers in the form of lower interest rates.

CHALLENGES OF VIRTUAL CURRENCIES

Criminality

Bitcoin-facilitated crime: trade in illegal goods and services

19 We have already seen briefly how the relative anonymity offered by Bitcoin can facilitate the purchase of illegal goods and services online. Bitcoin in effect functions as a digital analogue to cash, which medium has traditionally been used to enable illicit exchanges in person.

20 Bitcoin's association with Silk Road has certainly damaged its reputation; but this is only the tip of the iceberg. While Silk Road facilitated the sale of illegal articles such as forged identity documents and illicit drugs, it at the very least did not permit the sale of any goods that resulted from harm or fraud, such as child pornography or stolen credit card details. Other online fora, however, do not demonstrate the same moral compunctions. Increasingly, Bitcoin is being used to fuel other forms of undesirable trade[22] within the deepest recesses of the Dark Web.[23]

Money laundering and terrorism financing

21 The pseudonymity offered by Bitcoin also lends itself to abuse by groups seeking to launder money in order to finance terrorism.

---

21 This is usually done via mobile phone, as individuals in the poorest countries usually do not have access to a computer. For example, the M-Pesa mobile payment system in Kenya allows individuals to store balances, make payments and send money all through their mobile phones.

22 D Carroll, "European Banking Authority to Consider Bitcoin Regulation" *Public Affairs Policy Review* (December 2013) at http://www.policyreview.eu/european-banking-authority-to-consider-bitcoin-regulation (accessed 12 July 2015).

23 The Dark Web is comprised of World Wide Web content that exists on networks that overlay the public Internet, requiring specific software, configurations or authorization to access. It forms part of the Deep Web, which is the part of the Internet not indexed by search engines.

While cash at the very least required face-to-face transactions, Bitcoin permits the development of faceless customer relationships through its online character. As a result, anonymous funding can take place through virtual exchanges that do not properly identify the funding source.

22 The global reach of virtual currency also increases – exponentially – anti-money laundering and counter-terrorism financing risks. Where previously cash would have, for most part, limited such illicit activities to within a single jurisdiction, money laundering and terrorism financing in the modern age can take place across several countries, some without adequate anti-money laundering and counter-terrorism financing controls in place. This fragmentation of process causes responsibility for anti-money laundering supervision and counter-terrorism financing enforcement to become very unclear.[24]

23 Indeed, given that there is no central authority overseeing the ecosystem of most decentralised virtual currencies, law enforcement agencies are unable to target a single central location or entity to investigate wrongdoing or to seize assets.[25]

Bitcoin-specific crime: digital exchanges and wallets

24 One of the largest criminal opportunities in Bitcoin manifested itself in Mt Gox, the bitcoin exchange based in Tokyo, which until the time of its implosion had been the largest digital currency exchange for Bitcoin online. In early 2014, the company announced that around 850,000 bitcoins (approximately US$450m at the time) belonging to both customers and Mt Gox itself had gone missing or been stolen. Subsequently, Mt Gox suspended all

24 Financial Action Task Force Report, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks" *Financial Action Task Force* (June 2014) at p 9.

25 It should be noted that *centralised* virtual currencies present less of a difficulty to contain: in 2013, authorities in Costa Rica shut down Liberty Reserve, a centralised virtual currency service created by a private company for the express purpose of facilitating money laundering. Unlike Bitcoin, Liberty Reserve promised its users anonymity; in contrast, Bitcoin provides a public record of all transactions.

trading and filed for corporate rehabilitation under Japanese insolvency laws.

25 As at the time of writing it is still unclear what was truly responsible for the missing bitcoins. Mt Gox maintains that the bitcoins' disappearance was a gradual theft over a relatively long duration attributable to a transaction malleability flaw in the underlying code.[26] Another theory proposes that two automated trading robots or "bots" at Mt Gox had gone rogue by "buying" bitcoins at random prices (but never actually spending any fiat money on the transactions) before disappearing with the "bought" bitcoins. Still another theory contends that the missing bitcoins resulted completely from fraud or mismanagement *within* Mt Gox.

26 The meltdown of the Mt Gox exchange was and still remains a public relations nightmare for Bitcoin infrastructure. In spite of the existence of the public blockchain, which purports to record validated transactions, police investigators still do not know, for most part, what happened to the missing bitcoins.[27]

27 This perhaps should not have come as a surprise, given the nascent nature of the technology and the relative lack of experience in the subject matter on the part of law enforcement in Japan and around the world. The key takeaway, however, appears to be that the security offered by the Bitcoin protocol itself will not count for much *if it is not supported by equally robust security in Bitcoin exchanges and other parts of the Bitcoin ecosystem*. As has been noted by some commentators, "Mt Gox was like a bank storing

26 Such a flaw would permit a person to change the unique identifier of a Bitcoin transaction before the transaction is confirmed and recorded on the blockchain. In effect, exploitation of this flaw would allow someone to pretend that a transaction has not taken place when in actual fact it had.

27 Around 200,000 bitcoins were "found" shortly after Mt Gox's initial announcement that it had lost nearly 850,000 bitcoins. According to a notification on Mt Gox's website, these 200,000 bitcoins were apparently discovered in an electronic wallet that had been in existence since 2011. However, investigators found that Mt Gox's account contradicted the evidence on the blockchain, which showed that the bitcoins had only been recently transferred to a single new address.

valuables in the lobby entrance."[28] In order for Bitcoin to become a truly viable alternative to traditional currency, Bitcoin exchange security will have to mature to become as tight as that at traditional banks.

28 In order to safeguard their bitcoins without having to rely on insecure exchanges, some users have opted to use digital wallets that are stored on remote servers.[29] While these digital wallets simplify the process of holding bitcoins for non-technical users, there are other attendant problems. For example, because these digital wallets contain private keys that provide access to customers' bitcoins, digital wallet servers have become a priority target for cybercriminals. In late 2013, 4,100 bitcoins (worth around US$1.2m at the time) were stolen from inputs.io, a digital wallet service for bitcoins.[30] To date there has been no authoritative investigation into the allegations concerning the stolen bitcoins, including both allegations about external hackers and other allegations that the operators of inputs.io themselves had absconded with the bitcoins.

29 In order to reduce the likelihood of cybercriminals making off with the contents of digital wallets, best practices have been promulgated recommending, *inter alia*, the locking of digital wallet passwords in a bank vault.[31] Until digital wallet services develop

28 T Wan & M Hoblitzell, *Bitcoin: Fact. Fiction. Future.* (Deloitte University Press, 26 June 2014) at p 6.

29 There are two types of digital wallet – client-side wallets and server-side wallets. Client-side wallets are maintained by the customer (*eg*, smartphone wallets utilising near-field communication to transfer customer credentials), while server-side wallets are provided by an organization and maintained for the benefit of the customer (*eg*, virtual currency wallets issued by companies providing digital wallet services). Both types of wallet are made up of a software and information component – the software provides encryption for personal data and for the transaction in question, while the information comprises data extracted from user inputs.

30 R McMillan, "$1.2m Hack Shows Why You Should Never Store Bitcoins on the Internet" *Wired.com* (7 November 2013).

31 As recommended on the "Secure Your Wallet" section of the bitcoin.org website at https://bitcoin.org/en/secure-your-wallet (accessed 12 July 2015). It should be noted that unlike bank account passwords, there are very limited password recovery options with Bitcoin.

more user-friendly and secure processes, it is unlikely that Bitcoin will be able to penetrate the mainstream market.

Consumer protection

Irreversible transactions

30 The manner in which Bitcoin architecture is structured means that payments are usually irreversible. While this helps minimise chargeback fraud,[32] whenever payments are made due to fraud or error, there is no mechanism for correction or rescission. Given the variety of payment schemes available to the consumer in this modern age, the lack of reversibility puts Bitcoin at a significant disadvantage.[33] For example, in the US, credit card dispute rights are guaranteed by the Fair Credit Billing Act,[34] providing consumers with a mechanism to protect themselves against unauthorised transfers.

Informational asymmetry

31 Another concern from the consumer protection perspective is that Bitcoin, as a payment system, is complex. Users who do not have a proper grasp of how the system works can download – quite easily – software that will allow them to start making payments with Bitcoin. These users will usually not be aware of the risks they are taking by participating in the Bitcoin framework. Such risks, in conjunction with the absence of central administrative oversight and the relative legal uncertainty surrounding Bitcoin, combine to present an extremely high-risk situation. Bitcoin is ultimately an

32 This is where a consumer makes a purchase online with a credit card, then requests a chargeback from the bank issuing the credit card after he or she has received the goods or services "purchased". Once this chargeback request is approved, the transaction is cancelled and the consumer is refunded his payment – while still having possession of the goods or services in question. The merchant, on the other hand, usually has to pay a fee to the bank for the chargeback transaction.

33 R Böhme *et al*, "Bitcoin: Economics, Technology and Governance" (2015) 29(2) *Journal of Economic Perspectives* 213 at 227.

34 15 USC (US) § 1666.

experiment that could fail if poorly informed people, who treat the virtual currency as equivalent to other more traditional forms of currency, are unable to exit the system because of its illiquidity.

Deflation

32 As a result of the total number of bitcoins being capped at a finite 21 million, Bitcoin is an inherently deflationary currency. The global modern economy, on the other hand, is premised upon state-issued, infinite-supply and *inflationary* currencies. It has been noted by some commentators that "[f]or a global economy that runs on credit and is no longer accustomed to the rigor of monetary control, such a system [like Bitcoin] could do great harm if it's not properly introduced."[35]

33 Indeed, for deflationary currencies such as Bitcoin, which are limited in supply and highly sought after, it would be entirely conceivable that users would eventually turn to "extreme hoarding", particularly in times of financial crisis.[36] Such hoarding behaviour would restrict the flow of money to other actors in the economy and, as a result, accelerate the economic downturn. Given the decentralised nature of Bitcoin, there would be no central bank to inject more money into the economy to free up credit for the creation of jobs. While it is unlikely that Bitcoin or supply-limited cryptocurrencies would form a significant part of currencies in circulation in any particular economy, where such a situation does come to pass (or in closed systems where such cryptocurrencies are the *de facto* currency) it is possible that a depression would result.

35 P Vigna & M J Casey, *The Age of Cryptocurrency* (St Martin's Press, 2015) at p 294.

36 M T Williams, "Testimony of Mark T Williams" *New York State Department of Financial Services* (28–29 January 2014) at http://www.dfs.ny.gov/about/hearings/vc_01282014/williams.pdf (accessed 12 July 2015).

REGULATION

Existing regulatory approaches

34 The challenges highlighted in the preceding section will present a formidable hurdle to regulators, many of whom are still coming to grips with the disruptive nature of Bitcoin technology. It is perhaps for this reason that the legal treatment of Bitcoin varies to such a great extent among different countries.

35 Brazil, for example, has been very quick to welcome the adoption of Bitcoin. In October 2013, the Brazilian authorities passed a law regulating the creation and exchange of "electronic currencies", defined as "resources stored on a device or electronic system that allow the end user to perform a payment transaction".[37] The law, which was motivated by a vision of mobile payment systems becoming the norm in Brazil, brings virtual currencies within the regulatory ambit of the authorities. The recognition of Bitcoin as an actual currency deserving of regulation had a great impact on its credibility – in December 2013, less than two months after the law was enacted, the trading volume of Bitcoin went up to around US$4.5m on the Brazilian national exchange for Bitcoin, Mercado Bitcoin.[38]

36 China, on the other hand, has taken a very different approach. On 5 December 2013, the central bank of China announced that financial institutions in China would be prohibited from handling Bitcoin transactions.[39] Subsequently on 1 April 2014, the central bank further ordered for the closure of all Bitcoin trading accounts held in commercial banks.[40]

37 Lying in between the courses charted by Brazil and China is the wait-and-see approach taken by many countries that have yet

37 P D Filippi, "Bitcoin: A Regulatory Nightmare to a Libertarian Dream" (2014) 3(2) *Internet Policy Review* 1 at 5.

38 P D Filippi, "Bitcoin: A Regulatory Nightmare to a Libertarian Dream" (2014) 3(2) *Internet Policy Review* 1 at 5.

39 S Yang & S Lee, "China Bans Financial Companies from Bitcoin Transactions" *Bloomberg* (5 December 2013).

40 C Deng & L Wei, "China Cracks Down on Bitcoin" *The Wall Street Journal* (1 April 2014).

to determine the legal status of Bitcoin. Singapore, for instance, recognises that regulators must "maintain a finely-tuned balance between the growth of industry and the mitigation of risk for consumers".[41] This thinking is consistent with the stipulation by the Monetary Authority of Singapore (the country's central bank) in March 2014[42] that any virtual currency intermediary that buys, sells or facilitates the exchange of virtual currency with fiat currency will be required to observe reporting requirements, implement record-keeping measures[43] and notify the authorities of suspicious transactions.[44] The Inland Revenue Authority of Singapore has taken a similar moderated approach, welcoming virtual currencies as a valid mode of payment but requiring that they be subject to normal income tax rules.[45] The Inland Revenue Authority has also stipulated that while sales of virtual currencies are not forbidden, such sales are to be construed as a *supply of services* and are therefore are not exempt from goods and services tax.[46]

38 Given the hodgepodge nature of regulatory responses to Bitcoin, it would appear that the very first issue for regulators to agree on would be the legal status of Bitcoin. Without a consistent legal treatment of Bitcoin, users of the virtual currency would

41 Foo Chek-Tchung, Deputy Director, Specialist Risk Department, Monetary Authority of Singapore, speaking at the "Virtual Currencies – The Future of Money or Just Another Passing Fad?" panel at the Global Technology Law Conference (29 June 2015).

42 Monetary Authority of Singapore, "MAS to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks" (13 March 2014).

43 These requirements and measures are set out in the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap 65A, 2000 Rev Ed) and the Terrorism (Suppression of Financing) Act (Cap 325, 2003 Rev Ed).

44 The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap 65A, 2000 Rev Ed) envisages, at s 39, a duty on the part of the intermediary to disclose suspicious transactions to the Suspicious Transaction Reporting Office.

45 See Inland Revenue Authority of Singapore, "Income Tax Treatment of Virtual Currencies" at https://www.iras.gov.sg/irashome/GST/GST-registered-businesses/Specific-business-sectors/e-Commerce/#title5 (accessed 21 October 2015).

46 See Inland Revenue Authority of Singapore, "Sale of Virtual Currency" at https://www.iras.gov.sg/irashome/GST/GST-registered-businesses/Specific-business-sectors/e-Commerce/#title5 (accessed 21 October 2015).

inevitably come to engage in regulatory arbitrage, leaving some economies at risk of capital flight.[47] Despite this risk, however, regulators around the globe have not been able to reach any consensus on a consistent approach to the legal status of Bitcoin. We turn now to the two largest markets for Bitcoin – the US and Europe – to see why.

Legal status of Bitcoin in the United States and Europe

Currency

39 Like all virtual currencies, Bitcoin appears to fulfil the three essential functions of money.[48] It serves as a medium of exchange when used to buy goods or services from merchants who accept bitcoins for payment. It satisfies the unit of account criterion when merchants choose to denominate the prices of their goods and services in bitcoins. And finally, bitcoins function as a store of value when users hold on to them for speculative purposes, to sell or send at a later date.

40 The key question, therefore, appears to be: are private currencies like Bitcoin legal? In the US, privately issued currencies are not prohibited, insofar as they do not resemble or compete with the actual US currency.[49] The Stamp Payments Act, however, does make it an offence to issue, circulate or pay out "any note, check, memorandum, token or other obligation … intended to circulate as money or to be received or used in lieu of lawful money of the United States".[50] While it is difficult to envisage Bitcoin, which has no third party issuer, as an "obligation" under the Stamp Payments Act, and while the Act itself appears to contemplate physical

47 The reality of the risk of capital flight will depend on a number of conditions, including in particular the market appetite for the currency that individuals are fleeing from.

48 See para 1 above.

49 See Art I § 10 of the US Constitution and 18 USC (US) §§ 485–486. See also D A Dion, "Defendant Convicted of Minting His Own Currency" (18 March 2011) at http://www.fbi.gov/charlotte/press-releases/2011/defendant-convicted-of-minting-his-own-currency (accessed 12 July 2015).

50 Stamp Payments Act 18 USC (US) § 336 (1862).

objects rather than computer files, the manner in which the Act may apply to Bitcoin is unknown.

41 In Europe, the European Banking Authority has indicated that virtual currencies, including Bitcoin, are "a form of unregulated digital money, not issued or guaranteed by a central bank, which can act as means of payment".[51] However, the European Central Bank has also previously defined virtual currencies, including Bitcoin, as "a type of unregulated, digital money ... which act[s] as a medium of exchange and as a unit of account within a particular virtual community", but which does *not* clearly "fulfil the 'store of value' function in terms of being reliable and safe".[52] This caveat by the European Central Bank is of no small moment; the characterization of virtual currency under law goes a long way to affecting the manner in which the law applies to its misappropriation, the nature of the transactions carried out with it, and so on and so forth. The knee-jerk rejoinder to this, of course, is that the fiat currencies of countries such as Argentina and Zimbabwe – notoriously unstable and inflationary – also do not qualify as currencies for failure – in effective terms – to satisfy the "store of value" criterion. The precise legal status of Bitcoin as a currency, accordingly, remains uncertain.

Commodity or good

42 Given the finite numbers of Bitcoins projected and the diminishing pace at which new bitcoins are mined, it would appear *prima facie* that Bitcoin – which is traded on Bitcoin exchanges worldwide – shares many traits with an ordinary *commodity*, which has been defined to be a "comparatively homogeneous product" that is "often traded on commodity exchanges".[53] Both Bitcoin and commodities are subject to the laws of supply and demand in the determination of their value. However, the Harmonised

51 European Banking Authority, "Warning to Consumers on Virtual Currencies" (12 December 2013).

52 European Central Bank, *Virtual Currency Schemes* (October 2012) at pp 11 and 13.

53 "Economics A-Z Terms: Commodity" *The Economist* at http://www.economist.com/economics-a-to-z/c#node-21529407 (accessed 12 July 2015).

Commodity Description and Coding System[54] is clearly predicated upon the assumption that commodities are tangible items, and does not appear at present to extend to digital protocols such as Bitcoin.

43 The Agreement on the European Economic Area[55] separately provides that a *good* can be either a "material" or a "product".[56] A "material" is defined as "any ingredient, raw material, component or part *etc*, used in the manufacture of the product". A "product" means "the product being manufactured, even if it is intended for later use in another manufacturing operation". Since Bitcoin is not used in the manufacture of any product, it cannot be a "material"; and since it is also not being "manufactured" in the ordinary sense of the word – bitcoin mining is a process quite different from manufacturing, which countenances a single manufacturer available to comply with regulations set out by regulators and to be responsible for defects – it cannot be a "product". Bitcoin therefore also appears to fall outside the definition of a good.

44 The Commodity Exchange Act of the US defines commodities as all "goods and articles … and all services, rights, and interests … in which contracts for future delivery are presently or in the future dealt in". Accordingly, it would appear that Bitcoins could qualify as commodities, since they could be "articles" or more likely "services" that can be traded (as they are on Bitcoin exchanges) and made subject to futures contracts.

45 As it turns out, the US Commodity Futures Trading Commission, which has authority over the regulation of commodity futures and the markets where they trade, has taken a keen interest in Bitcoin.[57] Notwithstanding this, it should be noted that the Commission only has authority only over commodity

54 HS Nomenclature 2012 Edition (World Customs Organization).

55 Agreement on the European Economic Area [1994] OJ L1/3.

56 Protocol 4 on the rules of origin to the Agreement on the European Economic Area [1994] OJ L1/54, Art I point (d).

57 T Alloway *et al*, "US Regulators Eye Bitcoin Supervision" *Financial Times* (6 May 2013).

futures, and not commodities themselves.[58] Insofar as an exchange of bitcoins for fiat currency takes place instantaneously, and not as part of a futures contract,[59] the extent to which the Commission can regulate bitcoins as commodities could be limited. In any event, the treatment of bitcoins as commodities is untested in the US.

Financial instrument

46 As bitcoins possess value derived from market demand and supply, Bitcoin can be said to represent the ownership of financial assets, and therefore should be rightly considered a class of financial instrument. In this connection, the Markets in Financial Instruments Directive,[60] promulgated by the European Parliament and Council, defines a common financial instrument, the transferable security, as being "negotiable on the capital market" and inclusive of securities such as those "giving the right to acquire or sell any 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".[61]

47 It is beyond doubt that Bitcoin is negotiable[62] – it is being traded on Bitcoin exchanges around the world, at relatively volatile

58 J Brito & A Castillo, *Bitcoin: A Primer for Policymakers* (Mercatus Center, George Mason University, 2013) at pp 30–31.

59 Conceivably, a Bitcoin futures contract could be made and regulated by the Commission, but only if the underlying bitcoins are construed to be commodities. If they are viewed as intangibles, the Bitcoin futures contract would have to be regulated as a security interest.

60 Directive 2004/39/EC of the European Parliament and of the Council on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council, and repealing Council Directive 93/22/EEC [2004] OJ L145/1 (21 April 2004) ("Directive 2004/39/EC").

61 Directive 2004/39/EC at Art 4, para 1, point 18.

62 The word is used here in the same vein that the European Parliament and Council employed it in its definition of a transferable security being "negotiable on the capital market", *ie*, being transferable from one person to another by being delivered so that the title passes to the transferee. Pursuant to the terms of the Markets in Financial Instruments Directive, such

(*continued on the next page*)

prices, is testament to this fact. It is also clear that bitcoins are transferable, whether from user to user or between exchanges and users. Under the European framework, therefore, it would appear that Bitcoin qualifies as a financial instrument and ought to be regulated as such. Indeed, Bitcoin exchanges – by providing "investment services" defined in the Markets in Financial Instruments Directive as the "[r]eception and transmission of orders in relation to one or more financial instruments" – seem also to slot nicely within the definition of "investment firms" under the Directive,[63] thereby leaving them subject to regulation by the same.

48 However, the US Securities Exchange Act of 1934, which governs the exchange of securities in the US and contains registration, disclosure and anti-fraud provisions,[64] does not appear to countenance Bitcoin as a security for its purposes. The Act defines "securities" broadly to comprise notes, stocks and investment contracts. Bitcoin is not an instrument wherein the maker (indeed, who would the maker be in the context of Bitcoin, since there is no one "issuer") promises to pay a sum of money to another party; therefore it does not possess note-like characteristics.[65] Bitcoin also does not qualify as stock as it does not confer voting or dividend rights.[66]

49 Finally, it is also doubtful that Bitcoin will be classified as a form of investment contract. The Supreme Court of the US had in *SEC v WJ Howey Co*[67] stipulated four elements to be satisfied before a finding of the existence of an investment contract may be made: (1) an individual investing money; (2) into a common enterprise; (3) from which profits are expected; (4) which profits are generated solely from the efforts of a third party. In the case of Bitcoin, while

"transferable securities" include shares in companies and other forms of security not traditionally falling within the rubric of "negotiable instrument".

63 Directive 2004/39/EC at Annex I(A).

64 15 USC (US) § 78.

65 D A Dion, "I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker-Cash" (2013) *University of Illinois Journal of Law, Technology and Policy* 165 at 176-177.

66 R Grinberg, "Bitcoin: An Innovative Alternative Digital Currency" (2012) 4 *Hastings Science and Technology Law Journal* 160 at 195.

67 328 US 293 (1946).

an individual may pay fiat currency to purchase bitcoins, that payment does not equate to investment. In any event, the money used to purchase bitcoins does not go to a common enterprise that is expected to generate profits via the efforts of any third party.[68]

Status report?

50 As can be gathered from the foregoing discussion, even limiting our scrutiny to only the US and Europe, the issue of the legal classification of Bitcoin is extremely complex. Bitcoin could be considered a commodity in the US, but not in Europe; and a financial instrument in Europe, but not in the US. Closer to home in Singapore, the authorities have taken a pragmatic approach, construing payments in bitcoins and sales of Bitcoin to be taxable, but maintaining that virtual currencies are not "money", "currency" or "goods". The differing approaches adopted in these three regions underscores the difficulty in policy-making *vis-à-vis* Bitcoin and other decentralised virtual currencies: without consensus as to what Bitcoin actually *is*, deciding how to regulate Bitcoin will provide a stern challenge.

51 One observant commentator, however, has noted that "[t]he mere recognition of Bitcoin as one of the … categories within the current legal framework would not have any practical effect, since Bitcoin still would contradict the traditional angle of legal reasoning based on the centralised approach to money, payments and financial services".[69]

52 An example to flesh out this observation would be instructive. The Consumer Financial Protection Bureau in the US has issued rules requiring remittance providers to disclose exchange rates and fees associated with international funds transfers, and to

68 M K-M Ly, "Coining Bitcoin's 'Legal-Bits': Examining the Regulatory Framework for Bitcoin and Virtual Currencies" (2014) 27(2) *Harvard Journal of Law and Technology* 587 at 598.

69 S Shcherbak, "How Should Bitcoin be Regulated?" (2014) 7(1) *European Journal of Legal Studies* 45 at 85.

investigate and remedy processing errors.[70] The rules also require that consumers be given 30 minutes or *more* to cancel a transfer. The application of these rules to Bitcoin would be anathema: Bitcoin transactions are irreversible. While compliance might be obtained through deliberate delays in the execution of transfers, this would defeat the purpose of Bitcoin technology, which at its core exists to enable fast and fuss-free transactions.

53 The answer, therefore, may not lie in global accord for the legal classification of Bitcoin in accordance with existing categories of regulated articles. But what of new categories and *sui generis* legislation specifically to rein Bitcoin in? This, too, is an approach to be counselled against. The Bitcoin protocol as it currently exists – with its emphasis on decentralisation and reliance on the peer-validated blockchain – is practically impossible to amend, given the diffusion and pseudonymity of the relevant stakeholders throughout the world. Any regulatory requirements imposed *on* the Bitcoin protocol layer itself would be as ineffectual as the service of a cease-and-desist letter on the Bitcoin Foundation.[71] In any event, the protocol's open-source nature would mean that the protocol would never be amended in a manner that would not be for the benefit of the majority of Bitcoin stakeholders.

54 The proper way forward to reach a satisfactory balance between regulators and users, therefore, would appear to require a

70 Consumer Financial Protection Bureau, "Summary of the Final Remittance Transfer Rule (Amendment to Regulation E)" (2013) at http://files.consumerfinance.gov/f/201305_cfpb_remittance-transfer-rule_summary.pdf (accessed 12 July 2015).

71 This was in fact done by the California Department of Financial Institutions on 30 May 2013. The cease-and-desist letter stated that the Bitcoin Foundation may have been "engaged in the business of money transmission without having obtained the license or proper authorization required by the California Financial Code", and warned the Foundation that it was a federal violation to engage in money transmission without the appropriate state license or registering with the US Treasury Department. Embarrassingly for the California Department of Financial Institutions, the Bitcoin Foundation was and is only a non-profit organization established to standardise, protect and promote the use and adoption of Bitcoin. It does not conduct any money transmission business whatsoever.

more nuanced approach involving the regulation of other layers of the Bitcoin ecosystem.[72]

Principles for a balanced regulatory framework

Deciding at which layer to regulate

55 We have just seen that for regulators to impose constraints at the logical or conceptual layer of the Bitcoin protocol – "computer layer", if you like – would be ineffective. Likewise, regulation of the next immediate layer – users – would be equally unproductive and just as impossible. Bitcoin users are a legion and scattered throughout the globe; any legislation targeting them as a demographic would first have to overcome issues of limited resources and jurisdiction. In addition, to impose restrictions that can only be selectively and sporadically enforced would invariably lead to the undermining of the overall regulatory framework.

56 This brings us to the third layer: online merchants, including exchanges and digital wallet services, which trade in and accept bitcoins as payment. Given their relatively small numbers and their potential for high volumes of Bitcoin transaction traffic, regulation can and should attach to this layer. To combat the risk of criminality in connection with the use of Bitcoin highlighted earlier in this article,[73] the implementation of know-your-customer and anti-money laundering policies can be made mandatory for these merchants. With merchants maintaining records of every transaction, identifying information on their customers can be made available to the authorities for inspection in the event of any suspicious transactions.

57 In respect of consumer protection, the issuance of guidelines to users and merchants alike by regulatory bodies would go a long way to ameliorating informational asymmetries in the Bitcoin ecosystem. These guidelines can help at each of the individual

72 The idea of "layers" in the Bitcoin ecosystem has been adopted from A Yee, "Internet Architecture and the Layers Principle: A Conceptual Framework for Regulating Bitcoin" (2014) 3(3) *Internet Policy Review* 1. However, a different set of layers has been identified for this article.

73 See paras 19–28.

layers highlighted above:[74] for example, by clarifying in an official capacity the unregulated nature of Bitcoin technology (conceptual layer); communicating to users that Bitcoin transactions are irreversible and that use of the virtual currency is at the users' own risk (user layer); and providing detailed regulations about how merchants should go about complying with know-your-customer and anti-money laundering requirements, and the rights and remedies available to users against these merchants in the event of default (merchant layer).

Justifying a permissive Bitcoin policy

58 In the aftermath of the Silk Road and Mt Gox debacles, the knee-jerk reaction of policymakers in some quarters was to lobby for restrictions or even bans on the Bitcoin technology.[75] Submission to these impulses, however, is likely to be counter-productive. As a technology, Bitcoin is neither good nor bad; like cash, Bitcoins can be used for legitimate and illicit purposes. A good policy would dictate only the restriction of Bitcoin for illicit uses. This point is all the more significant when we consider that as Bitcoin matures and its vulnerabilities are identified and plugged, legitimate uses of the technology will in all likelihood outstrip the illegitimate uses. For example, the Silk Road online marketplace had a monthly transaction quantum of US$1.2m. In contrast, the overall Bitcoin economy processed US$770m in transactions during the month of June 2013, sometime just before the authorities clamped down on Silk Road.[76]

59 An onerous regulatory framework or an outright ban would punish the vast majority of (law-abiding) Bitcoin users and deprive

74 See paras 54–55.

75 C Schumer & J Manchin, "Letter to Attorney General Eric Holder and Drug Enforcement Administration Administrator Michele Leonhart" (6 June 2011) at https://votesmart.org/public-statement/615129/letter-to-eric-holder-attorney-general-and-michele-leonhart-administrator-drug-enforcement-administration-illegal-drug-websites#.VnDXNdJ96Uk (accessed 12 February 2016).

76 J Brito, "National Review Gets Bitcoin Very Wrong" (20 June 2013) at http://techliberation.com/2013/06/20/national-review-gets-Bitcoin-very-wrong (accessed 12 July 2015).

them of access to an efficient and groundbreaking technology. At the same time, the small minority of tech-savvy criminal users would continue to be able to dodge regulation by driving themselves further underground into the Dark Web. This unfortunate situation would result simply because Bitcoin is by its nature *decentralised*; making the use of Bitcoin illegal would not achieve much, since the peer-to-peer architecture means that there is no single entity to be targeted, moreover the shutting down of individual node computers would have little effect on the rest of the network. Society would therefore be giving up potential utility gains from a next-generation payments system without seeing any corresponding reduction in the associated criminal activities.

60 Separately, should any one country decide to prohibit or restrict severely the use and adoption of Bitcoin – China, for instance – other countries with more permissive Bitcoin policies, like Finland,[77] would stand to benefit from regulatory arbitrage. It is submitted that no country would voluntarily choose to be left behind in the adoption of new technology that could potentially benefit its citizens in so many ways, and that policy choices should reflect that. The international competitive advantage that comes from being a first-mover in any nascent market should not be discounted.

A possible regulatory framework

61 Marian at the University of Florida Levin College of Law has proposed a novel regulatory framework for Bitcoin. The proposed approach addresses the issues of criminality associated with Bitcoin, while maintaining the core functionality of the currency.[78] Marian's premise is that to many governments, the most obvious regulatory response to increased criminality facilitated by the pseudonymous Bitcoin would be to impose stricter sanctions for infractions, given that increasing *surveillance* of Bitcoin users –

77 M Clinch, "Bitcoin Utopia? Interest is Sky High in this Euro Nation" *CNBC* (4 April 2013).

78 O Marian, "A Conceptual Framework for the Regulation of Cryptocurrencies" (2015) 82 *University of Chicago Law Review* 53.

who, as we have noted, make up a huge number and spread throughout the world – would be all but impossible.

62 However, this approach would mean that the same crime would attract different penalties, depending on the currency – fiat or virtual – with which it was committed. This is a difficult normative proposition to accept. In addition, there is also academic literature that suggests that "increased *probability* of sanction has a larger deterrent effect than increased *severity* of sanction".[79] By increasing sanctions, governments may not be achieving the optimal level of deterrence that they seek to achieve.

63 To avoid these issues, Marian suggests the adoption of a system whereby "an individual transacting in cryptocurrencies in the open economy could elect between bearing the cost of regulation, and waiving the trait that makes cryptocurrencies suited for illicit behavior – anonymity".[80] In essence, he proposes that the regulatory costs that come with virtual currencies be traded off with anonymity. Accordingly, where a user provides his or her identification information to an online merchant in a transaction, any regulatory taxes that the transaction is subject to become waivable. On the other hand, where a user prefers to maintain anonymity (not only in the context of criminal use, but also in respect of uses where privacy is prized), the transaction will be fully taxed.

64 It may be contended that this framework does not remove criminal activity – it simply makes it more expensive for criminals to do business. This critique, however, is easily addressed. The taxes imposed in connection with the non-disclosure of identification information can be tailored such that it does not make economic sense for criminals to engage in sustained illegitimate use of Bitcoin. Alternatively, to take a more extreme

79 O Marian, "A Conceptual Framework for the Regulation of Cryptocurrencies" (2015) 82 *University of Chicago Law Review* 53 at 61, citing G S Becker, "Crime and Punishment: An Economic Approach" (1968) 76 *Journal of Political Economy* 169 at 176.

80 O Marian, "A Conceptual Framework for the Regulation of Cryptocurrencies" (2015) 82 *University of Chicago Law Review* 53 at 62.

form of the idea, the use of any bitcoins that have been transferred without sufficient disclosure can be prohibited altogether.

65 Marian's proposed framework has an additional knock-on benefit: with more and more users voluntarily disclosing identification information, it becomes easier to identify other pseudonymous users even where they have not disclosed any identification information. Accordingly, with increased voluntary disclosure of identification information by legitimate users, the Bitcoin protocol becomes much less attractive to illegitimate users, since they would not want to be exposed to the probability of increased detection.

66 While the proposed framework invariably involves more costs for law-abiding users who, from time to time, wish to transact privately, it is arguable that the societal gains derived from the ability to monitor, dissuade and enforce against criminals would outweigh the disutility involved therein. However, it should not be overlooked that society may well not be able to accept, even on a conceptual level, a criminal code that is premised upon an optional system where criminals may elect to pay their way out of detection and prosecution.[81]

CONCLUSION

67 Developments in the virtual currency space are continuing to evolve rapidly. Financial technology innovations such as Bitcoin, with their unprecedented characteristics, bring with them many new risks and opportunities and have tremendous potential to disrupt existing business models. Against this backdrop, regulators must be aware of the need to anticipate the emergence of new financial, economic and social interaction and linkages. While financial innovation is to be prized, the mandate to minimise financial risk cannot be gainsaid.

68 Importantly, given the decentralised nature of Bitcoin, regulation in a single jurisdiction can no longer be considered an effective response to combating the risks of trade in illegal goods,

81 The author is grateful to Alexander Loke for this insight.

terrorism financing and money laundering. Intermediaries in one country are now able to transact easily with intermediaries in another. A coordinated approach across multiple jurisdictions is therefore necessary for risk mitigation in the cryptocurrency era. However, while an international effort is required, the present lack of virtual currency regulation in most countries prevents any such effort from crystallising in a concrete fashion. Strong thought leadership, particularly from the US and Europe, would go some way to ameliorating the unsatisfactory status quo.

69 We are poised at the cusp of the take-off of a breathtaking technology that could, if properly harnessed, bring banking and financial services to even the most disenfranchised of populations. A technology that could pave the way for a global payments system that would do away with the risks and inefficiencies associated with government-issued currencies, and by extension even foreign exchange. Indeed, the annual net savings from the adoption of Bitcoin, just for merchants and consumers alone, could potentially surpass US$150bn.[82] The Bitcoin industry must therefore be permitted to explore, but with caution; and regulators would do well to regulate, but through the lens of innovation.

70 As Nelson Mandela once said, "Money won't create success, the freedom to make it will." The proper formulation of Bitcoin policy will determine not just the success or failure of a niche payment system, but the future of wealth and the manner in which it is distributed throughout the world.

---

82 R Leal, "Is Bitcoin the Future of Payments?" *Top of Mind* (Goldman Sachs Global Macro Research, Issue 21, 11 March 2014) at p 18 <http://www.academia.edu/7413513/All_About_Bitcoin> (accessed 12 July 2015).

Contracting for the "Internet of Things": Looking into the Nest

The world of the "Internet of Things" ("IoT") is just one manifestation of recent developments in information and communication technologies, closely tied to others, including "cloud computing" and "big data". For purposes in this paper, the "Thing" in the IoT is "any physical entity capable of connectivity that directly interfaces the physical world, such as embedded devices, sensors and actuators".[1] In considering IoT contracts, this paper adopts a case study approach, examining the complexity of IoT through the lens of a specific product: the Nest connected thermostat, part of the Nest Labs business and owned by Google. The authors focus on the "legals" of Nest (contractual documents, licences, *etc*) to provide a case study of IoT complexity. After touching on some general contract law issues in relation to the IoT supply chain, the authors examine the rights and obligations represented in these legals and discuss the extent to which, collectively, they present a coherent and comprehensible private law framework. The authors then consider the extent to which certain statutory regimes may treat IoT contracts in terms of addressing two characteristic contractual concerns: liability attribution and unfair terms. Our main conclusion is that the world of IoT demonstrates a need to consider recasting the concept of product to reflect the frequent inextricable mixture of hardware, software, data and service.

Guido **NOTO LA DIEGA***
LLB (Università Degli Studi Di Palermo), LLM (Università Degli Studi Di Ferrara), PhD (Università Degli Studi Di Palermo); Associate Lecturer in Law, Buckinghamshire New University, Former Research Assistant, Centre for Commercial Law Studies, Queen Mary University of London.

1 Microsoft Cloud Computing Research Centre's definition. See also J Singh *et al*, "Twenty Security Considerations for Cloud-Supported Internet of Things" (2015) PP(99) *IEEE Internet of Things Journal* 1.

* The authors are grateful to the members of the Microsoft Cloud Computing Research Centre and others for their valuable comments and to Microsoft for generous financial support. The views, however, are solely the authors'.

Ian **WALDEN***
BA (Nottingham University), MA (Virginia Polytechnic Institute), PhD (Nottingham Trent University);
Head (Institute of Computer and Communications Law), Centre for Commercial Law Studies, Queen Mary University of London.

INTRODUCTION

1 The world of the "Internet of Things" ("IoT") is just one manifestation of recent developments in information and communication technologies ("ICTs"), closely tied to others, including "cloud computing" and "big data". For purposes in this paper, the "Thing" in the IoT is "any physical entity capable of connectivity that directly interfaces the physical world, such as embedded devices, sensors and actuators".[2] This contrasts with other definitions that extend to virtual things, as well as physical, and can encompass the user.[3]

2 To examine IoT contracts, different research perspectives could be adopted:

(a) an empirical survey of the contracts used in the emerging IoT market;[4]

(b) a theoretical study on contract law issues in an IoT context, or

(c) focus on a case study, examining the complexity of IoT through the lens of a specific product.

---

2 Microsoft Cloud Computing Research Centre's definition. See also J Singh *et al*, "Twenty Security Considerations for Cloud-Supported Internet of Things" (2015) PP(99) *IEEE Internet of Things Journal* 1.

3 See respectively, International Telecommunication Union-Telecommunication Standardization Sector Recommendation Y.2060, *Overview of the Internet of Things* (June 2012) at para 3.2.3, which includes virtual things, and the Joint Technical Committee 1 of the International Organization for Standardization and the International Electrotechnical Commission, *Internet of Things (IoT): Preliminary Report 2014* at para 4.1, which infers that persons are included within the definition.

4 See S Bradshaw, C Millard & I Walden "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services" (2011) 19(3) *International Journal of Law and Information Technology* 187.

3 It is the last perspective that this paper adopts. The case study is the Nest Learning Thermostat, part of the Nest Labs business, which was purchased by Google in February 2014 for US$3.2bn.[5] Nest's main IoT products are a thermostat and smoke detector, although it recently also launched a camera.[6] Given the nature of the IoT environment, these products are inevitably designed to interconnect with an emerging array of other IoT products, known as the Nest ecosystem (or "Works with Nest") which includes cars, washing machines, lights, locks and communication devices.[7]

4 This paper focuses on the "legals" of Nest Labs[8] to provide a case study of IoT complexity.[9] The "legals" refers to the entire set of legal documents relevant for those who purchase the IoT device. The legal nature of each document varies and the set includes contractual documents, licences, notices, declarations, and reports. While acknowledging such variety, in this paper, reference will be made to them collectively as the "legals" and focus primarily on the contractual aspects.[10] After touching on some general contract law issues in relation to the IoT supply chain, the authors examine the rights and obligations represented in these legals and discuss the extent to which, collectively, they present a coherent and comprehensible private law framework. Thereafter they consider the extent to which certain statutory regimes may treat IoT contracts in terms of addressing two characteristic contractual concerns: liability attribution and unfair terms. With regard to the former, the inevitable complexity of IoT products and their ecosystems may result in calls for the adoption of clearer liability rules for consumers; as represented by product liability regimes. For the latter, considerations of fairness may arise not simply from

5 See https://investor.google.com/releases/2014/0113.html (accessed 8 December 2015). Google has since become a subsidiary of Alphabet Inc.

6 See https://nest.com/uk/camera/meet-nest-cam/ (accessed 8 December 2015).

7 *Eg*, Mercedes, Kēvo, Philips Hue, Ooma and Whirlpool. See https://nest.com/uk/works-with-nest/ (accessed 8 December 2015).

8 Also referred to as "Nest" or "the company" within this paper.

9 As regards the main clauses analysed, the authors have found many analogies with IoT contracts of businesses different from Nest, which could confirm the validity of the chosen use case.

10 Some of the non-contractual documentation, *eg*, the Intellectual Property ("IP") licences and the privacy policy, is incorporated into the contract.

the unilateral imposition of inappropriate obligations (issues of substance), but also the unworkable multiplicity and layering of so many legals (issues of form). Both product liability and unfair terms are regulated at the European Union ("EU") level, which will be the jurisdictional perspective considered.

IOT AND CONTRACT LAW

5 Not surprisingly, many of the considerations that are valid for IoT contracts are equally applicable to the majority of ICT contracts. Such contracts can be notoriously difficult to understand for at least four reasons.

(a) They are often characterised by opaque wording incorporating a plethora of technological terms.

(b) They have often been written with previous states of technological development in mind and thus are not wholly suitable for the new technology.

(c) It is not unusual that the European version of a contract reproduces verbatim the contractual wording of the original US source.

(d) The multi-layered structure of the market can make it challenging to identify all the applicable contracts and to interpret them.

6 There will be further discussion on the two final points when analysing the Nest use case, however it is sufficient to note that IoT contracts seem rarely to be drafted with EU law in mind. Moreover, the multi-layered structure of the market, which has been seen in cloud computing contracts, can make contracts difficult to understand not only for consumers, but also for enterprise customers, due to a lack of awareness of all the actors involved.

7 In these chains of contracts (which are not always expressly interlinked), it is frequently impossible to have a clear picture of the relevant legals, not only because it is hard to find them (let alone read them) but also because they claim to apply to just a part of a product, whilst they actually apply to it as a whole, or they

purport to apply to a single product, when they affect the whole cloud of things.[11]

8 IoT contracts also generate dependencies in two senses. On the one hand, in the constellation of IoT actors, where market power resides within the supply chain will vary considerably between different actors; from the retailer, to one of the software developers, the manufacturers of components, or the cloud providers. On the other hand, the end users are dependent in the sense of being locked-into a contract where there is no room for customisation (either at the moment of accepting the agreement, or afterwards when you "accept" every modification made to the contract just by continuing to use the product or an associated service) and where interoperability and portability are very limited.

9 Another contractual issue is partly very traditional in nature. In simplified terms, one might refer to it by saying "things that sell things".[12] To some extent, the phenomenon is not that different from the vending machine that distributes drinks and snacks.[13] However differences can be seen to lie in the fact that the IoT is becoming prevalent in every realm of our lives; the autonomy and decision-making ability of Things is of a qualitatively different nature, and Things can also sell themselves, in terms of proactively seeking out commercial opportunities, rather than being passive recipients of consumer interest.

10 In 1990, Ray Kurzweil asserted that machine intelligence would become the same as that of a human brain,[14] while a year

11 W K Hon, C Millard & J Singh, "Twenty Legal Considerations for the Clouds of Things", Microsoft Cloud Computing Research Centre discussion document (draft 1 October 2015) at 7, defines "Clouds of Things" as the "ecosystems in which there are communications between things and clouds, including M2M communications mediated by cloud".

12 W K Hon, C Millard & J Singh, "Twenty Legal Considerations for the Clouds of Things", Microsoft Cloud Computing Research Centre discussion document (draft 1 October 2015) at 13.

13 The authors do not only have in mind the Coke machine at Carnegie Mellon, which reportedly was the first IoT device. See M U Farooq *et al*, "A Review on Internet of Things (IoT)" (2015) 113(1) *International Journal of Computer Applications* 1.

14 R Kurzweil, *The Age of Intelligent Machines* (Cambridge: MIT Press, 1990).

later Mark Weiser commented that computing was becoming ubiquitous and that "the most profound technologies are those that disappear".[15] These ideas provide a backdrop to the reality of the IoT.[16] In the modern commercial environment, lawyers have observed (and sometimes caused) a sort of dehumanisation of the contract, with scant opportunities for authentic negotiation or customisation and everything shaped by the philosophy of adhesion: take it or leave it.[17] The adoption of "privacy by design" has shown that the new frontier of law enforcement is technology. One could also envisage "consent by design"[18] or "awareness by design", where, for example, it would be feasible to disable the feature enabling the user to confirm that "I have read" the applicable terms when he could not have read them, for example, an algorithm could measure the time spent on the page and scrolling through the text. Regarding awareness, it should be feasible to have an application comparing standard terms and alerting a user to any peculiar terms in the contract.

11 Speaking of things that sell themselves, there seems to be no apparent systemic danger from a contract law perspective, but "Brad" comes to mind. Brad is a toaster and a design experiment named "Best in Show" at the 2014 Interaction Awards. Brad

15 M Weiser, "The Computer for the 21st Century" (1991) 265(3) *Scientific American* 94.

16 An example of a nearly autonomous thing that bought things is Random Darknet Shopper, a bot that, for art's sake, purchased randomly counterfeit clothing (namely a pair of "Diesel" jeans and a "Louis Vuitton" handbag), a baseball cap with a hidden camera, a stash can, a pair of Nike trainers, a decoy letter, two hundred Chesterfield cigarettes, a set of fire-brigade issued master keys, and ten ecstasy tablets <http://www.theguardian.com/technology/2014/dec/05/software-bot-darknet-shopping-spree-random-shopper> (accessed 8 December 2015).

17 See E Mik, "The Unimportance of Being 'Electronic' or Popular Misconceptions About 'Internet Contracting'" (2011) 19(4) Int'l J L & Info Tech 324.

18 See D D Clark *et al*, "Tussle in Cyberspace: Defining Tomorrow's Internet" (2005) 13(3) *IEEE/ACM Transactions on Networking* 462 at 473 where they observe that:

> ... the laws of men and the so-called whims of bureaucrats are part of the fabric of society, like it or not. They are some of the building blocks of tussle, and must be accepted as such. We, as technical designers, should not try to deny the reality of the tussle, but instead recognize our power to shape it.

communicates with a social network of other toasters and wants to be used like the others: if one uses it less or does not even use it, Brad will try and draw the host's attention, until it eventually looks for a more suitable host.[19] In a time of consumerism and emancipation of the transaction from actual human needs, maybe so-called "smart"[20] things selling themselves is not such a dangerous idea. The traditional understanding of property is a static one, whilst the IoT device can constantly evolve over time (whether automatically upgraded or downgraded) and now it has an autonomous life and it may, eventually, decide not to be one's property anymore!

12 For the purposes of this paper, private ordering does not mean simple compliance with agreements nor the abuse of contracts in order to elude the law.[21] What is meant is that one form of response to a legislative framework that always lags behind technological developments, resulting in a regulatory lacunae, is the use of contracts.[22] As a consequence, looking at the contracts is an inevitable requirement for those who want to give an account of how law operates in the IoT field.

13 Lastly, it is worth noting the phenomenon of legal paternalism. As is common knowledge, the European legislator and, consequently, the legislators of the Member States, have shaped consumer law based on an assumption that the consumer is structurally the weaker party, incapable of fully understanding the

19 For more information, see the video at https://vimeo.com/41363473 or visit the website of Brad's designer Simone Rebaudengo <http://www.simonerebaudengo.com/#/addictedproducts/> (both accessed 8 December 2015).

20 Although the authors use the adjectives "smart" and "intelligent" in respect of IoT applications, reflecting common usage, the authors consider it confers undesirable anthropomorphic connotations; while in the not too distant future, if everything is smart, then nothing will be.

21 For a range of possible meanings of "private ordering", see *The Role of Intellectual Property Rights in Biotechnology Innovation* (D Castle ed) (Edward Elgar Publishing, 2009) at p 312, especially fnn 42–44.

22 This phenomenon is described as "legal hysteresis" by G Noto La Diega, "In Light of the Ends. Copyright Hysteresis and Private Copy Exception After the British Academy of Songwriters, Composers and Authors (BASCA) and Others v Secretary of State for Business, Innovation and Skills Case" (2015) 2 *Diritto Mercato Tecnologia* 1.

contract and with no realistic prospect of being able to negotiate its terms and conditions. This presumed asymmetry of bargaining power has resulted in laws and regulations that undermine the freedom of contract and has led to contractual remedies favourable to the consumer, to a point where it is possible to label the relevant political choice as paternalistic.[23] One of the very few scholars who has dealt with IoT contracts has focused on this aspect, arguing that "augmented reality calls into question leading justifications for distrusting consumer contracts — and thereby strengthens traditional understandings of freedom of contract as enforcing contracts as written".[24] The underlying reason being the existence of IoT, consumers have ubiquitous real-time access to information about the places, goods, people, firms, and contracts around them; therefore they can make informed and conscious choices on a peer-to-peer level. The authors of this paper do not think that the time has come to overturn the paternalistic approach to consumer contracts. Even with the tools available to consumers enabling them better to understand the reality; that reality has grown so much more complex with the IoT.

THE IOT SUPPLY CHAIN

14 This paper has cast light on the multi-layered structure of the IoT ecosystem and some of its consequences. Providing a full account of all the actors in the IoT supply chain is beyond the scope of this research. One reason for the difficulties, in achieving a shared definition of the IoT, is that it encompasses a plurality of heterogeneous domains whose greatest common factor has not been found. One may commonly talk about the actors in the healthcare, transportation, energy or manufacturing sector *etc*. Examining the Nest product ecosystem as a use case, which helps narrow down the relevant supply chain to the smart homes

23 A similar effect can also be seen in the US, *eg*, the doctrine of unconscionability. See J E Murray, "Unconscionability" (1969) 31 U Pitt L Rev 1; H J Stedronsky, "Unconscionability and Standardized Contracts" (1975) NYU Rev L & Soc Change 65.

24 S R Peppet, "Freedom of Contract in an Augmented Reality: The Case of Consumer Contracts" (2012) 59 UCLA L Rev 676, abstract.

environment (also known as "domotics"). It would simplify the analysis as distinctions are drawn between the hardware, software and service components of the device; although, these distinctions are not necessarily sustainable or desirable from the perspective of the customer.

15 In its Terms of Service ("ToS"), Nest informs that it "uses third party service providers to enable some aspects of the Services", but only provides an indicative list that includes Amazon Web Services ("AWS") for data storage, synchronization, communication, and mobile device notifications through mobile operating system vendors and mobile carriers.[25] Mention of the use of other service providers, such as Rackspace for redundancy,[26] is scattered among the other legals, although it is not possible to assess whether all such subcontractors are listed. These "third party service providers" also add to the legals that would require review if a comprehensive review was to be carried out.[27] The need to have transparency about subcontractors raises issues from both a legal and security perspective. From a contractual perspective, the customer is unable to identify the parties upon whom the service is dependent and therefore who may potentially be liable in the event of loss; while from a data protection perspective, knowledge of processors and subprocessors is seen as a prerequisite for a data controller to ensure compliance with its obligations.[28] In terms of security, an

25 Nest Terms of Service (17 June 2015 version) s 5(b).

26 See https://nest.com/uk/security/ (accessed 8 December 2015). While the Nest security policy references the Nest privacy statement, the latter simply pledges to use "best-in-class security tools", without further elaboration.

27 *Eg*, see http://www.rackspace.co.uk/legal (accessed 8 December 2015).

28 See Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (WP 169) (adopted on 16 February 2010) at pp 27–30, regarding the "plurality of processors" (see also *Opinion 5/2012 on Cloud Computing* (WP 196) (adopted on 1 July 2012). The draft "Data Protection Code of Conduct for Cloud Service Providers", prepared by the Cloud Industry Select Group established by the European Commission (see further https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct), requires service providers to "maintain an up-to-date list of any subcontractors engaged in the processing personal data under the Services agreement" (at s 5.4). However, note Article 29 Data Protection Working Party, Opinion *2/2015 on C-SIG Code of Conduct on Cloud Computing* (WP 232) (adopted on 22 September 2015).

absence of transparency would seem to substitute confidence with reliance on good faith and ignorance.[29]

16 To understand the complexity of the supply chain, it is useful to read the Nest Developer ToS,[30] which alerts the developer that the "Nest [application programming interfaces] and other Nest Developer Materials may allow [the Developer] to control Nest devices and software or gain access to certain information, which *may impact the safety of Nest customers and end users* of Nest's products and services" [emphasis added].[31] Customers may not expect that connecting their Nest products to third-party apps and devices can let third parties control their own product and affect their safety, therefore it is critical that this information is also stated clearly in the third party's ToS and privacy policy.

17 As people are at the centre of every IoT model, unlike the traditional machine-to-machine ("M2M") realm, it makes sense to start with them when describing the IoT supply chain, even though the end user does not generally have significant power in the value chain,[32] above all because they usually have reduced control over

29 It is perhaps noteworthy that following the latest update to the Nest legals, most references to "cloud" have been deleted. The security policy and website privacy policy still mention cloud, but the Privacy Statement, the Terms of Service, the Terms & Conditions of Sale, and the End User License Agreement are silent on the matter. The role of third party cloud providers is confirmed in information about Nest Aware only available in the Nest blog, which notes that advanced algorithms aimed at sending more accurate motion and audio alerts and motion sensing features (*ie*, face detection and depth sensing) require a lot of computing power, "much more than Nest Cam can deliver by itself. So we have to use powerful cloud servers to deliver this state of the art detection": (https://nest.com/support/article/What-do-I-get-with-Nest-Aware-for-Nest-Cam) (accessed 8 December 2015).

30 The Nest Terms of Service is available at https://developer.nest.com/documentation/cloud/tos (accessed 8 December 2015).

31 See Pt IX (Liability) of the Nest Terms of Service available at https://developer.nest.com/documentation/cloud/tos (accessed 8 December 2015).

32 Mark Fell, *Roadmap for the Emerging "Internet of Things"* Carré & Strauss (2014). <http://sweden.nlembassy.org/binaries/content/assets/postenweb/z/zweden/netherlands-embassy-in-stockholm/iot_roadmap_final_draft_0309145.pdf> (accessed 8 December 2015).

the data flows.[33] Clearly the central person when it comes to a smart thermostat is the end user, who is the main data subject (and sometimes data controller as well). However, two further distinctions of legal consequence need to be made. First, the end user may be the contracting customer or a third party, such as a family member. Second, the device itself may be owned by the customer or may be leased to the customer by the supplier (or provided as part of rented or leased premises). In the case of ownership, the distinction between the device and the associated services becomes critical, because the Nest ToS states that if the device owner does not agree with the terms "you should disconnect your products from your account [...] and cease accessing or using the services".[34] This raises an issue concerning the status of a "disconnected IoT device". Where the customer does not own the device but is simply leasing it, then the issue is relatively straightforward, since the contract allows for the customer to simply return the device to the supplier. However, where title in the device is transferred to the purchaser, as in the case of Nest,[35] then the issues can be more complex. In terms of UK contract law, statute implies a term into the contract that the purchasers of goods will "enjoy quiet possession",[36] which term would be potentially breached if when the Nest device were disconnected as it loses most of its functionality.[37] In addition, from a regulatory perspective, a contractual rule that restricts or prohibits use or reconnection of an IoT device, could fall foul of competition rules. In the broadcasting sector, for example, *ex ante* intervention exists in respect of access control systems in television set-top boxes to ensure certain public interest objectives are met, specifically access

33 The situation might change in a personal cloud context, where people can have more control over their data.

34 See preamble of the Nest Developer Terms of Service available at https://developer.nest.com/documentation/cloud/tos (accessed 8 December 2015).

35 *Eg*, Nest Terms & Conditions of Sale s 7: "Title for Products purchased from the Store passes to the purchaser at the time of delivery by Nest to the freight carrier".

36 *Eg*, the UK Sale of Goods Act 1979 (c 54) s 12(2)(b).

37 See *Rubicon Computer Systems Ltd v United Paints Ltd* (2000) 2 TCLR 453.

by competitors and user access to certain content services.[38] One could envisage for certain IoT products considered integral to our daily lives that regulatory intervention may be deemed necessary, in the form of a "must provide" obligation, to safeguard certain public interests in the event of IoT disconnection.

18 Any IoT supply chain will have a range of actors who are dependent on the smart hardware device. In terms of the manufacturer of the "thing", most IoT products will be compound, with different manufacturers responsible for different aspects of any "thing of things", such as a smartphone. Even when there is simply one thing, during the process of manufacturing a lot of different people will be involved, contributing components and facilitating the production process.

19 As with many large companies, Nest also has established a network of resellers,[39] retailers, wholesale distributors,[40] and installers. Resellers have to enter into the "Nest Pro" agreement, the terms of which are not publicly available. As regards installers, even though Nest "maintains a list of recommended installers of the Products on its website", it declares that it is not "responsible for any conduct of or liability associated with these installers".[41]

38 Ofcom statement, *Review of Sky's Access Control Services Regulation* (17 March 2015).

39 For instance, in the heating, ventilation and air conditioning sector or electricity sector.

40 As far as the authors are aware, the only Nest UK Wholesale Distribution Partner is WF Senate, following an agreement between the latter's parent company Rexel and Nest Labs <http://www.voltimum.co.uk/articles/wf-senate-distribute-google-owned-nest-self-learning-domestic-energy-saving-and-safety> (accessed 8 December 2015); see also the WF Senate contractual quagmire <http://www.wfsenate.co.uk/d/22/Terms_%26_Conditions%2C_Privacy_Policy_%26_Legal.html> (accessed 8 December 2015). In the US there is for instance eDist, a New Jersey company, see http://security.edist.com/index.jsp?path=nest-distributor (accessed 8 December 2015).

41 The Terms & Conditions of Sale are available at https://nest.com/uk/legal/sales-terms/ (accessed 8 December 2015). See also the Installation Terms of Service available at https://nest.com/uk/legal/installation/ (accessed 8 December 2015).

20 Unsurprisingly, Nest as the central actor responsible for the device as well as the services and software, is in reality a shorthand for Nest Labs Inc and its various affiliates and subsidiaries, such as Nest Labs (Europe) Ltd. When it comes to services, the supply chain becomes even more complex. This paper has already referred to the cloud providers (Amazon and Rackspace), but there are also the analytics tools provided by Google Analytics (a "third-party" despite being part of the same group of companies), the credit card processing service provider CyberSource,[42] and advertising services provided "by third-party ad partners, such as Google Display Network and AdRoll".[43] Another service is "Safety Rewards",[44] even though it is not mentioned in any of the legals, in which Nest is

42 Cybersource, a California e-commerce credit card payment system management subsidiary of Visa, "will collect and store full payment card information from you, even as a guest user, when an order is placed until when it ships. If you create a Nest account and elect to have payment card information saved, CyberSource will store your payment information" <https://nest.com/legal/privacy-policy-for-nest-web-sites/> (accessed 8 December 2015). There is always the possibility to use e-commerce platforms, for instance one may buy the product via eBay and therefore it may be necessary to take into account also PayPal's privacy policy and other relevant legals.

43 The qualifier "such as" suggests other unnamed partners and third parties offering advertising services.

44 Nest will let the insurer know that Nest Protect is installed and working. In exchange, the insurer will take up to 5% off the insurance premiums. Nest promises that "Your insurer will never know if the alarm went off because you burned the popcorn"; system also tests itself to make sure the batteries have power, the sensors are working and that it is connected to Wi-Fi. Nest will then provide a monthly basic summarised information about your Nest Protect to your insurance company and that summary "includes" the three pieces of information (battery, sensor and connection), which does not mean that other information is excluded, such as your postal code and the names of the rooms where you have your Nest Protects installed. While Nest promises not to share "any smoke or carbon monoxide alarms that may have occurred in your home", if the batteries rapidly run low, it is not hard to infer that an alarm occurred. One can decide not to grant permission to share the data requested in connection with the Safety Rewards service, but, again, "you won't be able to participate in Safety Rewards". The service appears in the US website, but the UK version of the Website Privacy Policy mentions insurance companies among the partners <https://nest.com/support/article/When-I-enroll-in-Safety-Rewards-what-kind-of-data-is-shared-with-my-insurance-company> (accessed 8 December 2015).

partnered with leading insurance companies.[45] Similarly, Nest collaborates with "energy partners", for example npower for the UK, whose services are based on machine learning technologies (so-called "Auto-Tune"), from which peculiar liability issues may arise.[46] Even though the US legals mention them and the UK ones do not, there are "Customer Agreements for Rush Hour"[47] and "Customer Agreements for Rebates"[48] with Nest energy partners that will share data with Nest, which in return, "may also collect your energy usage and pricing data from your energy provider".[49] These energy partners are apparently "helping to subsidize all the processing power required to implement Auto-Tune, which needs a

45 The information is available at https://nest.com/insurance-partners/ (accessed 8 December 2015). Along with what has been stated in n 44 above, it is not clear, for instance, what would happen if the house catches fire and Nest sends the insurance company information that the product user had been alerted when it had not alerted product user. (Nest does not guarantee the accuracy of the shared information.)

46 See https://nest.com/energy-partners/ (accessed 8 December 2015). The services offered are Rush Hour Rewards and Seasonal Savings; the technology involved is Auto-Tune. Among the main legal issues relevant to machine learning and artificial intelligence are liability (*eg*, is the owner of a Thing liable for its autonomous actions?) and contracts (*eg*, can a contract be concluded autonomously by a Thing?).

47 The "Customer Agreements for Rush Hour" is available at https://nest.com/legal/customer-agreements-for-rush-hour-rewards/ (accessed 8 December 2015).

48 See https://nest.com/legal/customer-agreements-for-rebates/ (accessed 8 December 2015). Currently this "Rebates" service is provided only by Xcel Energy. It is not regulated by Nest legals, but by "Xcel Energy's Rebate Terms & Conditions", even though "Nest is providing this Rebate Redemption Tool in accordance with, and your use of the Rebate Redemption Tool is subject to, the Nest Terms of Service, privacy policies and other policies on Nest's website." In any event, unlike the insurance case, here Nest states that it will "share the information provided by you in your application (including, but not limited to, your name, email address, service address, Xcel Energy account number, Nest Learning Thermostat serial number, date application completed". Furthermore, on Xcel Energy's website, the general Terms of Service are readily available, but not the "Xcel Energy's Rebate Terms & Conditions" <http://www.xcelenergy.com/staticfiles/xe/Admin/CLI_1793261_10_FINAL_CLEAN_Xcel%20Energy_OAM_My%20Account_Terms%20and%20Conditions.pdf> (accessed 8 December 2015).

49 The Nest Privacy Statement states: "With your consent, MyEnergy may access different types of information from your utility. For example, MyEnergy may download, analyze, and store your utility bill statements."

huge amount of memory, storage and processing power, all maintained in the cloud".[50]

21 To complete the supply chain picture, one should also mention the website developer and webmaster, the app store,[51] the embedded software developer(s), other software providers, the facilitators of communication between things, the rights-holders, the e-commerce platforms,[52] and the network operators.

THE NEST USE CASE

22 A consumer interested in a thermostat does not expect to face a legal mountain![53] However, if a UK-based customer wants to have a comprehensive picture of the rights, obligations and

50 See Nest website https://nest.com/support/article/What-is-Auto-Tune (accessed 8 December 2015).

51 The Nest app is available on the Apple's iTunes and Google Play, as well as the web. See https://nest.com/blog/2015/06/17/one-home-one-app/ (accessed 8 December 2015).

52 Nest products can be bought from e-commerce platforms, such as eBay, Amazon and Alibaba. Under the Terms & Conditions of Sale, it notes that that the "Store" is accessible worldwide, but states that if you use Nest products and services "outside the United Kingdom, Ireland, France, Belgium or the Netherlands (each, a "Target Country"), as applicable, you do so on your own initiative and you are solely responsible for complying with applicable local laws in your country. You understand and accept that the Store and our Products and Subscription Services are not designed for use in a non-Target Country and some or all of the features of the Store, Products and Subscription Services may not work or be appropriate for use in such a country. To the extent permissible by law, Nest accepts no responsibility or liability for any damage or loss caused by your access or use of the Store, Products and Subscription Services in a non-Target Country" <https://nest.com/uk/legal/sales-terms/> (accessed 8 December 2015). One can question if Nest can limit its liability to products sold in "Target" countries when they acknowledge that their products are purchased worldwide: the company admits that their products are installed in over 120 countries <https://nest.com/blog/2014/09/06/nest-is-coming-to-the-EU/> (accessed 8 December 2015).

53 There is apparently no separate contract for businesses, but the Nest Sales Terms state that "The Store is for retail sales to private consumers only. Please contact orders@nestlabs.com if you wish to purchase wholesale supplies." Presumably separate terms are used for such purchases, but they are not publicly available.

responsibilities of the various parties in the supply chain, he has to read at least 13 legal items.[54] The main documents are:

(a) the Terms of Service ("ToS"), with "Nest Labs, Inc and its subsidiaries and affiliates (collectively, 'Nest')", covering sites, web apps, mobile apps, and "subscription services";[55]

(b) the End User Licence Agreement ("EULA"), with "Nest Labs, Inc", including embedded software;[56]

(c) the Terms & Conditions of Sale ("T&Cs"), with "Nest Labs (Europe) Ltd", covering hardware and certain aspects of the services;

(d) the Limited Warranty ("Limited Warranty"), with "Nest Labs (Europe) Ltd";

(e) the Privacy Statement, regarding Nest Products and Services, for information relating to the operation of Nest products and services ("Privacy Statement");[57]

54 Since Google acquired Nest, it seems likely that Google's legals will eventually come to influence the Nest legals.

55 It is not entirely clear what these subscription services are, which is surprising given that their inclusion is one of the stated reasons for the last update of Nest legals. The Terms of Service says nothing more than that the subscription services include "services that can be accessed using the Web Apps and Mobile Apps". In addition, the Privacy Statement refers to the Terms of Service for the definition (which is not provided), while the Terms of Service refers to the Terms of Sale (either the Nest's Terms & Conditions or the service provider's terms) for the regulation of the fees ("Certain Services may be provided for a fee. You shall pay all applicable fees in connection with the Services selected by you in accordance with the Terms of Sale.").

56 The End User Licence Agreement is available at https://nest.com/uk/legal/eula/ (accessed 8 December 2015).

57 One can find the Privacy Statement at https://nest.com/uk/legal/privacy-statement-for-nest-products-and-services/ (accessed 8 December 2015). Previous policies are available at https://nest.com/uk/legal/privacy-statement/archive/ whilst the old Dropcam Privacy Policy is at https://www.dropcam.com/privacy/dropcam (both accessed 8 December 2015). If the Privacy Statement is accessed from the Nest app, the US version appears.

(f) the Website Privacy Policy ("WPP"), for information collected through the websites, including the online store;[58] and

(g) the Security Policy.[59]

23 It may also be important to read also the Open-source Compliance,[60] the Intellectual Property and Other Notices,[61] the Community Forum Agreement,[62] the Transparency Report,[63] the EU Declarations,[64] the Installation Terms and Conditions[65] and the Nest Developer Terms of Service.

---

58 The scope of these privacy policies is unclear. While the Privacy Statement covers information collected through Nest products, which include web apps, mobile apps, and subscription services; the Website Privacy Policy provides that Nest uses permanent cookies in order to understand "how you use our website *and products and services*, to diagnose and fix technology problems, and otherwise enhance our Site, products, and services".

59 Vulnerabilities that users discover should be reported to Google's Vulnerability Reward Program or security@nest.com.

60 Some 30 open source code modules for the thermostat are listed with associated compliance notices; available at https://nest.com/uk/legal/compliance/ (accessed 8 December 2015). These notices are generally required of those that wish to use open source modules, under the module licences.

61 With regard to patents, trademarks, the Trademark Usage Policy and the Policy Regarding Unsolicited Idea Submissions, see https://nest.com/uk/legal/ip-and-other-notices/ (accessed 8 December 2015).

62 The Community Forum Agreement is available at https://nest.com/uk/legal/community-forum-agreement/ (accessed 8 December 2015).

63 The Transparency Report was last updated on 17 June 2015 and deals with requests received for law enforcement purposes <https://nest.com/uk/legal/transparency-report/> (accessed 8 December 2015). It states that if a US government agency presents Nest with a warrant to investigate a crime they think had been captured by Nest products, the company would not simply hand over user data. Nest would first analyse the request to be sure that the warrant was not overly broad and then ensure the information the agency requested was within the scope of the warrant.

64 There are various declarations of conformity for the Nest Thermostat at https://nest.com/uk/legal/eu-declarations/ (accessed 8 December 2015). This means that the product is stated to be in conformity with:

(a) Directive 2006/95/EC of the European Parliament and of the Council of 12 December 2006 on the harmonisation of the laws of Member States relating to electrical equipment designed for use within certain voltage limits ("Low Voltage Directive"),

(b) Directive 2004/108/EC of the European Parliament and of the Council of 15 December 2004 on the approximation of the laws of the Member

(*continued on the next page*)

24 To these documents one can add the legals of the partners, affiliates, *etc*, plus those of the actors of interoperable products (both the "Works with Nest" realm as well as interoperable apps),[66] and some Nest documents that are not published, such as the Nest Pro agreement and the terms of the free trials of subscription services.[67]

25 Unsurprisingly, the list goes on. In fact, the essence of the grand vision of the IoT is the idea of a network of things (and people). In the Nest use case, this is epitomised by the section

---

States relating to electromagnetic compatibility and repealing Directive 89/336/EEC Text with EEA relevance ("Electromagnetic Compatibility Directive"),

(c) Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity ("Telecommunications Terminal Equipment Directive"),

(d) Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products ("Ecodesign Requirements for Energy Related Products Directive"), and

(e) Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment ("Hazardous Substances in Electrical and Electronic Equipment Directive").

As a consequence, the product carries the CE mark.

65 *Eg*, the Nest Installation Terms and Conditions states: "These terms and conditions are in addition to any terms and conditions of the Installer."

66 Interoperability is a major issue in the Internet of Things. Reportedly, Nest products are not compatible with Apple HomeKit and cannot be controlled via Apple's voice controller Siri, although a Nest application is available for the Apple Watch.

67 An end user may not expect that they have to take into consideration not only Nest's third parties, but also the third parties' third parties. See the Developer Terms of Service: "You [the developer] will not permit use of any Customer Data or disclose any Customer Data to any third party except to those third parties who provide services on your behalf in connection with your Client and who are obligated to maintain Customer Data only for your own benefit and under reasonable confidentiality terms". One may question why this provision is limited to the developer, whereas Nest's parent provides that "We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to *strict contractual confidentiality obligations* and may be disciplined or terminated if they fail to meet these obligations." [emphasis added]

"Works with Nest",[68] which is – in the ambitious words of the company – "about making your house a more thoughtful and conscious home". Nest suggests a number of devices and apps that interact with the thermostat, the smoke alarm and the camera, thus ensuring "personalized comfort, safety and energy savings". So, for example, one can simply speak the command: "Ok. Google, set the temperature to 75 degrees" and the thermostat will do as commanded. In addition, with Google Now, the user can be on their way home and the thermostat will start heating or cooling before they get there. The user does not even need to speak if he owns a Mercedes-Benz as the automatic car adapter will tell the thermostat to start getting the home comfortable before he arrives. The new version of the thermostat can even control the boiler.[69] The list of useful connections is continually growing, encompassing smart sprinklers, webcams, locks, sleep systems and lights. All these apps, devices and appliances send data to Nest, as well as receiving data from Nest on terms that are not easy to understand, as one has to cross-refer to the Nest Privacy Statement, the Nest WPP and third-party privacy policies.[70] If you add to Nest legals those of the connected devices, apps and appliances, the result is that for what appears to be a single product, a thousand contracts may apply!

The concept of product

26 One of the main conclusions of this research is that a new legal conception of a "product" may be required in the context of

68 More information is available on "Works with Nest" at https://nest.com/works-with-nest/ (accessed 8 December 2015).

69 On 17 November 2015, Nest has announced its third generation thermostat: http://www.wired.co.uk/news/archive/2015-11/17/nest-third-generation-boiler (accessed 8 December 2015).

70 To find out more about the data shared within the context of "Works with Nest" see https://nest.com/support/article/What-kinds-of-data-is-shared-with-Works-with-Nest-developers (accessed 8 December 2015). Please note that even though "United Kingdom" is selected as the relevant country, the website redirects you to the US version. Along with the Works with Nest legals, the customer has to double-check also those of the connected devices, apps and appliances (see, *eg*, Daimler privacy policy at http://drive-kit-plus.com/en/privacy/ (accessed 8 December 2015)).

the IoT. Even though the ToS professedly apply only to the Nest-related services and not to the Nest hardware,[71] what is left when one is obliged to disconnect the product from the account and to cease access and usage of the service, because one disagrees with or cannot accept the provisions of the ToS?[72] The end customer's ability to use the hardware's functions would be profoundly affected.

27 The same thing happens to the concept of "product" under the T&Cs. Originally, they referred only to the Nest product as hardware, but now they openly cover both the product and any subscription services,[73] notwithstanding the fact that the ToS "constitute the entire agreement between you and Nest regarding the use of the Services", which include also the subscription services.[74] This is confirmed in the Privacy Statement, where it

71 Under these Terms of Service, Nest provides (1) a Nest user account website that may be accessed at home.nest.com or www.dropcam.com (each a "Site"), (2) services accessible through the Sites ("Web Apps"), (3) software that may be downloaded to your smartphone or tablet to access services ("Mobile Apps"), and (4) subscription services, including services that can be accessed using the Web Apps and Mobile Apps ("Subscription Services"), and (5) a MyEnergy user account website that may be accessed at www.myenergy.com ("MyEnergy Service"), all for use in conjunction with Nest hardware products ("Products") and in other ways that Nest provides.

72 A similar clause can be found verbatim in the Legal Terms of Azert LLC Smart(er) Socket at http://www.smartersocket.com/legal-terms/ (accessed 17 September 2015). This US smart socket supports in-door navigation, proximity based messaging, power consumption monitors and presence sensors.

73 The original wording was "These Terms constitute the entire agreement between you and Nest regarding the use of the Services" (and a similarly worded section can still be found, for instance, in the Wellntel Terms of Service Agreement). After the last update, the situation became more complex, given that hardware products and subscription services are regulated "by these Terms & Conditions of Sale ("Terms & Conditions") and any additional terms we provide, *including but not limited to* our Terms of Service and the terms of the Limited Warranty included in-box with a Product". Hence, a single aspect of a product is covered by an unpredictable number of legals (for example, the subscription services is regulated at least by the Privacy Statement, the Terms of Service and the Terms & Conditions).

74 The services covered by the Terms of Service are the websites, web apps, mobile apps, subscription services and MyEnergy service, whereas the services under the Terms & Conditions seem to refer to the subscription services only, thus creating a partial, albeit confusing, overlap. MyEnergy is

(*continued on the next page*)

states: "Nest Products also include our Web Apps, Mobile Apps, and Subscription Services".[75] One question that might come to mind would be were the websites not already covered by the WPP?

28 It is then useful to look at the EULA. If the customer does not agree with its provisions, they simply "should cease accessing or using the product software" (the same happens if they do not consent to software updates). Not only is the customer not able to modify the agreement, but the company has the right to modify it "without providing any additional notice or receiving any additional consent".[76] If you do not want such updates, "your remedy is to stop using the Product".[77] The situation is slightly better for the T&Cs, since amendments should not affect the customer's position, given that "Every time you order Products from Nest, the Terms & Conditions in force at that time will apply between you and Nest." This rule, however, does not apply to the subscription services, in which case Nest will notify changes affecting the subscription.[78]

---

the only service enjoying a specifically dedicated section within the Privacy Statement.

75 The most recent update to Nest legals has gone in the direction of a further blurring of the lines between hardware, software and services. Specifically, the substitution of the term "service" with the term "product" in the Privacy Statement.

76 This clause is quite common in Internet of Things and cloud contracts; *eg*, the respective Terms of Service for both the Leeo Inc, Smart Alert™ Nightlight at https://www.leeo.com/legal/terms-service/ (accessed 8 December 2015) and Snupi Technologies Inc, WallyHome™ at http://www.wallyhome.com/legal/ (accessed 8 December 2015).

77 See also the End User Licence Agreement of Orion <http://www.orionlabs.co/eula-android/> (accessed 8 December 2015).

78 This is an improvement of the last update to the Terms & Conditions and leaves out the changes of prices, for which Nest will provide notification "via (at its option) email to the primary email associated with your Nest account, hard copy, or posting of such notice on the Nest website". Under the previous regime, continued use of the services indicated acknowledgement of the changes and the burden of checking the site to see if any modification was posted was on the customer. In the unlikely event that a user checked the legals over time, if the changes were not highlighted and previous versions were not stored and made easily accessible, it would be very difficult to understand what had changed.

29 From the above, it would seem that this IoT product has become an inseparable mixture of hardware, software and service. Despite attempts through the legals to distinguish the different elements, this has become untenable. This convergence has, arguably, implications for the applicability of consumer protection laws, discussed further below.

Security, privacy and data protection

30 Data security is already an increasingly "hot" topic for the Internet, but it becomes utterly critical in an IoT context for at least two reasons.[79] First, IoT is not only about sensing, but also about actuating; this impact on the physical world may result in greater risks for personal safety (for example, hacking a smart vehicle can cause a car accident).[80] Second, with the IoT the Internet is everywhere (or "everyware"),[81] in every nook and cranny of private spaces (which is, homes and offices) and also constantly with you (wearables and ingestibles *etc*). Potentially (but not necessarily), this means the generation of much more data (big data) and more intimate data. Thanks to the dynamic flow of information within

79 J Singh *et al*, "Twenty Security Considerations for Cloud-Supported Internet of Things" (2015) PP(99) *IEEE Internet of Things Journal* 1, where it is explained that "Work in IoT tends towards the subsystem, often focusing on particular technical concerns or application domains, before offloading data to the cloud. As such, there has been little regard given to the security, privacy and personal safety risks that arise beyond these subsystems; that is, from the wide-scale, cross-platform openness that cloud services bring to IoT."

80 These scenarios are not entirely new, see for example, J P Zammit and M A Savio, "Tort Liability For High Risk Computer Software" (1987) 23 PLI/PAT 373 at 375, for a case in which a bug in a computerised therapeutic radiation machine caused it to administer incorrect dosages and, as a consequence, two people were killed and several others were seriously injured. Let us imagine, however, what can happen if entire hospitals are affected. See also C S Massingale and A F Borthick, "Risk Allocation for Injury due to Defective Medical Software" (1988) 2 J Prod Liab 181.

81 This is one of the many names given to the Internet of Things. See A Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing* (Berkeley: New Riders, 2006).

the IoT system and potentially between systems,[82] it is also easier to infer personal data even from raw data, while benign streams of personal data can become sensitive once combined.[83] Let alone the latest developments in cross-device tracking.[84] It is therefore not comforting to read the EULA and discover that the company "makes no warranty that the product software will be uninterrupted, free of viruses or other harmful code, timely, secure, or error-free"; particularly if that fault leaves you in the cold![85] Once again, the distinction between hardware and software in an IoT context dissolves; software insecurity may mean physical insecurity.

31 Further security issues may arise from two other characteristics of the IoT. First, the Thing may be capable of being controlled in a number of ways that could conflict with each other, leading to unexpected actions and potential harm. This issue will be exacerbated where there is a multitude of users (for example, family members) who have different preferences. For instance, while Apple's Siri cannot control the Nest thermostat, it can control the Philips Hue lights that in turn can control the Nest thermostat, which can be controlled manually, as well as via the

82 The current lack of interoperability, the heterogeneity of standards and protocols and the prevalence of proprietary models render communications between the "silos" difficult. See P Desai, A Sheth & P Anantharam, "Semantic Gateway as a Service Architecture for IoT Interoperability" in (2015) *IEEE International Conference on Mobile Services* (O Altintas & Jia Zhang eds) (IEEE, 2015) at p 313.

83 This leads to the issues of recombination, repurposing and reconfiguration, which merit further research. As to Nest legals, see for instance the section of the Privacy Statement whereby "MyEnergy data can be combined with other information in your Nest account and can help us to better understand things like your energy usage" or, as regards the exchanges of data and requests for control by third parties, "Nest requires your explicit consent before sharing information in these circumstances. We may also obtain information from other sources and combine that with the information in your Nest account."

84 On the use of high-frequency sounds to covertly track across a range of devices, see C Calabrese *et al*, "Comments for November 2015 Workshop on Cross-Device Tracking", Letter of the Center for Democracy & Technology to the Federal Trade Commission (16 October 2015) at https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf (accessed 8 December 2015).

85 J Wakefield, "Nest thermostat bug leaves users cold" *BBC* (14 January 2016) at http://www.bbc.co.uk/news/technology-35311447 (accessed 8 December 2015).

Nest app, the website or third party-apps and devices, such as "Kontrol" an app designed for communication between the Apple Watch and Nest products. Second, IoT products are being equipped with a greater range of sensors, although the information they gather may not be consistent which can have consequences for actuation. For instance, the Nest smoke alarms feature "Wave", whereby one could switch the alarm off by waving the hands. As of 3 April 2014, the feature has been disabled, because "movements near Nest Protect that are not intended as a wave can be misinterpreted by the Nest Wave algorithm. If this occurs during a fire, this could delay the alarm going off".[86]

32 One of the main problems stemming from the labyrinth of IoT contracts is that it is difficult to understand the protection actually granted to a user's personal data. It is not always possible to read and interpret the scattered provisions; while, when gathered together, they do not provide a uniform level of protection. Moreover, there are some differences between what Nest declares publicly (thus creating a legitimate expectation in the minds of customers) and what the legals state. For example, with respect to the microphone on 2nd generation Nest Protect devices, while the website reassures visitors that the microphone is used exclusively for the sound check and that no data are sent to Nest servers, the Privacy Statement only states that "Nest Protect emits sound samples during Safety Checkup or Sound Check that the microphone will capture to verify that the speaker and horn are functioning."[87]

86 Nest website https://nest.com/support/article/Nest-Protect-Safety (accessed 8 December 2015).

87 Nest website https://nest.com/uk/support/article/Learn-more-about-Sound-Check and https://nest.com/uk/support/article/Learn-more-about-Nest-Protect-s-microphone (both accessed 8 December 2015). The former statement may be designed to address public concern over the Samsung Smart TV "listening in" on family conversations: see http://www.bbc.co.uk/news/technology-31296188 (accessed 8 December 2015).

33 The Nest Privacy Statement notes that "once this information is shared with the particular Third-Party Product and Service, its use will be governed by the *third party's privacy policy and not by Nest's privacy documentation*".[88] Even though one would naturally be led to think that "third party" refers to the realm of "Works with Nest", there is a broader and indistinct universe that needs to be taken into consideration. In fact, one feature of the last update to the Nest legals is a provision whereby the company states that it will share information with and receive information from unspecified "third parties outside of the Works with Nest program",[89] and that some of this information may be associated or stored with the user's Nest account. Information will be pulled without the customer's awareness, whereas "Nest may *also* share information with your permission" [emphasis added].

34 Furthermore, in the IoT it is difficult to identify who the controller is and who the processor is for data protection purposes.[90] The Nest ToS states that "You agree that you (and not Nest) are responsible for ensuring that you comply with any applicable laws when you use the Products and Services, including, but not limited to, (i) any laws relating to the recording or sharing of video or audio content that includes third parties, or (ii) any laws requiring notice to or consent of third parties with respect to

88 The Privacy Statement specifies that the determining point whether the application of either the Nest policy or the third party's one is the time when the data is in the third party's "possession". Possession of data is not always easy to assess, especially in the Internet of Things. Furthermore, data could be replicated, and be in the possession of both the third party and Nest at the same time. If there is a problem with Nest's service affecting data stored with it, can Nest escape all liability just because the same data has previously been sent to a third party?

89 Nest provides the example of rewards programs provided by its partners, but if one reads carefully, they discover that "We may also obtain information from *other sources* and combine that with the information in your Nest account."

90 W K Hon, C Millard & J Singh, "Twenty Legal Considerations for the Clouds of Things", Microsoft Cloud Computing Research Centre discussion document (draft 1 October 2015).

your use of Dropcam/Nest Cam."[91] Such a provision implies that the customer is considered by default as the controller, which contrasts with the reality as much of the data processing occurs in the IoT.

35 Data security can be hindered by the peculiar nature of the product in an IoT environment. If the thermostat was merely a simple piece of hardware, it could be defective at the moment of the purchase or stop working at some point, but there would be no security problem. The fact that IoT products are a mixture of hardware, software and services mean that weak or reduced security of any one of these elements will probably impact on the others. So, for example, Nest declares not to have any "responsibility to provide maintenance or support services with respect to the Product Software".[92] From this it follows, that if there is no more maintenance or support, the Thing as a whole can become open to external integrity attacks.

36 The Privacy Statement does not say much about security. It states that some information is processed and stored directly on the Nest device (and other information on cloud servers such as Amazon's S3 cloud service) and that "All personal information is *encrypted as it is transmitted* to Nest and cannot easily be accessed" [emphasis added].[93] This begs the question of how data "at rest" are protected. Moreover, Nest says it complies with the US-EU Safe

91 This provision has to be read jointly with the section of the Privacy Statement whereby "Data protection and privacy laws in your country may impose certain responsibilities on you and your use of Nest Cam. You (not Nest) are responsible for ensuring that you comply with any applicable laws when you use Nest Cam. For example, you may need to display a notice that alerts visitors to your home that you are using Nest Cam. Note in particular that recording and sharing clips that involve other people may affect their privacy and data protection rights." See *František Ryneš v Úřad pro ochranu osobních údajů* C-212/13 (11 December 2014).

92 Nest End User Licence Agreement.

93 Under the previous version of the Privacy Statement, all information was professedly encrypted.

Harbor Framework and the US-Swiss Safe Harbor Framework, as set forth by the US Department of Commerce.[94]

37 The WPP is more detailed and strikes a balance between security and Nest's commercial interests, with the balance appearing to incline in favour of the latter. In fact, the physical, administrative, and technological methods to transmit the data are those considered "commercially reasonable".[95] However, in the ToS, Nest admits that it "cannot guarantee that unauthorized third parties will never be able to defeat our security measures or use your personal information for improper purposes".[96]

38 Another point that is often stressed, relates to the physical location of data.[97] It is useful to underline that by signing the Nest contract, the customer acknowledges that his personal data will be transferred to the US and the fact itself of providing the data is considered equivalent to the expression of an informed consent. This would be another example of the complexities of interpreting all the legals. Why does the WPP inform and obtain consent from the user about the transfer, exempting Nest from its obligation not to transfer data to a country without an "adequate level of protection"; while the Privacy Statement stresses adherence to the relevant Safe Harbor Privacy Principles, which is intended to

94 The relevant documents are available at http://www.export.gov/safeharbor/ (accessed 8 December 2015). Note, however, the decision of the European Court of Justice in *Maximillian Schrems v Data Protection Commissioner* C-362/14 (6 October 2015), which declared the Commission decision on Safe Harbor (Decision 2000/520) invalid.

95 These measures include HTTPS, TLS/SSL protocol, AES and RSA data encryption.

96 The exact wording of this clause can be found in a vast variety of contracts; googling the cited passage would generate at least 140,000 results.

97 See C Millard, "Forced Localization of Cloud Services: Is Privacy the Real Driver?" (2015) 2(2) *IEEE Cloud Computing* 10 (March–April 2015) and W K Hon *et al*, "Policy, Legal and Regulatory Implications of a Europe-Only Cloud", Queen Mary University of London School of Law: Legal Research Paper 191/2015 (21 November 2014). For the technical considerations underpinning regional clouds, see J Singh *et al* "Regional Clouds: Technical Considerations" (November 2014) at http://www.mccrc.eu/Pages/Events.aspx (accessed 8 December 2015).

establish "adequacy"?[98] To a certain extent, this represents a common legal response to a regulatory environment, providing a range of possible justifications or defences to reduce the risk of non-compliance. However, the compound nature of IoT legals is likely to exacerbate this issue and, from a data subject's perspective, a multiplicity of conflicting messages would seem to undermine and confound any expectation they may have about the basis for the processing and the protections offered.

39 It has recently been forecasted that "every IoT-enabled device, whether an iron, vacuum, refrigerator, thermostat or light bulb, will come with terms of service that grant manufacturers access to all your data".[99] This may sound like mere conjecture, but it is not pure science fiction. Nest inform users in its Privacy Statement that the product "regularly sends the data [...] to Nest". However, which data are stored "on-board" the device and which on Amazon's S3 cloud platform? The legals inform of the storage itself but not the location,[100] although mentioned in the security policy what data is held on the device itself.[101] The granularity, quality and quantity of personal data stored will depend on the type of product; for instance, the Nest Cam, especially if one subscribes to Aware, enables the company to "capture, process and retain video and

98 The former reflects Art 26(1)(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Directive 95/46/EC"), while the latter falls under Art 25(6).

99 M Goodman, "Hacked dog, a car that snoops on you and a fridge full of adverts: the perils of the internet of things" *The Guardian* (11 March 2015).

100 Nest Website Privacy Policy.

101 The frequently asked questions about Nest security page states "What information is stored on Nest devices? Your Nest devices collect setup information like your ZIP or postal code, your Wi-Fi network information, environmental data from sensors like temperature and humidity, temperature adjustments, usage and occupancy information, and more" <https://nest.com/uk/security/> (accessed 8 December 2015). For a "full list" of information collected, it refers to https://nest.com/uk/legal/privacy-statement-for-nest-products-and-services/#what-does-nest-collect (accessed 8 December 2015).

audio data recordings from your device for the duration of your recording subscription period".[102]

40 Basically everything can be sent to Nest (and Amazon). It is important to know that not only Nest vendors, service providers, and technicians who help with processing and storage can "access certain information about you or your account",[103] but the same can be done by unspecified "Nest employees". Moreover, it is not clear if this can happen exclusively for external processing purposes: the access is envisaged not simply for that purpose, but in line with it (with the blurred boundary phrase of "non-Nest purposes"). In addition, while listing the situations where the company states that it shares personal information, this issue is kept separate by the reference to "external processing". Besides, Nest declares that is has strict policies and technical barriers in place to prevent unauthorised employee access to video data. One may question why these measures are confined to video data and to employees and why Nest does not conform to Google's policy of strict contractual confidentiality obligations.[104]

---

102 It has recently been reported that the Nest Cam remains "always on", even when the user has turned it off! See ABI Research, "Teardown Phone/Device: Nest Cam Works Around the Clock" (16 November 2015) at https://www.abiresearch.com/press/nest-cam-works-around-clock/ (accessed 8 December 2015). Nest says there is no truth in these allegations. "When Nest Cam is turned off from the user interface, it does not fully power down, as we expect the camera to be turned on again at any point in time," a Nest spokesperson told *El Reg*. "With that said, when Nest Cam is turned off, it completely stops transmitting video to the cloud, meaning it no longer observes its surroundings." <http://www.theregister.co.uk/2015/11/25/nest_cam_doesnt_spy/> (accessed 8 December 2015).

103 This same provision within the Privacy Policy for Nest Web Sites (including the reference to the employees) can be found in the Sugr Privacy Statement <http://www.sugrsugr.com/index.php/privacy-statement/> (accessed 8 December 2015).

104 The Google Privacy Policy, last modified 19 August 2015 states "We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations" <http://www.google.com/policies/privacy/> (accessed 8 December 2015). It should be noted that Alphabet Inc's privacy policy (and overall legals) are not available yet.

41 Regarding data sharing, which may occur locally among devices, between Nest Products and the customer's mobile device or application, or on Nest's servers, three more justifications are given. First, explicit consent, Nest states on the WPP that "you can change your mind at any time". However, if one does not give consent to the exchange of data with third parties providing products and services, use of those products and services will be impossible.[105] The same applies to sharing with partners (for example, energy and insurance companies). This seems to ignore that processing "necessary for the performance of a contract" is an equally valid justification under data protection law.[106]

42 Even before that, there is a technical reason why consent and awareness are threatened in the IoT. As stated also by the UK Information Commissioner's Office ("ICO"),[107] IoT devices often have no physical interface through which an individual can set, interact and control information flows, consequently one might question if the consent qualifies as valid and informed. On this point, it is important to stress that the Developer ToS binds the developer to "provide and adhere to a privacy policy for your Client that [...] is conspicuously displayed to all end users of your Client".[108]

43 Another justification is labelled "business transitions". It refers to the possibility of the sale or transfer of the Nest company or of all or part of its assets: in this case, the purchaser will be requested to treat the data in a manner consistent with the Privacy Statement in place at the time of its collection (even though it is unlikely that this point that the clause would be a deal-breaker).

105 The Nest legals provide plenty of examples of such "fictitious" consent. The authors have already shown and will see further cases where the only alternative to consent is not to enjoy the product.

106 Directive 95/46/EC Art 7(b).

107 Information Commissioner's Office, The Information Commissioner's response to Ofcom's consultation "Promoting Investment and Innovation in the Internet of Things" (1 October 2014) <https://ico.org.uk/media/about-the-ico/consultation-responses/2014/2512/ico-response-to-ofcom-consultation-on-internet-of-things-20141001.pdf> (accessed 8 December 2015).

108 The same provision can be found in the Bluvision Developer Terms of Service. Fibar group is a Polish manufacturer of wireless home automation systems; its "Climate" plug-ins work with Nest.

44 Lastly, Nest reserves the right to share information in the case where it "believe[s] in good faith" that there are "legal reasons" to do so. This appears as one of the most risky clauses of the legals relating to personal data. Its wording is significantly different from the average contract, where one usually finds expressions such as "legal requirement"[109] or "legal process",[110] let alone the cases when the company guarantees "not [to] hand over user data to authorities unless a warrant issued by [local court] is presented".[111]

45 While it is true that the Nest WPP specifies the legal process and commits to comply with state and federal laws, this is only provided as an example. Moreover, the fact that the example offered is from a US perspective ("with state and federal laws or the applicable laws of foreign countries other than the United States"), notwithstanding that the document is for the UK market, is evidence that the Nest legals are US-originating contracts that have been simply (and softly) adapted to a European context.[112]

46 It is well known why strict wording is important when it comes to disclosure of personal data. Law enforcement agencies ("LEAs") can use laws with extraterritorial effect to force not only companies based in the US into handing over user data (but also include preventing notification to customers about whom Nest has been asked to disclose data). An order can be addressed also to European subsidiaries having parents in the US, or to EU companies using the services of a US subsidiary for data processing,

109 See, for example, LinkedIn Privacy Policy at https://www.linkedin.com/legal/privacy-policy (last revised on 23 October 2014).

110 An example is provided by Google Privacy Policy. Google explains that it "regularly receives requests from governments and courts around the world to hand over user data", but it ensures that "frequently push back when the requests appear to be overly broad or don't follow the correct process" <http://www.google.com/policies/privacy/example/legal-process.html> (accessed 8 December 2015).

111 See JottaCloud Privacy Guarantee (last updated on 16 June 2013) at https://www.jottacloud.com/its-your-stuff-guaranteed/ (accessed 8 December 2015).

112 The US influence over Nest legals has become stronger since the last update of the legals. For instance, the UK version of the Privacy Statement has been changed to substitute "unauthorised", "programme", "postcode", "neighbourhood" and "personalise" with "unauthorized", "program", "postal or ZIP code", "neighborhood" and "personalize".

or, again, using any third-party to store or process data in the US.[113] The last case occurs in the Nest scenario and the conflict with EU law does not necessarily guarantee non-disclosure.[114]

47 As already underlined, part of the essence of the IoT is networking between things, often mediated through cloud services.[115] This means that things talk to each other. One should not be surprised then, when it is discovered that the thermostat "pulls information directly from your heating and cooling (HVAC) system".[116] And this is not the end, because obviously Nest products talk to other Nest products (and to the immense realm of "Works with Nest"). Consequently, "the products will share certain information with each other".[117] It is also noteworthy that the communication in the smart home does not entirely rely on one's house connection to the Internet. In fact, Nest Protects operates on Nest Weave that uses 802.15.4 and Wi-Fi 802.11 b/g/n; therefore, multiple products can remain connected to one another even if the household's connection to the Internet stops working.[118]

113 Such orders may also come from European LEAs and be imposed on US companies.

114 See I Bodle, "EU Data Protection Law and the Patriot Act in the Cloud" *Web Analytics World* (29 March 2012), where it reported that "Well known global software and search engine companies have admitted that EU customer data has been disclosed by them as a consequence of requests under the Patriot Act" <http://www.webanalyticsworld.net/2012/03/eu-data-protection-law-and-the-patriot-act-in-the-cloud.html> (accessed 8 December 2015).

115 For the interesting concept of "Social Internet of Things", see L Atzori, A Iera & G Morabito "Making Things Socialize in the Internet – Does it Help Our Lives?" in *Proceedings of the 2011 ITU Kaleidoscope Academic Conference: The Fully Networked Human? – Innovations for Future Networks and Services* (IEEE, 2011) at http://www.social-iot.org/d/kaleidoscope.pdf (accessed 8 December 2015).

116 Nest Privacy Statement.

117 Nest Privacy Statement.

118 The customer might be led to think that switching off their Wi-Fi router is sufficient to stop the communication between their devices. Therefore this information ought to be provided in the legals and not in Nest blog <https://nest.com/support/article/How-does-Nest-Protect-connect-wirelessly> (accessed 8 December 2015).

48 Now, one might imagine reacting to the massive collection of data with a sort of private enforcement of privacy by design.[119] There are many tools that aim at shielding the customer from being tracked. An example is the "Do Not Track" option provided by a browser.[120] It is important not to rely on such methods. Nest informs its users in the WPP that the selection of the mentioned option "*may not have any effect on our collection of cookie information* for analytic and internal purposes" [emphasis added].

49 This warning leads us also to the purpose of data collection via IoT products. Google has warned that "a few years from now, we and other companies could be *serving ads and other content on refrigerators, car dashboards, thermostats*, glasses and watches, to name just a few possibilities" [emphasis added].[121] As at the writing of this paper, advertisements are not currently displayed on Nest products, but the data from these products are nonetheless used to advertise. Even though Nest repeats several times that the information is used to provide users with Nest products and services, under this leitmotif is what is really important: the commodification and the commercial use of the users' personal data. In fact, the Nest WPP states what is collected is used "to provide advertising that is relevant to your interests".

50 This can deeply affect the customer's privacy, given that once again the multi-layered structure can act as a disclaimer of responsibility. As unsurprising as it may be, Nest warns in the WPP that it permits third-party advertising partners to use cookies and other technology to collect information and that "we have *no control over and cannot confirm whether these third party ad parties*

119 It should be noted that policy routing, cryptographic techniques, information flow control (IFC) constitute a cost, hence policy makers (and contracts drafters) have to strike the balance between privacy (by design) and competition.

120 For example, Mozilla Firefox website https://www.mozilla.org/en-GB/firefox/dnt/ (accessed 8 December 2015).

121 See C Clifford, "Google: In a Few Years, Ads Will Show Up on Refrigerators, Thermostats and Glasses" *Entrepreneur* (21 May 2014) <http://www.entrepreneur.com/article/234122> (accessed 8 December 2015).

honor the Do Not Track browser signal" [emphasis added].[122] Furthermore, the fact that advertising is part of the contract can additionally threaten the customer's privacy. Although the processing of personal data is lawful even without consent if necessary "for the performance of a contract to which the data subject is a party".[123] Consequently, with all the activities of processing, tracking and profiling forming part of the contract, the company could easily claim that the customer has no right to prevent such processing of their data.

51 Finally, it should be recalled that the IoT is not only about sensing and sending/receiving data, it is also about actuating. Actuation can affect both the physical environment and the processing of data. A good example is provided by a change in the most recent update to the ToS, whereby "you acknowledge that *Nest may activate Bluetooth on your smartphone or tablet*, with or *without prior notification*, in order to facilitate proper operation of the Services; enable communication with Nest Products connected to the same Nest account and enable certain features (such as remote silencing of a smoke or CO alarm on Nest Protect)" [emphasis added].[124] It is arguable that customers need to be aware that the IoT is not only a matter of people controlling things, but also things controlling people.

Applicable law and jurisdiction

52 When it comes to any contract, an important issue is the applicable law and jurisdiction. This has some unusual aspects in an IoT context. A customer who looks at a thing is likely to believe that the thing is located geographically in the place where the

122 In the original wording, Nest suggests that the customer might avoid third-party tracking, but in the most recent update, it notes that one can only avoid use of this information for advertising if "these third party ad parties honor the Do Not Track browser signal".

123 Directive 95/46/EC Art 7(b).

124 The customer who reads the Privacy Statement and not the Terms of Service may be led not to understand this point. In fact, under the former "Bluetooth-enabled Nest Products (such as Nest Protect 2nd generation and Nest Cam) may broadcast an identifying signal wirelessly. This is used to connect with your Bluetooth-enabled devices".

customer is. But what if it is a US device sold in Venezuela, whose embedded software runs, say, in Ireland, whose smartphone app is provided by a Chinese company, whilst the customer accesses the relevant account in Tunisia: where is the thing located?

53 The contract might provide some assistance. However, this is not the case in the Nest scenario. Under the EULA and the ToS, California law applies, even though the "courts in some countries will not apply California law to some types of disputes", presumably due to overriding mandatory rules of the state where the user is located,[125] whilst under the T&Cs Irish law applies.

54 Once again, one notices a fabricated separation, this time between embedded software and apps and services. In a case regarding a single IoT product, a judge may be required to create a novel expression of existing laws by applying fragments of California law and fragments of Irish law.

55 On top of everything, the Limited Warranty, which professedly concerns the product only as hardware,[126] states that "For a full description of your legal rights you should refer to the laws applicable in your jurisdiction". This clause can reasonably be interpreted as referring to the law of the customer's jurisdiction, whether under consumer protection law, private international law or otherwise. Therefore, even for issues related to the same part of the product (the hardware), the judge should apply different pieces of legislation. The importance of ascertaining the applicable law is well illustrated by the Limited Warranty. As a matter of fact, the disclaimers, exclusions, and limitations of liability under the Limited Warranty will not apply "to the extent prohibited by applicable law", not to mention that "to the maximum extent permitted by applicable law, Nest Labs disclaims all express, implied, and statutory warranties" and that "[t]o the maximum extent permitted by applicable law, Nest Labs also limits the

125 *Eg*, under intellectual property or consumer protection laws.

126 Section 4 of the Limited Warranty states "This warranty does not cover consumable parts, including batteries, unless damage is due to defects in materials or workmanship of the Product, or software".

duration of any implied warranties or conditions to the duration of this limited warranty."

56 The judge therefore needs not only to determine which is the applicable law, he also has to create it by the combination of different pieces of legislation and clarify what is "the extent prohibited by applicable law", a clause so unclear it can be hardly be considered reasonable and fair. While such phrases may not be novel in commercial agreements, and are indeed widely present in the ICT sector, the compound nature of the IoT lends such phrases an enhanced opaque quality.

57 The collection, processing, and storage in non-EEA countries (namely in the US and in unspecified "other countries where our servers reside")[127] give rise to considerable problems. In fact, as a result the WPP states "your personal information may be subject to legal requirements, including lawful requirements to disclose personal information to government authorities, in those jurisdictions".[128]

58 Applicable law and jurisdiction are connected issues. IoT contracts often include arbitration clauses in which both the applicable law and appropriate forum are designated, while also indicating that certain matters may be litigated rather than arbitrated. Both under the ToS and the T&C, for example, Nest customers submit themselves to binding arbitration and further agree "arbitration is final and binding and subject to only very limited review by a court" and accept to waive the right to any form

127 The authors do not know, for instance, if the servers used by Rackspace for redundancy are those in London or the ones in Chicago, Dallas, Northern Virginia, Hong Kong, or Sidney. Likewise, it is not clear which data centre is used by Amazon (AWS edge locations: Ashburn, VA (3), Atlanta, GA, Dallas/Fort Worth, TX (2), Hayward, CA, Jacksonville, FL, Los Angeles, CA (2), Miami, FL, New York, NY (3), Newark, NJ, Palo Alto, CA, San Jose, CA, Seattle, WA, South Bend, IN, St Louis, MO).

128 This is a significant development in the most recent update of the Nest legals. At the time of writing, the authors are still waiting for the appeal process to be completed in a case in which Microsoft has challenged a warrant issued by a New York magistrate requiring production of emails held on a server in Ireland.

of appeal, review or recourse to any court or other judicial authority, insofar as such waiver may be validly made.

59 At the same time, a trial could be initiated before at least three different courts. As a matter of fact, any action or proceeding relating to the ToS and the EULA must be brought "in a federal or state court located in Santa Clara County, California", but only the latter provides that Nest may seek injunctive relief "in any court having jurisdiction to protect its intellectual property or Confidential Information". As regards the disputes under the T&Cs, then, "The courts of Ireland will have non-exclusive jurisdiction" and customers may have the right under relevant consumer protection laws to bring proceedings in their country of residence (the reference is clearly addressed to a consumer). For the EULA, whereas the court of Santa Clara County will (theoretically) judge on cases regarding apps and services, the court of San Francisco will judge if one sends a counter-notice under the Digital Millennium Copyright Act (DMCA), claiming that the "user submissions" (mainly user-generated content) that was removed (or to which access was disabled), does not infringe the DMCA.[129]

60 So there would appear to be as many applicable jurisdictions as the number of legals! Therefore, in respect of the Nest product, it seem that one should initiate a dispute before different courts and it may also happen that even though the same right is at stake (for example, copyright) different courts may claim the jurisdiction. There is a real quagmire here.

PRODUCT LIABILITY

61 Product liability regimes address the attribution of liability between the producer of a product and the person using that product. They represent a departure from traditional contractual and tortious rules under which an injured party in litigation has to prove that the defendant is either in breach of contract or at fault and in breach of a duty of care towards the claimant. By contrast,

129 In particular, the user has to allege that the content is not infringing, or that they have the authorisation from the copyright owner, the copyright owner's agent or pursuant to the law.

under product liability law, the injured person is not required to adduce evidence of either a contract or any fault and will usually be able to bring a claim against a broader category of persons. By imposing strict liability, the law increases the risk of liability for the producer; enhances protection and the possibility of redress for the consumer and, as a by-product, ensure the safety and quality of products sold on the market.[130]

62 In Europe, the product liability regime dates back to a 1985 Directive,[131] which was seen from the outset, as a response to solving the problem, peculiar to the age of increasing technicality, of a fair apportionment of the risks inherent in modern technological production.[132] The regime cannot, therefore, be dismissed as not being intended to cover recent developments such as the IoT. However, the rules regarding liability for defective products seem to have been somewhat neglected over recent years,[133] due in part to the growth of the service-based economy, which includes the Internet and more generally intangible digital products and services.[134] Indeed, it has been noted that while the liability model established under the Product Liability Directive has

130 For a contrary view of product liability, see A M Polinsky and S Shavell, "*The Uneasy Case for Product Liability*" 123 *Harv L Rev* 1437 (6 April 2010).

131 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ 1985 L 210, p 29) ("Product Liability Directive"). It was amended by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 141, 4 June 1999, pp 20–21) ("Directive 1999/34/EC") to include agricultural and fishery products.

132 Directive 1999/34/EC, at recital 2.

133 See European Commission, Fourth Report on the application of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products amended by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999, COM (2011) 547 final (8 September 2011) at p 4, which notes that the number of cases rose in some countries such as Germany and France.

134 The Commission has considered a similar initiative on "safer services" ("Consumer Policy Action Plan 1999–2001", COM (1998) 696 final of 1 December 1998, at s 4.3), but no such proposal has been published.

been hugely influential internationally, to date "the practical impact of its ideas has been close to negligible".[135]

63 Although the Product Liability Directive has been relatively dormant, the Court of Justice has recently been asked to consider its application in a case involving health-related IoT devices, in the form of "pacemakers and implantable cardioverter defibrillators".[136] While it is too early to predict with any certainty, the implications of this decision for product liability regimes may be very significant.[137] With the explosive growth of the IoT market and an expansive concept of "product", the authors consider the possibility of a revival of product liability. On this basis, it is worth examining the EU regime and considering its applicability to the Nest case study.

64 In *Boston Scientific*, products contained a defect that could result in premature battery depletion and subsequent loss of certain functionality, including telemetry, which is, transmitting recorded data to an external device. Following identification of the defect, the supplier offered their replacement free of charge. However, claims were made for compensation in respect of the costs of the implantation of the original faulty products. The first issue for consideration by the court was whether a "product belonging to the same group or forming part of the same production series"[138] could be said to be defective under Article 6(1) without the need to evidence that the specific product was defective. The court held that it could, especially given the nature of the product and the high expectations of users of that product.

135 M Reimann, "Product Liability in a Global Context: The Hollow Victory of the European Model" (2003) 11(2) *European Review of Private Law* 128 at 129.

136 *Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt — Die Gesundheitskasse (C-503/13), Betriebskrankenkasse RWE (C-504/13)* Joined Cases C-503/13 and C-504/13 (5 March 2015) ("Boston Scientific").

137 B Van Leeuwen & P Verbruggen, "Resuscitating EU Product Liability Law? Contemplating the Effects of Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt and Betriebskrankenkasse RWE (Joined Cases C-503/13 and C-504/13)" (2015) 23(5) *European Review of Private Law* 899.

138 B Van Leeuwen & P Verbruggen, "Resuscitating EU Product Liability Law? Contemplating the Effects of Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt and Betriebskrankenkasse RWE (Joined Cases C-503/13 and C-504/13)" (2015) 23(5) *European Review of Private Law* 899 at para 28.

Second, the court was asked to determine whether damage under the first limb of its definition, relating to death and personal injury,[139] extended to the surgical procedure required to replace the defective device. The court held that it did, but only if the operation was necessary to overcome the defect.[140]

65 The Product Liability Directive is applicable to "products", which is defined as all "movables", even when incorporated into another movable or immovable, and including electricity.[141] Further clarity around this definition may be found in the instruments transposing the measure into national law. In the UK, for example, a product includes "a product which is comprised in another product, whether by virtue of being a component part or raw material or otherwise".[142] In a Nest and IoT context, therefore, a key issue is to what extent the "product" can be said to include its intangible component parts, specifically the software and data. The Commission saw the Directive's definition as extending to software, but not services, with Lord Cockfield noting that the Directive "applies to software in the same way … that it applies to handicraft and artistic products".[143] Notwithstanding the Commission's statement, uncertainty about the application of the Directive to software has persisted over the years, partly from the fact that software may be considered a service in certain circumstances.[144]

139 Product Liability Directive Art 9(a).

140 With regard to the defibrillators, evidence suggested that the defect could be addressed by deactivating a magnetic switch on the device, rather than removal.

141 Product Liability Directive Art 2.

142 Consumer Protection Act 1987 (Cap 43) s 1(2).

143 See "Answer given by Lord Cockfield on behalf of the Commission" (15 November 1988) to the "Written Question No 706/88 by Mr Gijs de Vries (LDR-NL) to the Commission of the European Communities" (5 July 1988) (89/C 114/76) at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOC_1989_114_R_0001_01&qid=1429892489522&from=EN (accessed 8 December 2015).

144 C Reed & J Angel, *Computer Law* (Oxford University Press, 6th Ed, 2007) at p 113, observed that "it seems likely … that the Act applies only to software which is marketed on some form of tangible medium (*eg*, a tape or disk) ownership of which is transferred to the purchaser". Others consider most consumer purchases of software as a sale of goods; *eg*, J Adams, "Software and Digital Content" (2009) 4 *Journal of Business Law* 396.

While UK law is also unclear, the concept of a "product" includes one whose "essential characteristics of which are attributable to an industrial or other process having been carried out."[145] This would certainly seem applicable to a product's integrated software. However, to date, there has not been any European case applying the Product Liability Directive directly to software, which has exacerbated the uncertainty.

66 The Nest legals have chosen to expressly distinguish the software from the "Product", with the "Limited Warranty" stating that it "does not cover consumable parts, including batteries, unless damage is due to defects in materials or workmanship of the Product *or software (even if … packaged or sold with the product*)" [emphasis added].[146] The validity of this exclusion would seem to depend not on Nest's ability to distinguish between hardware and software within the product, but rather on the basis that while Nest Labs (Europe) Ltd is acknowledging that it is the producer of the hardware, and hence liable for any "defect", it is not accepting this role in respect of the software, which, by virtue of the EULA, it would argue was produced by Nest Inc. Whether such a position would be vulnerable to challenge is debatable, as it is certainly a lacuna in the protective regime; but, if accepted, the treatment of the software itself as a component part of a product would continue to be an arguable point.

67 One of the main concerns for customers of IoT products is that the multi-layered structure of the supply chain could effectively act as a disclaimer of responsibility. Put simply, there is a risk that the manufacturer of the hardware claims that the software developer is the real party responsible for any defect, or tries to shift responsibility to the service provider. Under a strict liability regime, this should not be allowed. Under Article 3 of the Product Liability Directive, the concept of the "producer" is multi-layered, to prevent any shifting of responsibility. In the first instance, it means the manufacturer of the finished product, or the manufacturer of a component part, or any person who presents

145 This wording appear in relation to the definition of a "producer" in s 1(2) of the Consumer Protection Act 1987 (Cap 43) (UK).

146 Nest Labs (Europe) Ltd, Limited Warranty s 4.

himself as its producer, by putting his name, trade mark or other distinguishing feature on the product.[147] Next, where the product is imported and distributed in the territory, that person is deemed responsible as producer, which extends the territorial application of the Directive to foreign products.[148] Finally, where neither the producer nor the importer can be identified, then the supplier is considered the responsible producer, unless he can identify the producer, the importer or the person that supplied him within a reasonable time.[149] Such an inclusive and broad concept would seem perfectly applicable to the characteristic of IoT markets, where nearly all things are composite things. However, in relation to certain technological developments, such as 3D printing, the emergence of "prosumers" may challenge existing regulatory concepts.[150]

68 Under the Product Liability Directive, the injured person has to prove three things: the defect, the damage and the causal relationship between the two.[151] Of these, the first and last can be significant hurdles to overcome. With regard to defects, the threshold is that the product does "not provide the safety which a person is entitled to expect, taking all circumstances into account".[152] What constitutes a reasonable expectation may obviously vary considerably depending on the market segment in

147 Product Liability Directive Art 3(1).

148 Product Liability Directive Art 3(2). As noted above, the majority of consumers are likely to buy direct from Nest's website or from an e-commerce platform.

149 Product Liability Directive Art 3(3). See *Skov AEG v Bilka Lavprisvarehus A/S* (C-402/03), [2006] 2 CMLR 16, where the Court of Justice confirmed that the Directive focuses liability on the producer, not any intermediary party in the supply chain (except where the producer is not identifiable), since "by obliging all suppliers to insure against such liability, it would result in products becoming significantly more expensive" (at para 28). See also *Aventis Pasteur SA v OB* (C-358/08), [2010] 2 CMLR 16, which confirmed that where an injured person was not reasonably able to identify the producer, the supplier is obliged to act "on its own initiative and promptly" to identify the producer.

150 See N Berkowitz, "Strict Liability for Individuals? The Impact of 3-D Printing on Products Liability Law" (2015) 92(4) *Washington University Law Review* 1019 (11 January 2015).

151 Product Liability Directive Art 4.

152 Product Liability Directive Art 6(1) and recital 6.

which the IoT device is deployed. In *Boston Scientific*, the court held that such expectation must be assessed on the basis of "the intended purpose, the objective characteristics and properties of the product in question and the specific requirements of the group of users for whom the product is intended".[153] With regard to the specific devices under consideration, the court felt that an expectation of a near zero failure rate in an implantable device would be reasonable for patients, even though medical experts are aware that such devices are not free of the risk of failure.[154] To date, who bears the burden of evidencing that a defect exists has varied considerably across the Member States.[155] However, following *Boston Scientific*, it now appears sufficient for the claimant to demonstrate the risk of a defect or the "potential for failure", rather than that a specific device has a defect, which significantly lowers the threshold.[156]

69 A producer can also raise various defences, the most relevant of which in the context of IoT devices is:[157]

> ... that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered.

70 This provision, commonly known as the "development risk" or "state-of-the-art" defence, was seen as a compromise between the

153 In *Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt — Die Gesundheitskasse (C–503/13), Betriebskrankenkasse RWE (C–504/13)* Joined Cases C-503/13 and C–504/13 (5 March 2015) at para 38.

154 In *Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt — Die Gesundheitskasse (C–503/13), Betriebskrankenkasse RWE (C–504/13)* Joined Cases C-503/13 and C–504/13 (5 March 2015) at para 26.

155 European Commission, Fourth Report on the application of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products amended by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999, COM (2011) 547 final (8 September 2011) at p 7. For the UK, see *Ide v ATB Sales Ltd* [2008] EWCA Civ 424.

156 Opinion of Mr Advocate General Bot: Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt – Die Gesundheitskasse (C–503/13) and Betriebskrankenkasse RWE (C–504/13) Joined Cases C–503/13 and C–504/13 (21 October 2014) at para 3.

157 Product Liability Directive Art 7(e).

interests of consumers and facilitating innovation.[158] Since 1985, debate has continued over the relative costs and benefits of this provision for both consumers and producers. It has been held that this provision does not require consideration of the "practices and safety standards in use in the industrial sector in which the producer is operating", which would be a consideration under a traditional negligence analysis,[159] but instead requires a more holistic perspective involving considerations of accessibility.[160] Legislators were evidently aware that this defence could provide producers with too much leeway, especially in rapidly evolving sectors such as ICTs, where states of industry knowledge can be very difficult to determine with certainty. They therefore provided Member States with an option to exclude this defence, such that a producer would be liable "even if he proves that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of a defect to be discovered".[161]

71 Evidencing the causal relationship between the defect and damage can also be a challenge, particularly when complex technologies are involved. In *Hufford v Samsung Electronics (UK) Ltd*,[162] for example, the claimant was unable to discharge the burden of proof that a fridge-freezer caused a fire in his home. Such difficulties have led some Member States and consumer groups to call for the Product Liability Directive to be amended either to reverse the burden of proof or to adopt a presumption of producer

158 Fondazione Rosselli, *Analysis of the Economic Impact of the Development Risk Clause as Provided by Directive 85/374/EEC on Liability for Defective Products* (Contract No ETD/2002/B5) at http://www.palmigiano.it/wp-content/uploads/2013/12/dev-risk-clause-study_final-report.pdf (accessed 8 December 2015).

159 See *Baker v Quantum Clothing Group* [2011] UKSC 17.

160 *European Commission v United Kingdom* [1997] 3 CMLR 923 at paras 26-28.

161 Product Liability Directive Art 15.1(b). Only Luxembourg and Finland have adopted this position. C Reed & J Angel, *Computer Law* (Oxford University Press, 6th Ed, 2007) at p 113 in particular fn 141, note that given the practice of releasing software that is not entirely "bug-free", it would be arguable that a software producer who failed to discover even a serious defect would be able to take advantage of the defence, so long as the defect is not in an area of the program that would be tested as a matter of course by others in the industry.

162 [2014] EWHC 2956.

liability.[163] However, producers and insurers inevitably contest such proposals.

72 The concept of damage under the Product Liability Directive is limited to death, personal injury and damage to any other item of property.[164] In *Boston Scientific*, however, the court took an expansive view of what damage should be compensated, including "all that is necessary to eliminate harmful consequences and to restore the level of safety which a person is entitled to expect".[165] Where the damaged property is for private use or consumption, a maximum recoverable threshold of €500 is imposed, which would apply to the Nest products.[166] For recovery of non-material damages, such as distress, this is left for the Member State's law to determine. Finally, it is not permissible for a producer to limit or exclude his liability under the Directive.[167]

73 It must also be noted that product liability regimes are closely linked with the related field of product safety law. While the former addresses liability for defects in a product that is already on the market, the latter imposes controls on the quality of products that can be "placed on the market".[168] With respect to IoT devices, there is a range of potentially applicable product safety laws at an EU

163 European Commission, Fourth Report on the application of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products amended by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999, COM (2011) 547 final (8 September 2011) at p 7.

164 Product Liability Directive Art 9. So damage to the device itself, so-called "transaction damage" is not covered. See *Société Moteurs Leroy Somer v Société Dalkia France* C-285/08 (4 June 2009).

165 In *Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt — Die Gesundheitskasse (C–503/13), Betriebskrankenkasse RWE (C–504/13)* Joined Cases C–503/13 and C–504/13 (5 March 2015) at para 49.

166 Product Liability Directive Art 9(b).

167 Product Liability Directive Art 12.

168 Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11/4, 15 January 2002) at Art 1(1). As pointed out by G Pisciotta, *La responsabilità per danno da prodotto e la produzione agricola con metodo biologico, in Diritti fondamentali. Qualità dei prodotti agricoli e tutela del consumatore* (E Capizzano ed) (Camerino, 1993) at p 216, a product can be "secure" under the product safety regime and "unsecure" under the product liability regime.

level, both general and sectoral, such as the type approval regime applicable to all "radio equipment"[169] and "medical devices".[170] These provide for *ex ante* compliance procedures coupled with an *ex post* oversight mechanism. The *ex ante* compliance procedures may be carried out by external "notified bodies" or through self-certification mechanism.[171] Once a product completes the "conformity assessment procedure" (also known as "type approval"), it can be placed on the European market. Once on the market, if a defect is subsequently identified, the associated exposure under the Product Liability Directive (especially given the broadening of liability risk to potential defects under *Boston Scientific*) should create a positive feedback loop into the producer's product safety management systems.[172] In the context of IoT, for example, one could imagine the need to have software update procedures in place, to enable "defects" to be addressed rapidly and *en masse*.[173]

169 Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153/62, 22 May 2014). "Radio equipment" is defined in Art 2(1)(1) to mean:

> an electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination.

170 Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169/1, 12 July 93), as amended. The Directive defines "medical device", in Art 1(2)(a), as including "the software necessary for its proper application".

171 Nest Protect has been tested to comply with safety standards in the US and Canada set out by: Underwriters Laboratories Inc, California State Fire Marshal, Canadian Standards Association, and the British Standards Institution.

172 See B Van Leeuwen & P Verbruggen, "Resuscitating EU Product Liability Law? Contemplating the Effects of Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt and Betriebskrankenkasse RWE (Joined Cases C-503/13 and C-504/13)" (2015) 23(5) *European Review of Private Law* 899 at p 14.

173 Although updates may obviously also be the cause of a defect. See J Wakefield, "Nest thermostat bug leaves users cold" *BBC* (14 January 2016) at http://www.bbc.co.uk/news/technology-35311447 (accessed 8 December 2015).

74 It is easy to infer the potential unenforceability of some of the Nest clauses outlined above under product liability rules. For example, in the Limited Warranty, Nest states that products supplied "AS IS" are "ineligible products", without any further elaboration as to why they should fall outside the warranty. The phrase "AS IS" is another example of the US wording being transplanted into a European marketplace; despite it being known that such phrases would be unenforceable in many European states. However, Nest also acknowledges that its provisions may not apply "to the extent prohibited by applicable law",[174] which would obviously include product liability rules.

UNFAIR TERMS

75 Controlling the imposition of unfair contractual obligations by a producer or supplier upon a customer is a central strand of all mature consumer protection regimes. While product liability laws focus on defective products already on the market and the "producer" who made them, unfair contract terms laws focus on the balance of rights and obligations established between the seller or supplier of the product and the consumer. The rules proceed on the presumption that the consumer is in a weak position "both [in] his bargaining power and his level of knowledge",[175] and provide a public law framework to remedy private law failings. Unfair contract terms laws must also be distinguished from rules protecting consumers at other points in the transaction process, such as marketing practices.[176]

174 Nest Limited Warranty.

175 *Caja de Ahorros y Monte de Piedad de Madrid v Asociacion de Usuarios de Servicios Bancarios (Ausbanc)* (C-484/08), [2010] 3 CMLR 43 at para 27.

176 See Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (OJ L 149/22, 11 June 2005).

76 Within Europe, such matters are primarily governed by national laws implementing Directive 93/13/EEC "on unfair terms in consumer contracts".[177] The Directive is only applicable where the term has not been individually negotiated, while a term is considered "unfair" if:[178]

> ... contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer.

77 The Directive elaborates two different types of unfairness. First, it provides an "indicative and non-exhaustive" list of terms that may be regarded as unfair.[179] These can be referred to as "issues of substance", since the focus is on the rights and obligations detailed in the agreement itself. Second, the Directive provides that "unfairness" can also be assessed on the basis of "all the circumstances attending the conclusion of the contract", which includes any other contract on which the main contract is dependent, as well as the language in which the terms are drafted, which should be "in plain, intelligible language".[180] These can be referred to as "issues of form", as it is the manner in which the contract is presented to the customer that is being considered. The assessment of the Nest terms must therefore consider both issues of substance and form.

78 To date, European case law under the Unfair Terms Directive has generally focused on issues of substance rather than form. However, in *Árpád Kásler and Hajnalka Káslerné Rábai v OTP*

177 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95/29, 21 April 1993), as amended ("Unfair Terms Directive"). The provisions were transposed into the UK law by the Unfair Terms in Consumer Contracts Regulation 1999 (SI No 2083 of 1999), but these were replaced by the Consumer Rights Act 2015 (c 15) Pt 2, as from 1 October 2015.

178 Unfair Terms Directive Art 3(1).

179 Unfair Terms Directive Art 3(3), which makes reference to the Annex.

180 Unfair Terms Directive Arts 4(1) and 5 respectively. Art 4(2) is a limitation to the scope of assessment, excluding "the definition of the main subject-matter" and "the adequacy of the price and remuneration", if they are drafted in plain and intelligible language; although Member States may ignore this limitation when transposing the Directive, in favour of a higher level of protection (see *Caja de Ahorros y Monte de Piedad de Madrid v Asociacion de Usuarios de Servicios Bancarios (Ausbanc)* (C-484/08), [2010] 3 CMLR 43 at para 2).

Jelzálogbank Zrt,[181] the court held that the requirement of transparency, in terms of "plain, intelligible language", "cannot … be reduced merely to their being formally and grammatically intelligible",[182] but rather must be understood in a broad sense, on the basis of an "average consumer, who is reasonably well informed and reasonably observant and circumspect"[183] and who should be able to "assess the potentially significant economic consequences for him".[184]

79 In *RWE Vertrieb AG v Verbraucherzentrale Nordrhein-Westfalen eV*[185] ("*RWE Vertrieb*"), the court noted that it was not sufficient to include a "mere reference, in the general terms and conditions, to a legislative or regulatory act determining the rights and obligations of the parties. It is essential that that the consumer is informed … of the content of the provisions concerned".[186] The court went on to note that the level of information required will vary depending on the circumstances, with both *RWE Vertrieb* and *Invitel* being concerned with the levying of charges. However, on the face of it, such an obligation could have very significant implications for contractual drafting in Europe.[187]

80 In the Nest T&Cs, for example, it is noted that the consumer has "certain legal rights" and that any exclusions, disclaimers or limitation of liability provisions will apply to the extent permitted

181 *Árpád Kásler and Hajnalka Káslerné Rábai v OTP Jelzálogbank Zrt* C-26/13 (30 April 2014).

182 *Árpád Kásler and Hajnalka Káslerné Rábai v OTP Jelzálogbank Zrt* C-26/13 (30 April 2014) at para 71.

183 This wording has been inserted into the Consumer Rights Act 2015 (c 15) s 64(5).

184 *Árpád Kásler and Hajnalka Káslerné Rábai v OTP Jelzálogbank Zrt* C-26/13 (30 April 2014) at para 74. See also *Jean-Claude Van Hove v CNP Assurances SA* C-96/14 (23 April 2015).

185 *RWE Vertrieb AG v Verbraucherzentrale Nordrhein-Westfalen eV* (C-92/11), [2013] 3 CMLR 10.

186 *RWE Vertrieb AG v Verbraucherzentrale Nordrhein-Westfalen eV* (C-92/11), [2013] 3 CMLR 10 at para 50. See also *Nemzeti Fogyasztovedelmi Hatosag v Invitel Tavkozlesi Zrt* ("*Invitel*") (C-472/10), [2012] 3 CMLR 1 at 29.

187 See C Leone, "Transparency Revisited – On the Role of Information in the Recent Case-law of the CJEU" (2014) 10(2) *European Review of Contract Law* 312.

by law.[188] However, as regards what such rights may be, the terms simply suggest "you should refer to the laws applicable in your country or jurisdiction".[189] In the UK, the Competition & Markets Authority ("CMA"), the relevant enforcement authority, has stated that wide exclusion clauses "qualified merely by a statement that the trader's liability is excluded only to the extent permitted by statute" are manifestly both unfair and lacking transparency.[190] While Nest's phrasing would appear to be common industry practice,[191] one could imagine that for certain IoT applications, especially the more intimate they are to the user's well-being, a higher standard of transparency could be imposed on providers under unfair contract terms rules.

81 In the UK, the applicable legislation extends to non-contractual "notices" as well as contracts,[192] which would include the use of disclaimers stuck, or packaged with, on IoT products, attempting to add another layer of protection for the producer or supplier. With regard to the Nest legals, two key examples are the EULA for the product software and the "Open-source Compliance" notice. In both cases, although Nest attempts to make them contractual in nature,[193] such characterisation is debateable and could be subsequently rejected by a court, giving rise to legal uncertainty. Both also attempt to limit liability. In the latter case, as well as listing all the open source modules contained in the

188 Nest Terms & Conditions.

189 Nest Terms & Conditions preamble.

190 Competition & Markets Authority, *Unfair Contract Terms Guidance: Guidance on the Unfair Terms Provisions in the Consumer Rights Act 2015* CMA37 (31 July 2015) at para 2.54.

191 See for instance Meshare Terms and Conditions of Sale at https://www.meshare.com/sales-terms/; Losono General Terms and Conditions at https://lono.io/general-terms-and-conditions-of-sale; Neposmart Sale Terms and Conditions at https://neposmart.com/sales-terms-and-conditions (all links accessed 8 December 2015).

192 Consumer Rights Act 2015 (c 15) s 61.

193 The EULA states that "THIS IS A LEGAL AGREEMENT", while the Open-source Compliance Notice states that by clicking "Accept" you have read and accepted the Download Agreement. The uncertain status of open-source notices is well recognised, see L McDonagh, "Copyright, Contract and FOSS" in *Free and Open Source Software: Policy Law and Practice* (N Shemtov & I Walden eds) (Oxford: Oxford University Press, 2013).

Learning Thermostat, providing access to the related source code and indicating the applicability of General Public License Version 3 ("GPLv3"); it also disclaims all warranties and shifts the "entire risk and the entire liability" to any consumer who uses those software modules to modify the device. The rules on unfairness do not apply, however, where the notice is mandatory, which would be applicable to the EU Declarations of Conformity supplied by Nest and associated CE marking.[194]

82 The CMA has emphasised that although unfair contract terms rules have a distinct requirement of transparency,[195] which it terms a "transparency test", this in fact is simply an integral component of any assessment of fairness.[196] The CRA adds a requirement of "legibility" to the need for plain and intelligible language provided for in the Directive. However, while a finding that a term, an agreement or a set of agreements lack transparency may not in itself be sufficient to render a contract "unfair", any uncertainty about meaning arising from the lack should be interpreted in a manner most favourable to the consumer.[197] The need for transparency within a contract varies according to the nature of the provision. As noted above, the Nest legals make extensive use of text in capitals in order to give "appropriate prominence"[198] to terms that may be considered disadvantageous to the consumer.

83 From the earlier analysis, the Nest legals do not obviously contain any provisions that expressly fall foul of the "blacklist" or "greylist" of terms detailed in the Directive's Annex.[199] However, with respect to issues of form, it would seem at least arguable that, taken as a whole, the Nest legals could be seen as lacking sufficient transparency, by not enabling an average consumer to understand the complex dependencies and interaction between the product,

194 Consumer Rights Act 2015 (c 15) s 73.
195 Consumer Rights Act 2015 (c 15) s 68.
196 Competition & Markets Authority, *Unfair Contract Terms Guidance: Guidance on the Unfair Terms Provisions in the Consumer Rights Act 2015* CMA37 (31 July 2015) at para 2.5.
197 Unfair Terms Directive Art 7.
198 Phrase used by Lord Bingham in *The Director General of Fair Trading v First National Bank plc* [2002] 1 AC 481; [2001] UKHL 52.
199 Unfair Terms Directive Annex I.

service and software agreements that, as a minimum, underpin the Nest products. While each agreement in itself might be considered as clearly drafted, European law expressly recognises the critical impact that another contract on which it is dependent may have and the need for the relationship between terms among these dependent contracts, as much as within the individual agreements themselves, to be clearly set out.

CONCLUSION

84 This paper has focused on the Nest legals as a case study, a qualitative rather than quantitative approach, designed to identify issues of concern that may, or may not,[200] be rife within the emerging IoT marketplace, but which are worthy of consideration. After giving an account of some general contract law issues relevant in an IoT context, the authors have illustrated the complexity of their chosen IoT supply chain and its associated legals. Many issues that the authors discuss are not specific to the IoT context, especially the lack of bargaining power for consumers and issues of applicable law and jurisdiction. Further issues are important in other IT contracts, such as cloud computing, but may not have particular resonance for IoT contracts. That said, the main conclusion is that the world of IoT demonstrates a need to consider recasting the concept of product to reflect the frequent inextricable mixture of hardware, software, data and service.

85 Product liability and unfair contract term regimes are just two strands of a broader set of consumer protection rules designed to address the asymmetry of bargaining power in modern commerce.[201] Whether the integration of IoT devices into our lives

200 *Eg*, the Ecobee 3 smart thermostat comes with only three documents: Privacy Policy & Terms of Use, Terms of Sale, and Reseller Terms <https://www.ecobee.com/legal/> (accessed 8 December 2015).

201 *Eg*, "digital content" contracts under Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (OJ L 304/64, 22 November 2011). These aspects will be separately investigated.

will lead to a significant rise in claims being made under such laws will obviously depend on a range of factors, including national conditions in relation to access to justice, such as the availability of class actions.

Privacy and Data Protection Issues in Big Data: A Brave New World in the Cloud

Today, technology advances at an unprecedented and exponentially increasing rate never before witnessed by mankind. Almost overnight, the world has quietly transformed into a brave new world of big data. With the advent of big data, it is undeniable that there needs to be a shift in the way one sees the world. Privacy and data protection issues have come into sharp focus; in particular, queries arise as to whether these concepts are still fit for purpose in a world where boundaries are fast shrinking and the resultant threats to mankind are rapidly evolving. This paper will discuss selected current privacy and data protection concerns raised in the age of big data and hopes to facilitate an understanding of some of the complexities which result from the interaction between technology and law.

WONG Baochen*
LLB (Hons) (National University of Singapore);
Assistant Registrar, Supreme Court of Singapore.

INTRODUCTION

1 A world in the cloud: that is the big data world today. The textbook definition of big data is "*Big data is high-volume, high-velocity, and/or high-variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization.*"[1] Conventionally, therefore, the three key characteristics of big data are: (a) *volume*, which can be understood as quantity; (b) *velocity*, as the speed at which data is generated; and (c) *variety*, in terms of the innumerable sources and types of data.[2] The world is in the midst of an explosion of data

* Some of the ideas in this article springboard from and develop further the discussions of the panel "Privacy and Data Protection Issues in Big Data" chaired by Simon Chesterman, with members Jeff Bullwinkel, Aileen Chia, Stephen Deadman and Tan Shong Ye.

1 M Beyer & D Laney, "The Importance of 'Big Data': A Definition", *Gartner* (21 June 2012).

2 UK Information Commissioner's Office, "Big Data and Data Protection" (2014) at paras 21–33.

generated at exponential, uncontrolled rates, resulting from the expansion of the universe of digital devices and sources. Where the phrase "the rise of the machines" once had a futuristic ring to it, today this is brought to life by the Internet of Things – connected and highly programmed objects with a certain standard of intelligence and which generate data on their own and "speaking" to one another "in the cloud". The cloud (or, more accurately, cloud computing) is in itself made possible because of technological advancements which now allow for vast amounts of data to be processed through SuperSpeed microchip processors and stored on ever-shrinking servers.

2 How big is big data really? Let us look at some numbers. In 2012, it was estimated that the digital universe held 2.7 zettabytes (10^{21} bytes = one trillion gigabytes) of data[3] with five exabytes (10^{18} bytes = one billion gigabytes) of data generated every two days.[4] By 2015, 4.9 billion connected devices will be in use; by 2020, there will be more than 25 billion such devices.[5] Indeed, by 2018, it is expected that connected devices in the Internet of Things would generate more than 400 zettabytes annually.[6] To put those numbers in context, it has been said that if a byte was 1 character of text, a zettabyte would be like Leo Tolstoy's "War and Peace" 323 trillion times over.[7] Or assuming one gigabyte could store 960 minutes of music, one zettabyte would store two billion years of music.[8] That is just a little less than the amount of time that multicellular life on earth has been estimated to have existed.[9] That is *big* data indeed.

3 International Data Corporation, "Worldwide Big Data Technology and Services 2012–2015 Forecast" (March 2012).

4 Winterberry Group, "From Information to Audiences: The Emerging Marketing Data Use Cases" (January 2012).

5 Gartner, "Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015" (11 November 2014).

6 Cisco, "Cisco Global Cloud Index: Forecast and Methodology, 2013–2018 White Paper" (4 November 2014).

7 Daily Infographic, "2016: The Year of the Zettabyte" (23 March 2013).

8 Daily Infographic, "2016: The Year of the Zettabyte" (23 March 2013).

9 BBC, "History of Life on Earth" (last updated October 2014).

3 What does one do with so much data? In an information-hungry world, the answer is clear: mine and analyse it. It should be said from the outset that the concept of data analytics is not new. However, the exponential advance of technology (in particular, the Internet of Things) has catalysed the rate at which data is generated. There are now incredibly large data sets ripe for harvesting. Coupled with technology that can extract insights from those data sets, the world is firmly into a paradigm shift. Today, the imperative conversation revolves around *big* data, not *just* data.

4 Yet, the uncharted new lands of big data, big data technology and the cloud can be treacherous ones for an intrepid legal practitioner. It is therefore timely for this paper to discuss some current issues in the big data world, with a focus on privacy and data protection. This paper will cover briefly some obvious benefits and challenges associated with big data. It will then carry a discussion of selected privacy and data protection issues posed by big data that ought to be at the forefront of the legal practitioner's consciousness today, before rounding off the discussion[10] with a case study disclosing the dire need for multi-disciplinary international cooperation in a big data world.

BENEFITS

5 Big data and its associated technologies certainly – and naturally – inspire optimism. The availability of seemingly infinite data sets practically demands the proliferation of largely automated data-mining and predictive analytics. As such, it is incredibly exciting to consider some examples in order to better understand what one can achieve with big data.

Healthcare

6 For one, there are undeniable benefits in the area of healthcare. Arguably the most often cited example is Google Flu

10 See paras 60–73 below.

Trends, initiated in 2008.[11] Essentially, in the course of operating their search engine, Google observed patterns in search queries which coincided with the flu season annually. With this realisation, Google compared such data against publicly available data provided by the US Centers for Disease Control and Prevention, and found that they could estimate the number of people in each US state who had flu-like illnesses based on the search patterns. Such estimates were then shared in real time on the Google Flu Trends website, enabling the public to get a sense of where there might be flu outbreaks and how serious they might be. This was ground-breaking – prior to the advent of big data and data analytics, this sort of analysis (if even possible) would have taken a huge amount of time and effort; with the advance of technology, the collation and crunching of data are now possible in real time, thereby disclosing insights and trends as the situation unfolds.

7 It is immediately apparent that there is tremendous potential for such projects to benefit the human race. The key advantage is speed. It has been known for some time that flu poses a major public health threat to communities, particularly when combined with the phenomena of globalisation and ease of travel. With the ability to harness big data to detect flu trends quickly, one can hope to avert flu pandemics *in toto*. On a smaller scale, such data can be used to predict and prepare for seasonal epidemics; rapid responses can be deployed and the supply of medication channelled to where the demand is highest. Clearly, consumers benefit from the increased likelihood of ready access to medication. Businesses also benefit from the increased ability to manage their supplies and channel their resources in a targeted manner. It is difficult to see what downside, if any, such clever technology might bring.

8 Another textbook example is a study conducted in Kenya on how human travel affects the spread of malaria.[12] By harvesting mobile phone location data from 11,920 cell towers in Kenya, the

11 Google Inc, "Tracking Flu Trends", the Official Google Blog (11 November 2008).

12 A Wesolowski *et al*, "Quantifying the Impact of Human Mobility on Malaria" (2012) 338(6104) *Science* 267 (12 October 2012).

travel patterns of 14,816,521 Kenyan mobile phone subscribers between June 2008 and June 2009 were tracked (based on the daily location of calls or texts made to a cell tower). The data was then compared to statistics reported by health officials of incidents of malaria. The mapping suggested that malaria outbreaks during that period originated from around Kenya's Lake Victoria and spread east towards Nairobi, the capital. With that information, it was evident that the most efficient way to eradicate the malaria epidemic would be to focus on the Lake Victoria region – that is, the source – rather than to spread resources thinly in patching up incidents throughout the country in a piecemeal manner. In the thick of a global healthcare revolution, big data is the vehicle that is setting the human race clearly and firmly on the journey to better health.

Law enforcement and national security

9 For obvious reasons, law enforcement is another area where big data has immense utility. One fairly well-known project is the Next Generation Identification system which the US government has already put in place.[13] This system would reportedly include more than 50 million face images by 2015 and is expected to enable tens of thousands of facial recognition searches daily.[14]

10 To this magnitude of data set, add the increasing sophistication of data analytics technology – for instance, facial recognition technology such as Facebook's "DeepFace" project.[15] Harnessing a data set of four million identified faces taken from the Facebook pages of over 4,000 users, Facebook has created software which can automate the identification of human faces with 97.25% accuracy. This is almost as good as the 97.53% accuracy of human

13 K Chayka, "The Facial Recognition Databases Are Coming. Why Aren't the Privacy Laws?" *The Guardian* (30 April 2014).

14 J Lynch, "FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year" *Electronic Frontier Foundation* (14 April 2014).

15 Y Taigman *et al*, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification" in (2014) *IEEE Conference on Computer Vision and Pattern Recognition* (IEEE, 2014) at 1701.

review and can be said to approximate human performance – but carried out at a fraction of the time.

11 The staggering potential for big data to support law enforcers in protecting the communities that they serve is easily discernible. Law enforcement authorities could readily access and extract an image of a suspect from closed-circuit television ("CCTV") recordings around the vicinity where an offence was committed, run it through a database using high-speed facial recognition technology and *voila*! they would have a lead for the investigation. National security authorities could apply this technology towards counter-terrorism efforts such as running images of visitors seeking to enter the country at the airport against databases in the course of airport screenings in real-time. In a post-9/11 world, few would disagree with the utility of such applications.

Retail

12 Even for individual consumers, big data affords improved accuracy in targeting consumer profiles. Many retailers today mine customer data and statistics to enhance the retail experience for their customers. One of the trail-blazers in harnessing big data and big data technology for retail purposes was Amazon, which started adding a "Customers Who Bought This Also Bought" feature with customised suggestions for individual customers. Indeed, in December 2013, Amazon took it to the next level. It patented a process for "anticipatory shipping"[16] (essentially, a system that predicts what customers might want), to ship products – before customers even place an order. The theory behind this is that by harvesting data such as a customer's previous orders, searches and wish lists, orders can be anticipated, supply channelled and delivery time minimised. While it is not known whether this process has been implemented, the expected utility is clear: with greater accuracy in predicting what customers might want, retailers benefit from increased sales and individual consumers get time

16 G Bensinger, "Amazon Wants to Ship Your Package Before You Buy It" *The Wall Street Journal* (17 January 2014).

savings in more accurate suggestions tailored to their preferences and a better customer experience overall.

CHALLENGES

13 This is all very exciting. Big data's ability to elicit trends and predictions clearly augur so much promise, so much so that one of the most common buzzwords associated with it is "transformative".[17] Yet, it sometimes seems that for every potential benefit that big data promises, there is a corresponding problem posed.

Discrimination, lack of transparency and inaccuracy

14 While one would like to think that much of the information out there in the data universe is what one might call "digital exhaust" and, like its real-world counterpart equally inconsequential, this is not quite accurate. A recent proposed classification suggests the following taxonomy based on the origin of data:[18]

> (a) provided data – directly given by or originating from individuals (for example, when filling out a form);
>
> (b) observed data – recorded automatically and digitally (for example, as recorded on CCTV and processed with facial recognition technology);
>
> (c) derived data – computed from other data (for example, identifying flu outbreak patterns and severity by comparing trends in search queries against available health data);

17 For instance, The White House, Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values" (May 2014), foreword; also E Adler, "Big Data Has the Power to Transform How Businesses Operate, Assuming They Can Harness It" *Business Insider* (6 January 2014).

18 Organisation for Economic Co-operation and Development Working Party on Security and Privacy in the Digital Economy, "Summary of the OECD Privacy Expert Roundtable. Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking" (20 May 2014).

(d) inferred data – produced by applying analytics to data sets and using the correlations identified to predict behaviour and profile individuals (for example, anticipating and shipping retail purchases by consumers even before they have placed an order).

15 Clearly, the way data is viewed needs to be reconsidered. In earlier days, most data would have been in the form of provided data; hence, some effort had to be put into collecting data and creating databases. Today, however, it is indisputable that provided data has been overtaken by observed, derived and inferred data as the means as to how one is being identified and located in the world. At the risk of sounding like a conspiracy theorist, big data is creepily tracking and quantifying everyone, and yet, one often might not even aware of it. Take the ubiquitous mobile phone for instance. Each phone has a unique 15 or 16 digit International Mobile Equipment Identity Number ("IMEI number") which allows for it to be identified on a network. From a technology angle, the moment a mobile phone is switched on, it can be tracked and network service providers can easily identify the individual linked to that mobile phone. However, it is questionable whether individual network subscribers are even aware of this capability built on IMEI numbers or the extent of the data that becomes available to the network service providers by the simple act of turning on a mobile phone.

16 Against this backdrop, what is worse is that the individual is often not aware of how the data is used, how it has been used to make decisions about them and what decisions are actually made about them. With the opaqueness of how predictions are derived and/or inferred, it is usually too late by the time individuals realise that discriminatory decisions have been made against them. A classic illustration of this can be seen in cases involving financial profiling. In 2008, a Kevin Johnson from Atlanta (US) was informed by American Express that the credit limit on his American Express card was being cut from $10,800 to $3,800.[19] One of the reasons

19 T Alloway, "Big Data: Credit Where Credit's Due" *Financial Times* (4 February 2015).

cited was that he had frequented stores patronised by people whom the credit card company considered were credit risks in that they were late in paying their bills. However, Johnson was an entrepreneur with a good credit score and there was actually no real basis for the credit reduction. In this case, Johnson was at least informed and could therefore protest. Although American Express suffered some backlash when Johnson went public with his experience, banks have largely remained coy as to what data points are considered in reviewing and making decisions about its customers.[20] As compared to Johnson's case, in most other cases, the lack of transparency as to how industries, organisations and even governments are applying predictive analytics and using them to make decisions affecting people's lives is much more insidious. After all, one cannot protest what one does not know.

17 Insurance premiums are another example. In 1998, the US car insurers, Progressive, introduced tracking programmes to tailor motor insurance premiums according to some measurable habits of its customers. By agreeing to have a small tracking device installed in their cars, customers could secure discounts on their motor insurance premiums with the magnitude of the discounts depending on how safe a driver the customer was deemed to be, based on the data that the tracking devices recorded.[21] This is innocuous enough, probably because motor insurance is not typically one of those things which would cause one to lose sleep over in the greater scheme of things.

18 Turn, however, to healthcare, where the next big wave has been predicted to hit, and perhaps it would be more apparent why there is cause for concern. Similar to motor insurance premiums, information collected from wearable technology and devices such as wireless health bands can be passed on to insurers who might lower health premiums for customers.[22]

---

20 R Lieber, "American Express Kept a (Very) Watchful Eye on Charges" *The New York Times* (30 January 2009).

21 B Tuttle, "Big Data is My Copilot: Auto Insurers Push Devices That Track Driving Habits" *Time* (6 August 2013).

22 P Olson, "Wearable Tech is Plugging into Health Insurance" *Forbes* (19 June 2014).

19 The concern is that while the reason proffered for tracking such data has ostensibly been for the benefit of individual customers who might secure discounts on their premiums, no one really knows how and what other ways the data might be used for. This is particularly so with the movement towards the "Quantified Self". With the ready availability of sophisticated devices and increasingly intelligent technology connecting them (that is, the Internet of Things), a whole world of data can be generated and tracked about an individual (hence, the "quantified" self). And this all can be done quietly, efficiently and automatically, without an individual ever truly realising how much data is being collected about them. This has been neatly described as the transparency paradox: "Big data promises to use this data to make the world more transparent, but its collection is invisible, and its tools and techniques are opaque, shrouded by layers of physical, legal, and technical privacy by design."[23]

20 To the fact that a lot of data about individuals is being collected in ways that one does not see, add the observation that such data might not be accurate. It must be appreciated that a core characteristic of big data is that it is indiscriminate – it has volume, velocity and variety, but not necessarily accuracy. While big data analytics clearly is able to predict with some accuracy certain trends – and this is done in ways that even technologists do not fully comprehend – there is nevertheless still a question as to how accurate those predictions are, especially where they are premised on layer upon layer of assumptions. This is perhaps one of the key defining features of technology that one would come to realise – that it is often only as intelligible as the parameters used and only as accurate as the data that is put in – and big data proves no exception to that. To that extent, circumspection needs to be exercised in considering the utility of predictions derived and/or inferred from inaccurate big data. Given the lack of transparency of how data was used to arrive at a conclusion, a trend might be predicted and then applied to another situation which might be very different from the first. To then use such predictions in

23 N Richards & J King, "Three Paradoxes of Big Data" (2013) 66 Stan L Rev Online 41 at 42–43.

relation to communities and individuals would undoubtedly result in unfairness and injustice in many cases.[24]

21 One therefore sees that big data's inherent strengths also – ironically – give rise to its greatest flaws. Given the opaque and insidious manner in which discrimination can be perpetuated, there are very real concerns that big data could amplify and exacerbate social inequities already inherent in the world.

Potential for data misuse

22 With the huge data sets now available, a second major area of concern associated with big data can broadly be referred to as that of data misuse. Hot on the heels of the numerous hacking fiascos that have happened in the past year,[25] Ashley Madison, the infamous company which promises to connect members interested in having adulterous liaisons, recently had its website hacked and the personal data of an estimated 32 million users released. With a mother lode of personal data available on the Internet, it was not long before search tools which facilitated quick identification of individuals were created and shared publicly – for instance, the mere input of one's Gmail contact list into the search tool's database to turn up whether (and which of) one's contacts was an Ashley Madison subscriber. Reputational damage is one thing (and indeed, there were reports of suicides by subscribers connected to the leak);[26] increasing one's vulnerability to cybercrime is another (and much more palpable). Interestingly, there were also James Bond-like security concerns. Life being stranger than fiction

24 J Lerman, "Big Data and Its Exclusions" (2013) 66 Stan L Rev Online 55 at 57–59.

25 To name just a couple: the eBay hacking incident between February and March 2014, where about 145 million users had their encrypted passwords, names, addresses, numbers and dates of birth stolen <https://www.ebayinc.com/stories/news/ebay-inc-ask-ebay-users-change-passwords/> (accessed 22 December 2015); and the Sony hacking incident which came to light in November 2014, where information including unique Social Security numbers of around 47,000 employees (and celebrity gossip revolving around some famous actors) were leaked <http://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf> (accessed 22 December 2015).

26 C Baraniuk, "Ashley Madison: 'Suicides' Over Website Hack" *BBC* (24 August 2015).

sometimes, it has been reported that Chinese and Russian intelligence services were using data analytics to combine numerous data sets obtained from cyberattacks with the Ashley Madison one, and cross-reference personal data to "identify and potentially compromise operatives".[27]

23 A more serious example with wide-ranging and critical implications, especially with regard to national security, is the infamous Edward Snowden affair. In mid-2013, a ruckus erupted when it was reported that the US government was conducting secret surveillance on its own citizens. This arose from a leak by a government contractor to news agencies of classified information from the National Security Agency ("NSA"), including that the Federal Bureau of Investigation ("FBI") had obtained a secret order from the Foreign Intelligence Surveillance Court ("FISC") on 25 April 2013. Pursuant to the FISC order, at least one telecoms provider, Verizon, was required to provide the NSA with telephony metadata of communications made by its users both domestically and internationally on an "ongoing daily basis" for three months.[28] When the news reports broke, there was an immediate fallout, both domestically and internationally, with consequences that are still reverberating today (see paragraph 72 below). Other than the vast scope of the order, it was probably also the confidentiality order restraining the telecoms provider from disclosing the request or the court order that triggered the public's wrath. If not for the leak, the public would probably never have known of the secret order, particularly as the order specifically referred to "metadata" for which individual warrants are not required.

24 But while intuitively this incident seems unpalatable, what exactly is the concern here? Some might say that surveillance and gathering of data has always existed as a given in civilised society

27 J Sciutto, "China, Russia Amassing Personal Info Seized in Hacks for Counter-intelligence" *CNN* (2 September 2015).

28 G Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily" *The Guardian* (6 June 2013); see also "Verizon Forced to Hand Over Telephone Data – Full Court Ruling" *The Guardian* (6 June 2013). B Smith, "'In the Cloud We Trust': Brad Smith on the Changing Global Landscape of Information Security" *Microsoft* (12 November 2015), contains an interesting anecdotal description of the FISC.

from the beginning of time, and the only difference today is the extent and ease of such data-gathering; further, upright and law-abiding citizens who have nothing to hide correspondingly have nothing to fear. The answer is that in addition to the fear of data misuse, there is an instinctive discomfort caused by the perceived threat to one's privacy.

PRIVACY

25 At the outset, it must be observed that notwithstanding that the term "privacy" is often bandied around in response to the sharing of data about people, there is a disjunction between what individuals say and what they do in the virtual world. Earlier this year, the following joke went viral on social media:[29]

> Presently, I am trying to make friends outside of Facebook while applying the same principles.
>
> Therefore, every day I go down on the street and tell the passers-by what I have eaten, how I feel, what I have done the night before and what I will do tomorrow night. Then I give them pictures of my family, my dog and me gardening and spending time in my pool. I also listen to their conversations and I tell them I love them.
>
> And it works.
>
> I already have 3 persons following me: 2 police officers and a psychiatrist.

26 While this makes light of how people interact on social media websites such as Facebook, there is irrefutably a grain of truth at the heart of this example. The reality is that people behave differently in the virtual world than they would in real life. Individuals will always profess to strongly value privacy; yet, inhabitants of the virtual world are often more willing to share their private thoughts and views with strangers than expected. To some extent, this throws into disarray the conventional understanding of privacy and what one might reasonably expect to keep private. But what is understood by privacy anyway? When one

29 This joke can be found on Reddit, but having gone viral, many variants and versions of it can readily be found on the Internet <https://www.reddit.com/r/Jokes/comments/3di4e1/facebookin_real_life/> (accessed 4 March 2016).

complains about the threat to privacy, what exactly is it that one is concerned with?

27 Privacy has been referred to as the right not to be disturbed or the right to be let alone. Take, for instance, the US approach to privacy, which arises out of the Fourth Amendment to the Constitution, under which "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" is protected.[30] Privacy in the US has been said to be made up of a patchwork of the following four torts: (a) unreasonable intrusion upon a person's seclusion or solitude, or into his private affairs; (b) public disclosure of embarrassing private facts about an individual; (c) placing one in a false light in the public eye; and (d) appropriation of one's likeness for the advantage of another.[31] However, upon a quick review of this list, it is apparent that the threads linking these four torts together are actually quite tenuous and it is difficult to define a unifying underlying theme to them.[32]

28 Comparatively, across the Atlantic, privacy has a much more entrenched status in the European Union ("EU"). Privacy is enshrined as a fundamental human right under Article 8 of the European Convention on Human Rights, which provides in Article 8(1) that "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[33] The EU further recognises both privacy and data protection as distinct fundamental rights as *per* Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.[34]

---

30 See also The White House, Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values" (May 2014) at p 11.

31 W Prosser, "Privacy" (1960) 48 *California Law Review* 383.

32 For a comprehensive summary, see S Chesterman, *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Academy Publishing, 2014), paras 1.14–1.27, and in particular at para 1.20.

33 Convention for the Protection of Human Rights and Fundamental Freedoms, 213 UNTS 221 (4 November 1950) ("Convention for the Protection of Human Rights and Fundamental Freedoms").

34 Charter of Fundamental Rights of the European Union (2010/C 83/02) ("Charter of Fundamental Rights of the European Union"), first proclaimed on

(*continued on the next page*)

29 While it is easy enough to state as a general proposition that everyone has a right to respect for his or her private and family life, home and communications,[35] the devil is always in the details. Considered in isolation, the concept of privacy is reasonable and laudable; considered in the real world context where it interacts with other conflicting interests such as of "national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others",[36] and it would be appreciated that privacy practitioners have their work cut out for them.

30 Furthermore, there is an impression that the US views privacy from the perspective of "liberty", in that the individual ought to be able to lead a life free from external interference, while the mindset of the EU is founded on the commitment to uphold the sacrosanct ideal of honour or dignity of the individual.[37] In this sense, while it is self-evident that considerations such as the history and culture of a people will always inform a country's approach as to its laws, where privacy as a rights-based concept is concerned, it is arguable that there is little point in seeking to define in a unified and consistent manner the precise bounds of something as amorphous as privacy, particularly in the new world of explosive technological growth.[38] This may go some way towards explaining the friction that inevitably occurs from time to time when the US and the EU laws collide.[39] It is therefore understandable why privacy as a conceptual doctrine has been criticised as lacking coherence.

---

7 December 2000 at Nice, but entered into force pursuant to the Treaty of Lisbon on 1 December 2009.

35 Charter of Fundamental Rights of the European Union Art 7.

36 Convention for the Protection of Human Rights and Fundamental Freedoms Art 8(2).

37 S Chesterman, *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Academy Publishing, 2014) at para 1.17.

38 S Chesterman, *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Academy Publishing, 2014) at paras 1.14–1.27.

39 See paras 60–73 below.

31 Perhaps this author's discomfort with lofty notions of privacy is also attributable to the quintessentially pragmatic Singaporean psyche. Singapore has no statutorily prescribed right to privacy and indeed, privacy as a rational legal concept has not been formally recognised. As recent as August 2015, while acknowledging that recent legislative developments suggest that there is an increasing recognition of the need to protect personal privacy, and noting that in numerous common law jurisdictions, the law of confidence has been extended to accommodate the protection of private information, the Singapore Court of Appeal declined to express a definitive view on whether there should be a right to protection of private information acquired without consent by way of the law of confidence in Singapore.[40]

32 In that case, the parties were husband and wife who were in the midst of divorce proceedings. The wife surreptitiously managed to copy files contained in the husband's notebook computer and this came to light when the wife sought to rely on some of the contents of the notebook computer for the purposes of the divorce proceedings. The husband then commenced a separate action for, *inter alia*, breach of confidence and sought an interim injunction to restrain the use of the information allegedly obtained in breach of confidence. While the matter was settled before the hearing in the Court of Appeal, in its judgment recording the consequential directions given upon the parties' settlement, the Court of Appeal expressed the views as stated above,[41] and further, that the identification of a right to protection of private information under the law of confidence in Singapore ought to be left to be determined at trial in a future case. Meanwhile, Singapore has since 2012 had in place baseline data protection legislation similar in structure to data protection laws globally and arguably has focused on taking a practical approach in seeking to protect personal data by way of data protection laws. Perhaps one interpretation is that while pragmatic Singapore continues to cautiously make sense of the complex landscape of privacy and draw together the tenuous wisps of what the law might consider people to reasonably expect

40 *ANB v ANC* [2015] 5 SLR 522 at [22]–[23].
41 See para 31 above.

of privacy, she has recognised the urgency of having in place data protection laws to address the fundamental concern that people really have – *viz*, potential harm in the event of a misuse of data.

DATA PROTECTION

33 In this Part, the discussion will focus on some of the issues that data protection laws themselves suffer from as a result of the developments in big data and discuss whether they are still fit for purpose in a big data world.

Traditional data protection principles

34 Data protection law today is generally built on what is commonly known as "fair information principles" ("FIPs").[42] While the FIPs are made up of a number of principles, the key pillars of the institution of data protection are purpose specification and use limitation, which can loosely be understood as the "notice and consent" regime.

35 Take, for instance, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[43] ("OECD Guidelines") or the 1995 EU Data Protection Directive[44] built on the former. At the heart of these principles guiding the handling of personal data is the notion that where personal data is concerned, the individual data subject should be informed of the purpose for which his data is collected and used, and that he should be allowed to retain autonomy over how his data is collected and used –

42 Working Group organised by the Oxford Internet Institute, University of Oxford, "Data Protection Principles for the 21st Century" (Rev March 2014) at 3.

43 The Organisation for Economic Co-operation and Development, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (2013 Rev Ed) at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed 22 December 2015).

44 Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (24 October 1995) ("1995 EU Data Protection Directive").

primarily by the mechanism of informed consent (hence, "notice and consent"). However, while it is a truism that some control may be maintained over personal data by notice and consent regimes, in practice it may legitimately be asked how effective they really are. This is very much a result of the disruptive influence that big data and big data technology have on everyday life.

Personal data

36 Traditionally, the type of data which individuals have been motivated to safeguard is data which might identify people personally; anything else which is not apparently classifiable as "personal data" has not generally been protected under data protection laws. However, this is not a realistic mindset in the era of big data. Arguably the most fundamental illusion in today's big data world is that the label of "personal data" is a dichotomous one (that is, information is either personal data or not). The truth is that it is not.

37 Two main observations can be made which might go some way to bring to life the complexity of the concept of "personal data". The first – and possibly the more critical – is that it has gradually come to be realised that the relentless progression of data analytics and technological advancements is such that anonymised or de-identified data is often a temporary state rather than a stable category.[45] As such, the traditional fixes of anonymisation and de-identification are limited in effect in a big data world.[46]

38 A lifetime ago (by technology's standards), it was generally believed that if data is anonymised or de-identified, the data subject would no longer be identified or identifiable, and hence such data would not be considered personal data; not being personal data, the restrictions on disclosure and use would

45 P Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation" (2010) 57 UCLA L Rev 1701 at 1748. See also P Ohm, "Response: The Underwhelming Benefits of Big Data" (2013) 161 U Pa L Rev Online 339.

46 O Tene & J Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics" (2013) 11 Nw J Tech & Intell Prop 239, para 45 onwards.

technically not apply. Hence, organisations and businesses have traditionally relied on anonymisation and de-identification as the portals through which useful data could be safely sent out into the world. However, it has since come to be widely acknowledged that the various techniques of anonymisation and de-identification have their individual weaknesses and varying levels of robustness in truly detaching the data from the person and one now ought to know better than to place faith in them blindly.[47]

39 A classic case study which will illuminate the point involves anonymised data of state employees which was released by a government agency, Group Insurance Commission ("GIC"), into the public domain in the mid-1990s in Massachussetts. The data had been collected when GIC purchased health insurance for those employees and was subsequently anonymised prior to its release by removing most of the "identifiers" pointing to specific individuals (although some information – including ZIP code, date of birth and sex – was still retained). At the time, the Governor of Massachussetts, William Weld, even declared that patient privacy was preserved given that the identifiers had been deleted. This prompted a graduate student, Latanya Sweeney,[48] to go on a quest to identify Governor Weld's own data from that released by GIC. As has been narrated in other literature:[49]

> She knew that Governor Weld resided in Cambridge, Massachusetts, a city of fifty-four thousand residents and seven ZIP codes. For twenty dollars, she purchased the complete voter rolls from the city of Cambridge — a database containing, among other things, the name, address, ZIP code, birth date, and sex of every voter. By combining this data with the GIC records, Sweeney found Governor Weld with ease. Only six people in Cambridge shared his birth date; only three were men, and of the three, only he lived in his ZIP code.

47 Article 29 Data Protection Working Party, "Opinion 05/2014 on Anonymisation Techniques" (10 April 2014).

48 A graduate student then but currently, *inter alia*, the Professor of Government and Technology in Residence at Harvard University and the Director of the Data Privacy Lab in the Institute of Qualitative Social Science at Harvard University.

49 See also P Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation" (2010) 57 UCLA L Rev 1701 at 1719.

> In a theatrical flourish, Dr Sweeney sent the governor's health records (including diagnoses and prescriptions) to his office.

40 That was in the mid-1990s. Twenty years later, it is indisputable that reidentification has only become exponentially easier. It is quite immediately apparent that, once again, big data is the game changer. The efficiency of data analytics technology and the vast data sets (characterised by *volume*, *velocity* and *variety*)[50] out there in the big data world have tremendously increased the likelihood of the reidentification of the individual.

41 Of course, that is not to say that it was previously impossible to reidentify individual persons, the reason being that there is an obvious inverse relationship between privacy and utility of information. Often, in order to reap meaningful results in data analysis, facets of the identity of the individual would need to be retained. It has been pithily observed: "[P]erfect privacy can be achieved by publishing nothing at all–but this has no utility; perfect utility can be obtained by publishing the data exactly as received from the respondents, but this offers no privacy."[51] The most useful data is data about individuals as individuals. In a big data world, there is little utility to be had in data that does not say much about one and hence little incentive for data to be stringently anonymised or de-identified. As such, the risk of reidentification has always been a given. The real point to be made is that with the combination of big data and the constant advancement of data analytics, reidentification requires much less effort and is much more likely to happen than one would realise. Today, reidentification is not simply a hypothetical risk – it is a clear and present danger.

42 The inherently non-private nature and the infamously long memory of the Internet must also be kept in mind. In today's big data world, anonymity is an illusory concept. Technological fixes are no longer the miraculous antidote that they were once thought

---

50 See para 1 above.

51 P Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation" (2010) 57 UCLA L Rev 1701 at 1752, citing S Chawla *et al*, "Toward Privacy in Public Databases" (2005) 2 Theory Cryptography Conf 363 at 364.

to be. Put another way, "personal data" or more fundamentally, data that can identify a person, has taken on a mantle of fluidity due to the incremental effect of loss of anonymity,[52] or what another legal commentator has called the "accretion problem":[53]

> [O]nce an adversary has linked two anonymized databases together, he can add the newly linked data to his collection of outside information and use it to help unlock other anonymized databases. Success breeds further success. Narayanan and Shmatikov explain that 'once any piece of data has been linked to a person's *real* identity, any association between this data and a *virtual* identity breaks the anonymity of the latter.' This is why we should worry even about reidentification events that seem to expose only non-sensitive information, because they increase the *linkability* of data, and thereby expose people to potential future harm. [emphasis in original]

43 Recent history is rife with notable examples where information leaks have resulted in the irremediable exposure of personal identities. Some of these were deliberate – for example, the infamous Ashley Madison hacking scandal mentioned above.[54] Some of these were accidental – take, for instance, the 56 Dean Street clinic contretemps that happened recently in London.[55] On 1 September 2015, the clinic well known for treating patients with the human immunodeficiency virus ("HIV") sent a newsletter to about 780 recipients, in the process inadvertently disclosing their full names and email addresses. Anecdotal evidence indicated that some recipients found out through the incident about the HIV-positive status of acquaintances on the same list; further, it was not difficult to verify and discover even more information about others on the list by, for example, searching the names disclosed in combination with other databases such as Facebook.

44 In a nutshell, with the expanse of the digital universe out there, a little sleuthing work boosted by sophisticated technology

52 O Tene & J Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics" (2013) 11 Nw J Tech & Intell Prop 239 at paras 30–31.

53 P Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation" (2010) 57 UCLA L Rev 1701 at 1746.

54 See para 22 above.

55 J Halliday, D Campbell & J Elgot, "Inquiry Launched After HIV Clinic Reveals Hundreds of Patients' Identities" *The Guardian* (2 September 2015).

can make what would on its own be anonymised or de-identified data into data that can identify a person when viewed in combination with other data sets. It must be borne in mind that a loss of anonymity is – almost by definition – irreversible. For instance, once an individual is known to have the HIV-positive status, that revelation cannot be unlearnt. It is therefore no wonder that one legal commentator has quite memorably (albeit dramatically) said that "[p]owerful reidentification will draw every one of us closer to … our personal 'databases of ruin'".[56]

45 The second observation pertains to the added complication of how personal data interfaces with metadata. Often, when thinking about data, one does not include metadata (or, "data about data"). However, in today's world, this perspective is obsolete. First, it is premised on the fallacy that "personal data" and "metadata" are distinct types of data. This is not always true. Take, for instance, search terms typed into a Google search (for example, "what is big data"). The Uniform Resource Locator ("URL") indicating the destination of the search result would arguably be metadata (for example, https://www.google.com.sg/#q=what+is+big+data). However, the URL would also contain the search term itself. This example is innocuous enough; however, a good number of searches conducted is likely to point towards an identifiable person. One's understanding of what is "data" and what is "metadata" is, much like the understanding of what is "personally identifiable data", often fluid rather than fixed. Much will depend on the context of what one is dealing with.[57]

46 Indeed, the Australian Privacy Commissioner had in a 1 May 2015 decision[58] found metadata to constitute personal information under the Privacy Act 1988 (Cth)[59] ("Privacy Act") and ordered Telstra, a telecommunications provider, to furnish a customer with

56 P Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation" (2010) 57 UCLA L Rev 1701 at 1705.

57 This is explained in greater detail in Brad Turner, "When Big Data Meets Big Brother: Why Courts Should Apply *United States v Jones* to Protect People's Data" (January 2015) 16 NC JL & Tech 377 at 398.

58 *Ben Grubb and Telstra Corporation Limited* [2015] AICmr 35 (1 May 2015).

59 Privacy Act 1988 (Cth) (Act No 119 of 1988) s 6.

his personal metadata in relation to his mobile phone use in accordance with his right of access to the same. Such metadata would include "cell tower logs, inbound call and text details, duration of data sessions and telephone calls and the URLs of websites visited". The customer had argued, *inter alia*, that his identity could reasonably be ascertained from the metadata he was seeking and hence was personal information for the purposes of the Privacy Act. The Privacy Commissioner found that the metadata in question was information about an individual and could be considered to be personal information if the identity of the individual was apparent or could reasonably be ascertained from the information. Although the Privacy Commissioner was of the view that the customer's identity would not necessarily be apparent from some of the metadata, he agreed that the customer's identity could reasonably be ascertained from the information and therefore the metadata was personal information, notwithstanding Telstra's contention that retrieving such metadata would be burdensome and hence the requirement of reasonableness was not satisfied. In this regard, it is worth noting that the Privacy Commissioner was conscious of "the reality of data-linking and that a customer's identity and much more information about them can be established by cross-matching data sets".[60] While Telstra has indicated that it would appeal and the status of the matter is not clear, this decision shows the inherent difficulties involved in trying to neatly pigeonhole information as personal data or otherwise.

47 Again, while the term "personal data" on its face appears quite straightforward, in reality, personal data is a dynamic state. As can be seen, this is just one aspect of the complexity of applying data protection laws to a big data world.

60 This is apparent from the decision – *eg*, *Ben Grubb and Telstra Corporation Limited* [2015] AICmr 35 at paras 73 and 82 – although the quote above which this footnote references was taken from a post-decision writing by the Privacy Commissioner, Timothy Pilgrim (see T Pilgrim, "Timothy Pilgrim: OAIC has a mandate, powers, and is not afraid to use them" (3 September 2015)), where the point is summarised with greater clarity. Note also that this again ties back to the first observation made above at paras 37 to 40.

Notice and consent regimes

48 The next point for discussion is the notice and consent regimes. But first, even before delving into the principles proper, a point needs to be made about human behaviour.

49 The notice and consent regime is constructed on the foundation of informed consent – "informed" typically through the provision of a privacy policy which the individual would "consent" to govern the ways in which his personal data would be handled. However, are people really reading privacy policies in the first place?

50 An interesting experiment was conducted by British gaming company GameStation as an April Fool's Day joke in 2010 when they surreptitiously added the following clause to their standard terms and conditions online:[61]

> By placing an order via this Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant Us a non transferable option to claim, for now and for ever more, your immortal soul. Should We wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamesation.co.uk or one of its duly authorised minions. We reserve the right to serve such notice in 6 (six) foot high letters of fire, however we can accept no liability for any loss or damage caused by such an act.
>
> If you a) do not believe you have an immortal soul, b) have already given it to another party, or c) do not wish to grant Us such a license, please click the link below to nullify this sub-clause and proceed with your transaction.

51 As can be expected, GameStation promptly acquired the souls of more than 7,500 unsuspecting customers by way of fine print. This is not at all surprising given the amount of time required to pore through lengthy privacy policies or terms of use. In 2008, based on assumptions such as that the average individual would encounter about 1,462 privacy policies in a year and it would take him 10 minutes to read each one, two researchers from

61 FoxNews website http://www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls.html (accessed 5 February 2016).

Carnegie Mellon University estimated that it would take an average individual around 30 working days a year in order to read every privacy policy he or she came across.[62] That was back in 2008; today, when the world is so much more connected, the figures would no doubt have to be adjusted upwards. But the point that these examples drive home is this: given the prevalence and length of privacy policies, one has in fact been conditioned not to read privacy policies before accepting them. If so, does it still make sense to adhere to the mantra that acceptance of privacy policies constitutes informed consent so as to absolve organisations of liability?

52 Next, consider this typical scenario which illustrates the point that individuals leak personal data constantly: walking into a mall and being captured by the CCTV recording; making a call at the entrance of the mall and mobile phone information such as IMEI number is recorded by the network service provider; connect to Google on the wireless network provided by the mall to quickly research a product and information relating to the URLs of the websites browsed can be captured. Even if privacy policies exist to apply to each of those collections of data, and even if one could be clearly apprised of those privacy policies, can there be any meaningful consent to speak of?

53 Furthermore, it is arguable that it is simply not practicable for the notice and consent regime to apply to data which may in the first place have been passively disclosed rather than actively collected from the data subject directly – in particular, what one might term "derived" and "inferred" data (with all their underlying layers of assumptions) are fed back into the machinery of big data and added to "provided" and "observed" data.[63] If one is truly a believer in the notice and consent regime, one must acknowledge that the constant evolution of technology now makes big data an uncomfortable fit with the FIPs as traditionally understood.

---

62 A McDonald & L Cranor, "The Cost of Reading Privacy Policies", *I/S: A Journal of Law and Policy for the Information Society*, 2008 Privacy Year in Review issue.

63 See para 14 above.

54 Another common observation is that privacy policies have become complex and often seek to include references to future uses by broad and permissive drafting.[64] The reason for this is yet another glaring inverse relationship: the more defined the ambit of notice and consent, the more compliant with data protection laws but the less utility the data would have. While conventionally the collection and use of data are regulated by tying them to a specific purpose (that is, purpose specification and use limitation) which the individual consents to, in a big data world however, the foremost means by which big data can be harnessed is through repurposing of data collected for new uses. As has been insightfully pointed out by the President's Council of Advisors for Science & Technology, "[the] notice and consent is defeated by exactly the positive benefits that big data enables: new, non-obvious, unexpectedly powerful uses of data".[65] Where a privacy policy is narrowly scoped and consent for re-purposing data is required, innovation and the corresponding benefits to society would understandably be unduly restricted. No wonder there are growing murmurs within the data protection community that the present notice and consent regime is overly strained and no longer meaningful.

55 That is not to say that notice and consent regimes are necessarily outmoded. There have been numerous calls to update the traditional FIPs, for instance, by moving away from data collection and towards data use:[66]

> A revised approach should shift responsibility away from individuals and toward data collectors and data users, who should be held accountable for how they manage data rather than whether they obtain individual consent. In addition, a revised approach should focus more on data use than on data collection because the context in which personal information will be used and the value it will hold are often unclear at the time of collection.

64 Working Group organised by the Oxford Internet Institute, University of Oxford, "Data Protection Principles for the 21st Century" (Rev March 2014).

65 President's Council of Advisors on Science & Technology, "Big Data and Privacy: A Technological Perspective" (May 2014) at 38.

66 Working Group organised by the Oxford Internet Institute, University of Oxford, "Data Protection Principles for the 21st Century" (Rev March 2014) at 8.

56 That said, it appears that the status quo of notice and consent regimes is not in danger of being displaced any time soon, particularly not in the EU. In January 2012, a reform of the data protection laws in the EU was proposed. After three years of laborious discussions (including numerous so-called "trilogue" meetings), on 15 December 2015, the European Commission, European Parliament and the Council finally agreed on the draft texts of two instruments which collectively make up the EU data protection reform package, *viz* the General Data Protection Regulation and the Data Protection Directive.[67] The former is intended to deal with personal data generally (and will replace the 1995 EU Data Protection Directive) while the latter will deal with personal data in the context of law enforcement and criminal justice. In terms of next steps, the texts are expected to be formally adopted by the European Parliament and Council in early 2016 and applied in the EU member states two years thereafter.

57 While it is still early days given that there are further steps to be taken before these texts are enacted as law in the EU, some concerns have already been raised in relation to a number of the key changes to be made. As an example, companies outside the EU which offer goods or services to or monitor the behaviour of the EU data subjects will fall within the reach of the new General Data Protection Regulation.[68] Further, for some infringements of the General Data Protection Regulation, fines of up to 4% of the company's *annual worldwide* turnover can be imposed.[69]

58 More critically, some concerns have also been raised in relation to some of the constants retained under the new General Data Protection Regulation. For instance, with respect to an individual's consent to the processing of his or her personal data, such consent has to be freely given; and where the personal data falls within special categories of sensitive data, such consent must

67 European Commission, Press release on "Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market" (Brussels, 15 December 2015). For the draft texts as they currently stand, see http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE(2015)1217_1/sitt-1739884 (accessed 22 December 2015).

68 Art 3(2) of the draft General Data Protection Regulation.

69 Art 79(3a) of the draft General Data Protection Regulation.

be "explicit".[70] This is precisely the dilemma that big data presents – where arguably the foremost potential of big data lies in the "new, non-obvious, unexpectedly powerful uses of data",[71] to tie the hands of organisations and businesses by way of such consent provisions (particularly where they could be enforced by the sanctions of fines of up to 4% of annual worldwide turnover) is perhaps somewhat unreal.[72] As such, to the extent that the new General Data Protection Regulation is still founded on the notion of "notice and consent", questions can still be raised about its fitness for purpose in the 21st century.

59 On the other hand, it cannot be emphasised enough that however data protection laws are to evolve (even if the move is towards a focus on data use), they need to be deployed in tandem with market forces and technological developments. In the recent years, the expectations of privacy and how individuals interact in the virtual world have been changing as they adjust to this brave new big data world that is still evolving. Historically, laws have often been accused of being slow to change but this is arguably with good reason given that they do not exist in a vacuum but must necessarily react to the real world. In light of the rapid developments in big data and the fact that the conflicting considerations transcend privacy laws, it is crystal clear that concerted efforts must be made for a multi-disciplinary and international response to the threat to individual privacy posed by big data. This will be considered in greater detail in the next Part.

---

70 Arts 7 and 9, and in particular, Art 9(2) of the draft General Data Protection Regulation.

71 See also The White House, Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values" (May 2014) at p 38.

72 See infographic by Fieldfisher LLP on their Privacy and Information Law Blog, "Debunking EU Data Protection Reform" (24 September 2015). See also European Digital Rights, "EU Data Protection Package – Lacking Ambition But Saving the Basics" (17 December 2015), in which it was noted that "[o]ne of the key elements of modernisation, profiling, has not been dealt with thoroughly."

A BRAVE NEW WORLD – TERRITORIALITY AND CONFLICT OF LAWS

60 In a world of fast-shrinking boundaries, the ascendance of big data, big data technology and cloud computing has brought to the forefront cross-border interactions between sovereign states and the complex issues raised in their wake.

61 A neat illustration of these concerns can be seen in a case involving a search warrant served upon Microsoft in a fairly recent landmark case in the US.[73] In December 2013, the US government applied to the US District Court in the Southern District of New York and obtained a search warrant before a magistrate judge. The search warrant was stated to apply to "information associated with a specified [MSN account], that is 'stored at premises owned, maintained, controlled, or operated by Microsoft Corporation …'".[74] To the extent that the said information was within Microsoft's "possession, custody, or control",[75] Microsoft was to disclose it. This would seem straightforward enough. The difference here was that part of the information sought related to a customer's email account and was stored only on a server located in Ireland.

62 Unsurprisingly, Microsoft took the view that that part of the warrant was essentially for the purpose of extraterritorial search and seizure which the US courts were not authorised to issue. Hence, Microsoft applied to quash the search warrant. They were unsuccessful before both the magistrate judge and on appeal in the District Court. Microsoft has appealed further to the US Court of Appeals for the Second Circuit; that appeal is pending. Meanwhile, 12 *amicus curiae* briefs from 28 different technology and media companies, 23 technology and advocacy groups, 35 leading computer scientists,[76] a member of European parliament and the

73 *Re a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation* 13-MJ-2814 (25 April 2014) (SDNY).

74 *Re a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation* 13-MJ-2814 (25 April 2014) (SDNY) at 3.

75 *Re a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation* 13-MJ-2814 (25 April 2014) (SDNY) at 13.

76 B Smith, "'In the Cloud We Trust': Brad Smith on the Changing Global Landscape of Information Security" *Microsoft* (12 November 2015).

Republic of Ireland have been filed in the appeal, all of which support the reversal of the District Court's decision.

63 It is incontrovertible that cloud computing and big data technology are placing severe strain on the law as well as international relations, as sovereign states grapple not only with how data can be handled domestically but in a progressively virtual and political world, how to do so in harmony with other sovereign states and in a business-friendly manner. As one *amicus curiae* brief puts it:[77]

> One reason this case has garnered so much amicus attention is that the district court gave short shrift to an enormously complex issue relating to the power of the US government to compel global companies in an interconnected world to turn over data related to their foreign users, stored in foreign data centers, under the legal control of foreign subsidiaries, with no significant consideration of the international consequences of imbuing the US government with such power.

64 In this case, the obligation to disclose was governed by legislation in the form of the US Electronic Communications Privacy Act of 1986.[78] At first instance before the magistrate judge, amongst the reasons given for the decision, Microsoft was considered to have "possession, custody, or control" over the information;[79] further, in the context of digital information, "a search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer".[80] One of the reasons given by the court was therefore that since no such exposure takes place until the information is reviewed in the US, no extra-territorial search

77 Brief in Support of Appellant, Microsoft, Inc by Apple Inc as *Amicus Curiae* (15 December 2014) at p 1.

78 18 USC (US) §§ 2701-2712.

79 *Re a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation* 13-MJ-2814 (25 April 2014) (SDNY) at 13.

80 *Re a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation* 13-MJ-2814 (25 April 2014) (SDNY) at 13, citing O Kerr, "Searches and Seizures in a Digital World" (2005) 119 Harv L Rev 531 at 551.

had occurred and the warrant did not violate the presumption against extra-territoriality.

65 However, many *amici curiae* held a different view. The problem here was that the information sought was that of the third party individual's and not Microsoft's, and was stored on a server in Ireland. Even from the technologists' perspective, while information may loosely be said to be stored "in the cloud", in reality, it is stored on servers in data centres located remotely rather than locally within jurisdiction. In other words, while data is accessible "in the cloud", it is actually stored in at least one identifiable geographical location or jurisdiction.

66 While a gamut of reasons was put forward in support of Microsoft's appeal, including the technology-based reason above, the principal objection can be broadly summarised as resting on international law concerns as to the effect of enforcing the warrant. There was an existing treaty, the US-EU Agreement on Mutual Legal Assistance dated 25 June 2003 ("EU MLAT"), which was entered into to bridge the differences between the US and the EU data protection standards; by upholding the warrant, the EU MLAT had been bypassed and the sovereignty of states disregarded.[81] Thus, Jan Albrecht, a Member of the European Parliament,[82] noted in his *amicus curiae* brief that "the basic principle of confidentiality of personal data is enshrined as a human right in the European Union Charter on Fundamental Rights", and that the differences between the US and the EU data protection standards were precisely the reason for entering into the EU MLAT – to allow the US law enforcement authorities to obtain personal data located in the EU in compliance with the EU data protection rules. Further, even if the warrant could – for argument's sake – be enforced, it could result in a conflict of jurisdictions as "Microsoft would be required by the warrant, yet it is not permitted under the EU law to

81 Brief of *Amicus Curiae* Jan Philipp Albrecht, Member of the European Parliament (19 December 2014) at p 5.

82 Who also serves as the rapporteur of the European Parliament for the European Commission's proposed General Data Protection Regulation.

transfer the contents of the email account to the US."[83] Indeed, as pointed out by another *amicus curiae*, there may be cases in which domestic laws "may plainly prohibit disclosure and subject local employees to arrest and prosecution",[84] and may put service providers "in the untenable situation of being forced to violate one nation's laws to comply with another".[85]

67 Of course, it might be noted that most if not all of the *amici curiae* had some interest in having the decision below reversed. However, three key points were brought home. First, this is an area where what the law ought to be is inextricably intertwined with the realities of the underlying technologies. Take the example of the practices known as "sharding" or "partitioning",[86] where very large data sets are split across a number of servers (which could conceivably be located in different jurisdictions) for various purposes such as to more evenly utilise storage space and optimise computing power. Where web-based email is involved (such as in this case), it is presently very inefficient to shard or partition the emails contained in the account – at best, the entire customer email database of the corporation might be sharded or partitioned, but individual email accounts would still be stored in one location. However, this is only what is known now. As one progresses through the age of big data, data sets will get larger and there may come a day where sharding or partitioning of customer data will become commonplace or even necessary. Pinpointing the physical location of where data is stored may then become unrealistic or nonsensical.

68 Second, the problem with big data is that its implications cut across practically every sphere of life. From the earlier discussions of privacy and data protection, it can be seen that data protection and, to a more ethereal extent, privacy are key players

83 Brief of *Amicus Curiae* Jan Philipp Albrecht, Member of the European Parliament (19 December 2014) at p 9.

84 Brief in Support of Appellant, Microsoft, Inc by Apple Inc as *Amicus Curiae* (15 December 2014) at p 3.

85 Brief in Support of Appellant, Microsoft, Inc by Apple Inc as *Amicus Curiae* (15 December 2014) at p 9.

86 Brief for *Amici Curiae* Computer and Data Science Experts in Support of Appellant Microsoft Corporation (15 December 2014) at pp 17–21.

thrust into the limelight in the age of big data. However, their age-old nemeses, national security and public safety, are similarly still implicated in this new age. From the latter's perspective, it is understandable why it might be tempting in the Microsoft case to entertain the possibility of an alternative starting point premised on "control", for instance by drawing an analogy to the "possession, custody, or power" requirement[87] (or some variation of it) so often seen in applications for discovery or disclosure – in other words, to begin by asking whether one has some form of control over the data sought. Another variation of this would seek to exert jurisdiction over the data as long as the services were provided within the jurisdiction. While there is much attractiveness in the simplicity of "control", this is also not realistic in the context of the multitude of conflicting interests at play, and to some extent, ignores the physical realities of technology.

69 On the other hand, if the court is not with the US government on this matter, where there is no bilateral treaty or its equivalent in place, there might perhaps be no means of acquiring such data even if national security or public safety interests demand it. While the fair point might be made that this is in fact the status quo in respect of physical evidence (and to that extent, perhaps there is something to be said for consistency), it must be remembered that individuals are today living in an increasingly digital world – a world where cybercriminals may physically be dispersed across geographical jurisdictions while their nefarious activities are conducted furtively, swiftly and above all, virtually, in the dark, murky recesses of the Internet. When there has clearly been a paradigm shift in the way the world works, to insist on fitting present reality into the constraints of traditional concepts is practically Nelsonian. In an ever-globalised world with shrinking borders and in particular where the terrorism threat has never been so present and imminent, this could encourage the establishment of safe havens for cybercriminals and rogue organisations and would be a wholly unsatisfactory state of affairs.

87 *Re a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation* 13-MJ-2814 (25 April 2014) (SDNY) at 13.

70 And of course, even if national security or public safety interests are absent, other interests such as commerce and innovation will always be waiting in the wings.[88]

71 Third, multi-disciplinary, international cooperation is required to even begin to address the problem. Some headway has already been made with international conventions such as the Council of Europe Convention on Cybercrime,[89] which seeks to facilitate, amongst other things, mutual assistance requests in cybercrime matters. And yet, even such measures are not necessarily a panacea for the multitude of issues and conflicting interests in this complex area of law and technology.

72 For instance, for years, US organisations have relied on the so-called "Safe Harbour Privacy Principles", developed by the US authorities[90] after negotiations with the relevant EU counterparts, to transfer data from the EU to the US in compliance with the 1995 EU Data Protection Directive. Indeed, in July 2000, the European Commission had found, *inter alia*, the Safe Harbour Privacy Principles to ensure an adequate level of protection for personal data transferred from the EU to the US organisations. However, in June 2013, a Facebook subscriber living in Austria challenged the position that his personal data would be adequately protected if it were to be transferred to Facebook in the US, particularly in light of the Snowden revelations.[91] As such, he made a complaint to the Irish Data Protection Commissioner, and the matter eventually ended up in the Court of Justice of the European Union ("ECJ"). On 6 October 2015, the ECJ handed down a judgment invalidating the Commission's decision and requiring the Irish Data Protection Commissioner to examine and decide whether the transfer of data

88 See para 54 above.

89 Council of Europe, Convention on Cybercrime in Budapest, ETS No 185 (23 November 2001). On a related note, the draft Data Protection Directive (referred to at para 56 above) will pertain to "the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data" – but as stated, it remains to be seen how effective this will be in practice.

90 Issued by the US Department of Commerce on 21 July 2000.

91 See para 23 above.

of Facebook's European subscribers to the US should be suspended on the basis that an adequate level of protection of personal data is not afforded.[92]

73 To some extent, this decision can be understood in light of the exalted status of an accorded human right that data protection has in the EU jurisprudence.[93] Notwithstanding that, this decision provokes some uncomfortably wide-ranging repercussions, starting with the immediate impact on both the EU and the US organisations which transfer customer data from the EU to the US as an intrinsic part of their businesses. In turn, data protection authorities both in the EU and worldwide will of course also have to consider the implications of this decision in serving the communities that they work in, including to safeguard the interests of citizens while at the same time ensuring that commerce is not stifled. What is certain is that sheer multi-disciplinary international pressure will have to be brought to bear on governments on both sides of the Atlantic in order to arrive at "political, legal and technical solutions".[94] Given the decision, while there are still discrete transfer tools that can still be harnessed on a piecemeal basis,[95] it is absolutely critical for some form of high-level, transatlantic treaty or agreement to be in place as soon as possible such that data flows between the US and the EU can once again resume without fear of disruption.[96] One potential incarnation of

92 Court of Justice of the European Union, Press Release No 117/15 (on judgment in Case C-362/14), Luxembourg (6 October 2015), see http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf (accessed 22 December 2015), and judgment in *Maximillian Schrems v Data Protection Commissioner* Case C-362/14 (6 October 2015), see http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30ddac4c8d4cc5a44d70a4dde1978b429a3.e34KaxiLc3qMb40RchoSaxuRbhfo?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=298223 (accessed 22 December 2015).

93 See para 30 above.

94 Article 29 Working Party, "Statement of the Article 29 Working Party" (Brussels, 15 October 2015).

95 Such as existing practices around standard contractual clauses and Binding Corporate Rules; see also Article 29 Working Party, "Statement of the Article 29 Working Party" (Brussels, 15 October 2015).

96 Article 29 Working Party, "Statement of the Article 29 Working Party" (Brussels, 15 October 2015). As can be expected with this landmark decision,

(*continued on the next page*)

this could be the ongoing work between the US and the EU (even before the ECJ decision) to replace the Safe Harbour Privacy Principles, and perhaps the brightest hope that the US and the EU organisations can hold on to for the time being is that it will be concluded soon and will provide greater certainty in this area.[97]

CONCLUSION

74 From the discussions in this paper, it is self-evident that there are complex privacy and data protection issues thrown up in the wake of big data. Clichéd as it may be, there are simply no easy answers as technology evolves faster than its attendant consequences can be identified.

75 That said, one thing is for sure: big data is here to stay. Given that the game has changed and there is no going back, it is submitted that simply transposing the existing framework(s) of privacy and data protection laws to a whole new world of big data is but a short-term approach which will prove to be unsustainable in the long run. In particular, one must question whether and to what extent the notice and consent regime, which might be said to be a construct of (literally) the last century, is still viable and fit for purpose today.

76 At the same time – and almost as if it is not enough that privacy and data protection laws are already sufficiently complex – market forces and technological advancements will shape human behaviour more significantly and faster than laws can. For instance, it cannot be denied that this is an area which is especially partial to the influence of politics and economics. Newspapers all over the world recently reported on the Trans-Pacific Partnership Agreement ("TPP") entered into by the US, Australia, Brunei,

ripples of discussion as to the repercussions have been echoing all over the world since. For another perspective on the same issue, see also a post on Microsoft's blog by Brad Smith, Microsoft's President and Chief Legal Officer on "The collapse of the US-EU Safe Harbor: Solving the new privacy Rubik's Cube" (20 October 2015).

97 See the statement issued by the UK Information Commissioner's Office, "ICO Response to ECJ Ruling on Personal Data to US Safe Harbour" (6 October 2015).

Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam in October 2015.[98] While the TPP covers a broad range of areas of economic significance for the participating countries, it is noteworthy that the TPP has been touted to facilitate cross-border data flow as well.[99]

77 Yet, one cannot help but wonder whether the existing patchwork of international agreements and treaties[100] with its varying levels of protection across parts of the globe might – at least in some instances – complicate rather than help matters. While it cannot be gainsaid that individual agreements and treaties are steps in the journey along which slow and steady progress has been made, today more so than ever as individuals feel the scourges of cybercrime and terrorism nipping at the heels, the quest for the holy grail of global harmonisation has arguably never been more imperative.

78 While one needs to have faith that multi-disciplinary international cooperation can be the best solution that the human race has in shaping the privacy and data protection experience in a big data world, one can only hope that it will not be a long time coming in a world where technology evolves at the speed of light while the law continues to be ploddingly slow to change.

---

98 The Trans-Pacific Partnership Agreement ("TPP") is expected to be ratified and implemented by all participating countries within two years of its signing.

99 For instance, see Office of the US Trade Representative, Executive Office of the President, TPP fact sheet on "Ensuring a Free & Open Internet" and the summary of ch 14 of the TPP on Electronic Commerce on the official Medium blog of the Office of the US Trade Representative (5 November 2015).

100 See also paras 60–73 above.

Distributing the Economic Benefits of Databases: New Wine, New Bottles

Arising from the Internet of Things and the increasing capability of technology to record, store and organise information, the world is well and truly entering the age of big data. This presents both exciting opportunities and daunting challenges. One of the most pressing questions to be confronted is how the economic benefits of and rights to electronic databases ought to be allocated in order to allow big data to fulfil its vast potential. The patent and copyright regimes that have defined intellectual property law thus far seem ill-suited to provide a satisfactory answer. So too a *sui generis* approach attempted by the European Union. It is then time to think outside the box. To this end, this paper borrows perspectives from competition law, the tort of unfair competition and the economic analysis of law.

Paul **CHAN***
LLB (Hons) (National University of Singapore), LLM (Harvard); Assistant Registrar, Supreme Court of Singapore.

INTRODUCTION

1 The introduction of the printing press by Gutenberg circa 1440 changed the world. Contrary to popular belief, however, this was not because moveable type was invented then or indeed by him; printing technology has been in fairly widespread use in China since the Song Dynasty and in the Korean Peninsula since the Goryeo Dynasty.[1] In this regard, the French sinologist Étiemble was

* The author expresses his deepest appreciation to Tanya Aplin, Yeong Zee Kin and Wong Baochen for their comments on a working draft of this paper. Some of the points made in this article were also discussed by the panel on "Intellectual Property Issues in the Internet of Things and Big Data" chaired by Stanley Lai SC with members Tanya Aplin, Paul Goldstein, Corrine Tan and George Wei.

1 A Briggs & P Burke, *A Social History of the Media: from Gutenberg to the Internet* (UK: Cambridge, 3rd Ed, 2009) at pp 15–23 and 61–73.

right to observe that "Europe once borrowed something from China".[2]

2 Nevertheless, it is true that Gutenberg ushered in a worldwide revolution by introducing printing to Europe. His truly epochal contribution was to improve the basic design of the printing press to an extent that allowed for the economical reproduction of books. Prior to Gutenberg's introduction of the printing press, the duplication of manuscripts in Europe was time-consuming and laborious, performed only out of necessity. It was done in the main by monks who painstakingly copied religious documents word for word.[3] Upon the introduction of Gutenberg's printing press, entrepreneurs saw an opportunity and quickly acted as the antiquated equivalent of the modern publisher (they were known as "stationers"). They established guilds, acquired works from authors and organized the printing and sale of books in volumes hitherto unheard of.[4] In effect, Gutenberg's printing press created new industries and, to borrow a modern phrase, "disrupted" many others.[5] To facilitate the growth of these industries, the modern law of copyright was conceived.

3 The world is confronted today with an innovation that promises to be just as revolutionary and profound. In January 2014, the US government commissioned a study examining "how big data will transform the way we live and work and alter the relationships between government, citizens, businesses, and consumers".[6] The report pithily concluded that "[b]ig data technologies will be

2 R Étiemble, *L'Europe chinoise* (Paris: Gallimard, 1988-1989). Translated into Chinese as *Zhongguo wenhua xichuan ouzhou shi (History of the Cultural Transmission from China to Europe)*, Geng Sheng (trans), (Shangwu yingshu guan, Beijing: 2000) at p 34. (As cited by Ke Shao, "*An alien of copyright? A reconsideration of the chinese historical episodes of copyright*" (2005) 4 IPQ 400 at 403.)

3 K Garnett, G Davies & G Harbottle, *Copinger and Skone James on Copyright* (Sweet & Maxwell, 16th Ed, 2011) at para 2-09.

4 W Cornish, D Llewelyn & T Aplin, *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* (Sweet & Maxwell, 8th Ed, 2013) at para 10-01.

5 C Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail* (Harvard Review Press, 2013).

6 Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values" (May 2014), foreword.

transformative in every sphere of life".[7] This is no hyperbole, nor a voice in the wilderness. Indeed, it has been variously said that big data "marks an important step in humankind's quest to quantify and understand the world".[8] Others expected it to "reveal the buried treasures in the bit stream of life"[9] and "make the invisible visible".[10] The leaders of big data will have the "ability to suspend disbelief of what is possible, and to create their own definition of possible".[11] In short, big data will change the world as one presently knows it.

4 Of course, the deliberate, conscientious collection and analysis of data is not unprecedented. History bears witness to the societal benefits and progress derived by dint of record-keeping and statistical scrutiny.[12] Big data, nonetheless, promises to be different. The volume at which the collection and organization of data is done today allows for insights that have not hitherto been possible. Indeed, "[t]he quantitative change has begun to make a qualitative difference."[13] Thus, big data is not merely more of the same. Not unlike the difference between copying and printing, big data is qualitatively different in nature from previous attempts to collect and study empirical information.

---

7 Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values" (May 2014), foreword.

8 V Mayer-Schönberger & K Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (London: John Murray, 2013) at p 17.

9 C Borgman, *Big Data, Little Data, No Data* (Massachsetts: The MIT Press, 2015) at p 3.

10 S Lohr, *Data-ism* (Oneworld, 2015) at p 7.

11 R Thomas & P McSharry, *Big Data Revolution: What Farmers, Doctors and Insurance Agents Teach Us About Discovering Big Data Patterns* (UK: Wiley, 2015) at p 6.

12 See, for example, Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values" (May 2014) at p 1:

> Since the first censuses were taken and crop yields recorded in ancient times, data collection and analysis have been essential to improving the functioning of society. Foundational work in calculus, probability theory, and statistics in the 17th and 18th centuries provided an array of new tools used by scientists to more precisely predict the movements of the sun and stars and determine population-wide rates of crime, marriage, and suicide. These tools often led to stunning advances.

13 "Data, Data Everywhere: A Special Report on Managing Information" *The Economist* (25 February 2010).

5 As promising as big data is, still more daunting are the challenges that big data presents. As the US government noted:[14]

> Aside from how we define big data as a technological phenomenon, the wide variety of potential uses for big data analytics raises crucial questions about whether our legal, ethical, and social norms are sufficient to protect privacy and other values in a big data world. Unprecedented computational power and sophistication make possible unexpected discoveries, innovations, and advancements in our quality of life. But these capabilities, most of which are not visible or available to the average consumer, also create an asymmetry of power between those who hold the data and those who intentionally or inadvertently supply it.

One of the greatest questions confronting the age of big data – as it did the age of printing – is how the economic benefits of electronic databases ought to be protected. After all, a key feature of big data is the collection, storage and arrangement of information in the form of databases. In this area, two perennial interests collide:

(a) the need to encourage the continual generation of original content; and

(b) the need to maximise the full potential of the same content by allowing it to be liberally shared.

Typically, the challenge of resolving questions of this nature falls to intellectual property law.

6 The intellectual property world today is dominated by the patent and copyright paradigms, founded upon the principles agreed at the Paris and Berne Conventions of 1883 and 1886 respectively. As is well known, these principles were designed "[t]o promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries".[15] Conceivably, big data and databases may qualify both as science and "useful arts". Indeed, under Singapore law, databases are currently protected as literary

14 Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values" (May 2014) at p 1.

15 The US Constitution Art I, s 8, cl 8.

works under copyright law.[16] However, many authors have observed that databases do not sit comfortably with these regimes.[17]

7 This paper speaks to these themes in depth. The part immediately following will provide a brief explanation of big data,[18] if only to serve as a launch pad for the discussion to follow. Thereafter a summary on how traditional intellectual property frameworks are ill-suited to govern the distribution of economic rights to databases and touch upon the European Union ("EU") Database Directive,[19] an initiative to create a bespoke regime for databases. As these areas have been discussed extensively elsewhere, this paper will only go into such depth as is necessary to appreciate the need for a new approach to the allocation of economic benefits of databases. The penultimate part will then explore new possibilities – new bottles – for a different approach.[20] This paper does not provide the panacea, if one exists. Rather, the immediate and modest aim is simply to provide novel perspectives by borrowing principles from competition law (or antitrust), the tort of unfair competition and the economic analysis of law. It may

16 Under s 7A of the Copyright Act (Cap 63, 2006 Rev Ed), a database falls within the definition of "compilation in any form". A "compilation", in turn, is defined as compilations or table consisting wholly or partly of "relevant materials or parts of relevant materials" or data other than "relevant materials or parts of relevant materials". "Relevant material" means a work, including a computer program, a sound recording, a cinematograph film, a published edition of a work, a television or sound broadcast, a cable programme and certain performance recording.

17 See, for instance, P Baron, "Back to the Future: Learning from the Past in the Database Debate" (2001) 62 OHSLJ 879; J Reichman & P Samuelson, "Intellectual Property Rights in Data?" (1997) 50 VNLR 51; J Reichman, "Legal Hybrids Between the Patent and Copyright Paradigms" (1994) 94 Colum L Rev 2432; J Lipton, "Balancing Private Rights and Public Policies: Reconceptualizing Property in Databases" (2003) 18 Berkeley Tech L J 773; D Lim, "Re-defining the Rights and Responsibilities of Database Owners under Competition Law" (2006) 18 SacLJ 418 and T J Tan, "New Law for Compilations and Databases in Singapore?" (2012) 24 SAcLJ 745.

18 See paras 8–15 below.

19 Directive 96/9/EC of the European Parliament and of the Council on the legal protection of databases (11 March 1996) ("EU Database Directive"). See paras 16–33 below.

20 See paras 34–52 below.

be that no solution can ultimately be found in any of these areas; it will nevertheless suffice to demonstrate that there are enticing possibilities beyond the patent-copyright paradigms.

BIG DATA, BIG DEAL

8 When the film "Minority Report" was released in 2002, the premise seemed far-fetched. Set in Washington DC in the year 2054, it featured a specialised police unit known as "PreCrime" which sets out to apprehend potential criminals based on foreknowledge provided by three psychics (called "precogs"). As it turned out, the film was ahead of its time by only a decade, not a half-century. Today, predicting the site of future crimes has left the realm of science fiction and has entered reality. Many cities across the US now use a technique known as predictive policing to forecast where crimes or unlawful altercations may possibly occur.[21] However, in place of the fictional precogs is a computer program called "PredPol"; instead of psychic ability, big data.

9 The mission of PredPol is simple but lofty – place police officers at the right time and location to give them the best chance of preventing crime.[22] It does this by digitising millions of past police reports, stretching back many years.[23] Three data points are then extracted: type, place and time of crime. Thereafter, the software applies a unique algorithm based on criminal behavior pattern to produce marked-up maps for police officers. These maps are marked-up with small red boxes, each about half the size of a city block, which indicate the high-risk areas. By policing the areas represented by these boxes during regular patrols, it was noticed that crime rates dropped, sometimes dramatically, in many American cities.[24] One senior police officer opined that "the model

21 E Huet, "Server and Protect: Predictive Policing Firm PredPol Promises to Map Crime Before It Happens" *Forbes* (11 February 2015).

22 PredPol, "About Predictive Policing" <http://www.predpol.com/about> (accessed 29 October 2015).

23 T Clark, "How Predictive Policing is Using Algorithms to Deliver Crime-Reduction Results for Cities" *Route Fifty* (9 March 2015).

24 PredPol, "Scientifically Proven Field Results" <http://www.predpol.com/results/> (accessed 29 October 2015). For instance, it was recorded that as of 1 March

(*continued on the next page*)

was just incredibly accurate at predicting the times and locations where these crimes were likely to occur".[25]

10 Predpol is but one of countless examples in which big data has been used to transform an industry.[26] The origins of the term "big data" are not altogether clear.[27] It appears that the term may have been first used before the year 2000 in various contexts unrelated to the phenomenon.[28] The favoured attribution of the use of the term, as one now understands it, is to Mashey, former Chief Scientist at Silicon Graphics, an American manufacturer of high-performance computing solutions. In that position, he propounded upon the concept in order to promote Silicon Graphics products in many talks he gave to different groups in the 1990s. Some of the presentation slides he used are still captured on the internet including one entitled "Big Data … and the Next Wave of InfraStress".[29]

11 More important than its origins is its meaning. There are typically two ways in which big data is understood – one with regards to its *form* and the other with regards to its *effect*. As to the

---

2014, the Richmond, California Police Department saw a 21% drop in violent crime, a 28% decrease in property crime, a 50% drop in residential burglaries and a 34% decrease in vehicle theft as compared to the same period the previous year.

25 PredPol, "Scientifically Proven Field Results" <http://www.predpol.com/results/> (accessed 29 October 2015).

26 R Thomas & P McSharry, *Big Data Revolution: What Farmers, Doctors and Insurance Agents Teach Us About Discovering Big Data Patterns* (UK: Wiley, 2015). Thomas and McSharry covers nine different industries which have been transformed by big data: farming, medicine, insurance, retail and fashion, customer service, intelligent machines, government, corporations, and weather and energy. There are many more such examples.

27 See, for instance, S Lohr, "The Origins of 'Big Data': An Etymological Detective Story" *New York Times* (1 February 2013) and F Diebold, "A Personal Perspective on the Origin(s) and Development of 'Big Data': The Phenomenon, the Term and the Discipline" *PIER Working Paper 13-003, University of Pennsylvania* (26 November 2012). See also G Press, "A Very Short History of Big Data" *Forbes* (9 May 2013) for a chronological listing of the major milestones in the history of big data.

28 See F Diebold, "A Personal Perspective on the Origin(s) and Development of 'Big Data': The Phenomenon, the Term and the Discipline" *PIER Working Paper 13-003, University of Pennsylvania* (26 November 2012).

29 See J Mashey, "Big Data … and the Next Wave of InfraStress" (25 April 1998).

former, big data is famously characterised by three Vs: volume, velocity and variety.[30] All three emphasise the defining characteristic of big data – the magnitude of the data – from different perspectives. Volume refers to the amount of data stored, organised and analysed, velocity illustrates the speed at which such processes are performed, and variety the different types of raw data or information available as well as the different sources from which such data and information may be captured. In essence, big data is "high-volume, high-velocity, and/or high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight, decision making, and process optimization".[31]

12 Globally, nobody is really able to keep track of how much data is generated daily.[32] However, International Business Machines Corporation (more commonly known as "IBM") famously reckoned that the world creates 2.5 quintillion bytes of data every day and that 90% of the data in the world today was created in the last two years alone.[33] Conceptually, this is difficult to imagine. It may be easier to grasp the "bigness" of big data by considering the following. Every *minute*, 48 hours' worth of new video is uploaded onto YouTube, 34,722 "likes" are recorded on Facebook and 571 new websites are created around the world.[34] In *one hour*, Walmart captures more than one million customer transactions from its

30 D Laney, "3D Data Management: Controlling Data Volume, Velocity and Variety" *Meta Group Research Note* (6 February 2001). Note that there are many others who have added additional "V"s, such as veracity, variability, visualisation, value, validity and viability, *etc*. However, typically, these additional Vs do not describe the magnitude (or "bigness") of big data. Rather, they are aspiration qualities desired of all data; in that light, they do not aid to define big data. See also E Dumbill, "Volume, Velocity, Variety: What You Need to Know about Big Data" *Forbes* (19 January 2012).

31 M Beyer & D Laney, "The Importance of 'Big Data': A Definition" *Gartner* (21 June 2012).

32 M Wall, "Big Data, Are You Ready for Blast-off?" *BBC News* (4 March 2014).

33 IBM, "What is Big Data?" <http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html> (accessed 29 October 2015).

34 D Neef, *Digital Exhaust: What Everyone Should Know About Big Data, Digitization, and Digitally Driven Innovation* (Pearson, 2015) at p 10.

point-of-sale systems.[35] *Every day*, more than 180 billion emails are sent globally and the amount of new data entering the internet is 70 times larger than the entire collection in the Library of Congress.[36] It is estimated that 70% of all data currently generated is done so outside of the United States and by 2020, Asia will generate more data than the United States and Western Europe combined.[37]

13 However, understanding big data from the perspective of its form, impressive as it may sound, is deficient in one aspect – it does not quite elicit how big data is different in kind, and not just size, from previous attempts to collect data. Big data is, after all, not merely more data. As a result, some authors have preferred to focus on the *effect* of big data. In this regard, one predominant point that has been variously made is this: big data provides unique insights, analysis and, ultimately, value that may not be possible to extract with smaller datasets.[38] Put another way, "[t]he change of scale has

35 D Neef, *Digital Exhaust: What Everyone Should Know About Big Data, Digitization, and Digitally Driven Innovation* (Pearson, 2015) at p 10.

36 D Neef, *Digital Exhaust: What Everyone Should Know About Big Data, Digitization, and Digitally Driven Innovation* (Pearson, 2015) at p 9.

37 D Neef, *Digital Exhaust: What Everyone Should Know About Big Data, Digitization, and Digitally Driven Innovation* (Pearson, 2015) at p 10.

38 D Neef, *Digital Exhaust: What Everyone Should Know About Big Data, Digitization, and Digitally Driven Innovation* (Pearson, 2015) at p 17. Note that Neef names three other effects of big data, namely:

(a) big data underpins digital advertising and customised individual marketing;

(b) big data creates a market for harvesting and selling customer data; and

(c) big data supports supply chain and industrial services efficiencies.

These are indisputably important. However, these effects are either examples of or ultimately follow from the predominant point that big data creates new value not possible with smaller datasets. Another effect of big data postulated by Mayer-Schönberger and Cukier, is that the basis of individual decision-making, business strategies and government policies need no longer be causality but correlation: V Mayer-Schönberger & K Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (London: John Murray, 2013) at pp 50-72. This view is controversial. For a broad overview of this debate, see S Lohr, *Data-ism* (Oneworld, 2015) at pp 103-121. For a specific example of the failure of relying solely on correlation, see D Lazer *et al*, "The Parable of Google Flu: Traps in Big Data Analysis" (2014) 343 *Science* 1203.

led to a change of state. The quantitative change has led to a qualitative one".[39]

14 Consider the Predpol example. The success of Predpol relies on information that was both "born analog" (such as hardcopy police reports filed, over decades, by hundreds of police officers) and also information "born digital", (such as police reports that are currently submitted over a computer software or by email or information captured digitally). Individually, each piece of information provides no discernible pattern. They were, after all, generated or captured for a different reason. Police reports, for example, were written to give an account of what happened in each specific criminal activity. However, taken holistically, these hundreds and thousands of data points allow a unique algorithm to be formulated which, in turns, helps to identify the sites of possible future criminal activity. The quantitative change in the number of data points have therefore led to a qualitative change from crime reporting to crime forecasting.

15 To the uninitiated, big data may appear to be as poor or unreliable a basis for decision-making as intuition. Insofar as such sentiments are based on an inherent distrust of data and statistics, they are increasingly untenable.[40] While big data does give rise to legitimate concerns,[41] it cannot be gainsaid that the phenomenon is

---

39 V Mayer-Schönberger & K Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (London: John Murray, 2013) at p 6. See also S Lohr, *Data-ism* (Oneworld, 2015) at p 7:

> I think of this as the deeper meaning of Moore's Law. In a technical sense, the law, formulated by Intel's cofounder Gordon Moore in 1965, is the observation that transistor density on computer chips doubles about every two years and that computing power improves at that exponential pace. But in a practical sense, it also means that seemingly *quantitative* changes become *qualitative*, opening the door to new possibilities and doing new things.

40 The Economist observes that "data-mining has a dubious reputation. 'Torture the data long enough and they will confess to anything,' statisticians quip": "Data, Data Everywhere: A Special Report on Managing Information" *The Economist* (25 February 2010).

41 See, generally, D Neef, *Digital Exhaust: What Everyone Should Know About Big Data, Digitization, and Digitally Driven Innovation* (Pearson, 2015) at pp 215-250 and V Mayer-Schönberger & K Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (London: John Murray, 2013) at

(*continued on the next page*)

here to stay. Governments have embraced big data to drive public policy,[42] firms are using it to forge business strategies and new industries have emerged from it. It can be safely surmised that the use of big data has already affected a large portion of the world's population. It will also continue to be "the focus of economic activity for the foreseeable future" and "[t]here will be significant winners and significant losers, both in the business realm and in society as a whole".[43] The determination of such winners and losers will in no small measure be informed by the type of regime used to distribute the economic benefits of databases.

SQUARE PEGS, ROUND HOLES

16 Given that the patent and copyright paradigms have dominated the intellectual property landscape in the last century, it is natural that regard must first be had to them. If the law of patents and copyright are able to appropriately protect the economic rights to big data, there is little need to look elsewhere. As intimated earlier,[44] where the practice of big data is concerned, one of the most difficult issues is in allocation of the economic benefits of databases – after all, the collation, storage and organisation of large volumes of data is the hallmark of big data. To collect and study thousands of police reports, google entries or the movement of stock prices is a costly endeavour which could be

pp 150-170. For concerns relating to privacy specifically, see P Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57 UCLA L Rev 1701 and P Ohm, "Response: The Underwhelming Benefits of Big Data" (2013) 161 U Pa L Rev 339.

42 The cities involved in the use of big data and open data in one way or another to create "smart cities" include Suwon (South Korea), Stockholm (Sweden), Seoul (South Korea), Waterloo, Ontario (Canada), Taipei (Taiwan), Mitaka (Japan), Glasgow (Scotland, UK), Calgary, Alberta (Canada), New York City (USA), Tehran (Iran), Amsterdam (Netherlands), Barcelona (Spain) and Singapore.

43 D Neef, *Digital Exhaust: What Everyone Should Know About Big Data, Digitization, and Digitally Driven Innovation* (Pearson, 2015) at p 27.

44 See para 5 above.

fatally undermined by piracy.[45] Yet, it is unclear how databases may be protected.

17 To facilitate the foregoing discussion, it may be useful to establish a common, working understanding of databases. Many formal definitions have been attempted.[46] In general, it may simply be said that a database is a collection of information or data. For the purposes of this paper which deals with big data, such a collection is almost always stored in electronic form, which allows an end user to organize and manipulate the underlying data in a variety of ways. It has been suggested elsewhere that a database is comprised of two parts: the structure and the content.[47] This distinction underpins the European Commission Directive on the legal protection of databases,[48] to which the discussion will turn to shortly.

Patent

18 The discussion turns first to consider the law of patents. A patent is a right granted by the State to an inventor to exploit an invention, to the exclusion of others, for a period. The social justifications in allowing the exercise of such rights are generally

45 This issue was discussed in D Lim, "Re-defining the Rights and Responsibilities of Database Owners under Competition Law" (2006) 18 SacLJ 418 at 419–420, as follows:

> It is obvious enough that databases do not come about by themselves. They are the products of much skill, talent and hard work. Substantial investment of money and professional expertise are needed to ensure that database content is comprehensive and accurate … Without legal or technological restraints, free riders would be able to access and sell competing database products at substantially lower prices and in greater quantities than an undertaking saddled with massive developmental and marketing costs … 'parasitical' second comers could drive [the intellectual property rights owner] out of business and thus depress the market for innovative future compilations.

46 See, for instance, the EU Database Directive Art 1(2), which states "[f]or the purposes of this Directive, 'database' shall mean a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means."

47 K Garnett, G Davies & G Harbottle, *Copinger and Skone James on Copyright* (Sweet & Maxwell, 16th Ed, 2011) at para 18-02.

48 The EU Database Directive.

twofold. First, the law of patents mandates the full disclosure of all steps required for performance of the invention under protection. This, in turn, serves two purposes: it allows others to benefit from the invention for non-infringing purposes during the subsistence of the patent and allows them to benefit from the invention wholly after the expiry of the patent.[49] Secondly, the regime provides economic impetus for inventors to continue to create and innovate. Although the specific requirements of patent law differ from jurisdiction to jurisdiction, there are three almost universal conditions found in most countries around the world:[50]

(a) the invention must be new;

(b) it involves an inventive step; and

(c) it is capable of industrial application.

19 Although databases are in many countries protected by the law of copyright rather than patents, it is not beyond the realm of possibilities for databases to be a patentable subject matter. The concept of an invention under the Agreement on Trade-related Aspects of Intellectual Property Rights[51] ("TRIPS") is a fairly

49 The rationale for granting a patent was explained by Lord Hoffmann in *Kirin-Amgen Inc v Hoescht Marion Roussel Ltd* [2004] UKHL 46 (at [77]) thusly:

> An invention is a practical product or process, not information about the natural world. That seems to me to accord with the social contract between the state and the inventor which underlies patent law. The state gives the inventor a monopoly in return for an immediate disclosure of all the information necessary to enable performance of the invention. That disclosure is not only to enable other people to perform the invention after the patent has expired. If that were all, the inventor might as well be allowed to keep it a secret during the life of the patent. It is also to enable anyone to make immediate use of the information for any purpose which does not infringe the claims. The specifications of valid and subsisting patents are an important source of information for further research, as is abundantly shown by a reading of the sources cited in the specification of the patent in suit.

50 For instance, these conditions are found in s 13(1) of the Patents Act (Cap 221, 2005 Rev Ed), s 1(1) of the UK Patents Act 1977 (c 37), §§ 100–104 of 35 USC (US) and Art 52 of the European Patent Convention (15th Ed, October 2013).

51 Agreement on Trade-related Aspects of Intellectual Property Rights in Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization signed in Marrakesh, Morocco on 15 April 1994.

expansive one; it includes both product inventions as well as well as process inventions.[52] Presumably, a database may constitute a process invention. Interestingly, in order to conform to TRIPS, the Singapore Parliament deleted a provision which had previously declared "the presentation of information" as non-patentable.[53] The phrase "presentation of information" of course includes databases. It appears then that the Singapore government was cognizant of the possibility that the selection, compilation and arrangement of information in the form of databases were patentable processes under TRIPS and the previous provision making databases non-patentable would then be inconsistent with Singapore's obligations under TRIPS.[54]

20 Definitional issues aside, the attraction of using patent law to protect databases is not far to find. Foremost is the fact that, as mentioned earlier, the patent system is also an information system – full and frank disclosure is required of all steps necessary to make the invention operable. This is particularly significant where databases are concerned. The full value of a database is often only exploited incrementally; inventor upon inventor may find different uses for the same set of data or the database may be refined over time. Indeed, in this area, "innovation is incremental or cumulative

52 Article 27(1) of the Agreement on Trade-related Aspects of Intellectual Property Rights reads:

> [P]atents shall be available for any inventions, whether products or processes, in all fields of technology, provided that they are new, involve an inventive step and are capable of industrial application ... [P]atents shall be available and patent rights enjoyable without discrimination as to the place of invention, the field of technology and whether products are imported or locally produced.

53 The original s 13(2) of the Patent Acts 1994 (Act 21 of 1994) read:

> It is hereby declared that the following (among other things) are not inventions for the purposes of this Act, that is to say, anything which consist of:
>
> ...
>
> (*d*) the presentation of information,
>
> ...

54 See, A Kang *et al*, *A Guide to Patent Law in Singapore* (Sweet & Maxwell, 2nd Ed, 2009) at para 3.2.8. Whether databases comply with the other requirements of patent law is a different question and remains unresolved.

in nature".[55] Full disclosure of the steps leading up to the creation or use of the database allows others to study the database during the validity of the patent so that the database may be exploited immediately upon expiry of the patent. Further, full disclosure also allows others to verify the provenance and pedigree of the database. This is critical for data reuse.[56]

21 That said, using patent law to protect databases is not without difficulties. Most obvious is the requirement of novelty. The legal test of novelty may be somewhat convoluted but it essentially boils down to an investigation of whether the invention had already been made public.[57] For information to be considered public, the information must be sufficient to enable a person skilled in the art to put the innovation into practice, applying the common general knowledge of the craft.[58] In other words, would one data scientist be able to recreate the database composed by another data scientist, given publicly available information? Since databases are often created by collating and organising information that is already publicly available, the requirement of novelty is not an easy hurdle to cross.

22 Even if this obstacle is overcome in certain big data practices, it may only be because of an application of subjective judgment in which case a different concern arises.[59] In general, patent claims are required to be definite.[60] Because of this rule, the US Federal

55 P Baron, "Back to the Future: Learning from the Past in the Database Debate" (2001) 62 OHSLJ 879 at 892.

56 See M Mattioli, "Disclosing Big Data" (2014) 99 Minn L Rev 535 and O Tene & J Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics" (2013) 11 NW J Tech & Intell Prop 239.

57 In Singapore, the s 14 of the Patents Act (Cap 221, 2005 Rev Ed) states that "an invention shall be taken to be new if it does not form part of the state of the art". State of the art is in turned defined as "all matter (whether a product, a process, information about either, or anything else) which has, at any time before the priority date of that invention, been made available to the public (whether in Singapore or elsewhere) by written or oral description, by use or in any other way".

58 See, A Kang *et al*, *A Guide to Patent Law in Singapore* (Sweet & Maxwell, 2nd Ed, 2009) at paras 3.3.10–3.3.11.

59 M Mattioli, "Disclosing Big Data" (2014) 99 Minn L Rev 535 at 572.

60 See s 25(5) of the Patents Act (Cap 221, 2005 Rev Ed). See also the US Patent Act 35 USC (US) § 112.

Circuit has invalidated patents claiming processes that rely on subjective judgments.[61] Some big data practices may fall afoul of this rule. Data mining firms that require humans to sieve out useful information from a large amount of data are prime examples. For instance, DataSift is a company that specialises in extracting value from seemingly innocuous social media postings.[62] For a fee, DataSift will provide its clients with the general public sentiment on matters like brands, events and public figures. This is particularly valuable to firms whose business strategies hinge upon how public opinions trend. DataSift ascertains public opinion by culling significant data and metadata from millions of daily social media posts. This is mostly performed by advance technology but humans are required to identify anomalies.[63] Such processes are unlikely to qualify for patent protection as they most probably cannot be claimed definitively. As a result of the foregoing, it is difficult to foresee patent law as the solution to the allocation of economic rights arising from databases.

Copyright

23 Given the dim prospects of patent law, what then of copyright? As mentioned above,[64] copyright is the traditional framework used to protect rights to databases. Copyright is

61 *Re Musgrave* 431 F 2d 882 at 893 (1970) (CCPA) and *Datamize LLC v Plumtree Software, Inc* 417 F 3d 1342 (Fed Cir, 2005).

62 See DataSift, "About Us" <http://datasift.com/company/> (accessed 29 October 2015).

63 See M Mattioli, "Disclosing Big Data" (2014) 99 Minn L Rev 535 at 558–559. The author cites the following example:

> Recently, one of the company's clients requested a list of the twenty most popular athletes in America. The client, a clothing manufacturer, planned to use this list to decide which players' names to include on a new line of athletic jerseys. To find the answer, DataSift scoured the Internet to see which players on various sports teams were mentioned most often. The raw number of times a player was mentioned didn't reflect popularity alone, however: a player might be mentioned for positive or negative reasons. For this reason, the company relied on subjective human judgments to help determine the sentiment behind the online posts that it uncovered.

64 See para 19 above.

essentially a bundle of rights statutorily conferred on creators of certain, specified works. These rights allow them to prohibit others from doing certain acts in relation to those works. Such works typically includes books, plays, photographs, paintings, songs and, indeed, computer programs and databases.[65] The period of protection may vary according to the subject matter at hand. There are in the main two justifications for the conferring of such rights.[66] First, some subscribe to the belief that copyright protection is necessary to provide sufficient economic impetus for owners of works to continue to create original works. On the other hand, others argue that copyright is a natural manifestation of the general right to own the fruits of one's labour. These theories, commonly called the "creative spark" and "sweat of the brow" theories respectively, have influenced the way copyright law has developed in different countries. Even so, it may be said that there are at least three common requirements of copyright law everywhere:[67]

(a) the work must be a subject matter that qualifies to be protected;

(b) the work must be original; and

(c) it must be reduced or fixated to some "material form".

24 Although databases have long been protected under copyright law, they sit uneasily with the legal concept. For one, a fundamental premise of copyright law is that it does not protect facts, ideas or information, only the manner in which they are expressed.[68] For that reason, the information or data underlying

65 See, for instance, s 7 of the Copyright Act (Cap 63, 2006 Rev Ed) and s 1(1) of the English Copyright, Designs and Patents Act 1988 (c 48).

66 See generally, S Leong, *Intellectual Property Law of Singapore* (Singapore Academy of Law, 2013) at pp 35–37.

67 See, for instance, s 16 of the Copyright Act (Cap 63, 2006 Rev Ed).

68 See, for instance, K Garnett, G Davies & G Harbottle, *Copinger and Skone James on Copyright* (Sweet & Maxwell, 16th Ed, 2011) at para 2-06. See also Art 9(2) of the Agreement on Trade-related Aspects of Intellectual Property Rights: "[c]opyright protection shall extend to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such". In *Feist Publications, Inc v Rural Telephone Service Co, Inc* 499 US 340 at 357 (1991), it was argued that no one might claim originality in facts because facts do not owe their origin to an original act of authorship.

databases generally does not qualify to be protected. This usually leaves the mere act of collection or compilation of information unrewarded. More significantly, any protection afforded to databases is unlikely to effectively deter copying. Any pirate can simply appropriate the individual data and organize or arrange them in a slightly different manner. As has been observed, "it is often possible to steal the tiles without copying the entire mosaic".[69]

25 Furthermore, the requirement of originality also poses difficulties. For those that adhere to the "sweat of the brow" doctrine, this requirement imports a very low standard.[70] As long as the compilation, organisation or application of the database takes some effort, judgment or skill, this may suffice to attract copyright protection. The exact level of effort required will have to be mapped out by jurisdictional case law but, in general, almost any form of organisation of the data would suffice. The common criticism of such an understanding of originality is that too much protection would be afforded.[71] It creates a *de facto* monopoly that prevents latecomers from building and improving upon pre-existing compilations. This includes those who are not competing with the first mover in that they are using the database for completely different ends. It rewards laborious efforts at the

69 M Mattioli, "Disclosing Big Data" (2014) 99 Minn L Rev 535 at 574-575.

70 Originality, in this context, refers not so much as to the originality of expression but to the origins of the work. It was expressed by Pearson J in *University of London Press Ltd v University Tutorial Press Ltd* [1916] 2 Ch 601 (at 608–609) in the following manner:

> The word 'original' does not in this connection mean that the work must be the expression of original or inventive thought. Copyright Acts are not concerned with the originality of ideas, but with the expression of thought, and, in the case of 'literary work', with the expression of thought in print or writing. The originality which is required relates to the expression of the thought. But the [Copyright] Act does not require that the expression must be in an original or novel form, but that the work must not be copied from another work – that it should *originate* from the author. [emphasis added]

71 See P Baron, "Back to the Future: Learning from the Past in the Database Debate" (2001) 62 OHSLJ 879 at 900, J Lipton, "Balancing Private Rights and Public Policies: Reconceptualizing Property in Databases" (2003) 18 Berkeley Tech L J 773 at 814 and T J Tan, "New Law for Compilations and Databases in Singapore?" (2012) 24 SAcLJ 745 at para 34.

expense of creative endeavours and narrows the distinction between facts (which are non-copyrightable) and expression (which is copyrightable).

26 On the other hand, the "creative spark" doctrine is also not ideal where the distribution of the economic benefits of databases is concerned. This doctrine imports an element of creativity into the requirement of originality, as illustrated in the famous case of *Feist Publications, Inc v Rural Telephone Service Co, Inc*[72] ("*Feist*"). The respondent, Rural, was a public utility that provided telephone services to communities in Kansas. As part of that operation, it published a telephone listing by obtaining data from its subscribers when those subscribers were applying for services. The petitioner, Feist, on the other hand, was a company that specialised in publishing telephone directories. Feist used the listings provided by Rural without permission whereupon Rural brought an action for copyright infringement. The court held that Rural's listings were "uncopyrightable" because the selection of listings, being "obvious" and lacking the "modicum of creativity",[73] was not sufficiently original to deserve protection.

27 A requirement that creativity be necessary for copyright protection to latch poses two difficulties in the big data context.[74] Firstly, there may be underprotection. Some compilations are of value because they are comprehensive and not because they are uniquely organised. Such mundane databases would not attract protection under the *Feist* standard. On a more fundamental level, it is difficult even to speak of an "arrangement" to protect. This is because electronic databases "may be arranged or retrieved in variations limited only by the capabilities and the sophistication of the retrieval program. There is no particular 'arrangement' to protect".[75]

---

72 499 US 340 (1991).

73 *Feist Publications, Inc v Rural Telephone Service Co, Inc* 499 US 340 at para 51 (1991).

74 See generally, P Baron, "Back to the Future: Learning from the Past in the Database Debate" (2001) 62 OHSLJ 879 at 902.

75 See generally, P Baron, "Back to the Future: Learning from the Past in the Database Debate" (2001) 62 OHSLJ 879 at 900.

28 In short, copyright law seems ill-suited to protect rights to databases. In some scenarios, the grant of copyright would be difficult to establish. In others, there would be under or overprotection. In yet others, infringement, short of wholesale appropriation, would be difficult to establish. Conceived in an age of printing and books, copyright may no longer be fit for purpose at the dawn of big data. It is exactly such opinions that led to the development of a *sui generis* approach to the protection of rights to databases in the EU.

The European Union Directive

29 The EU Directive on the legal protection of databases[76] is a truly unique animal. Dating back to 1996, the complexity of the negotiations that preceded it is reflected in the sixty explanatory paragraphs contained in the preamble. A major impetus for the EU Database Directive can be found in the general sentiment that the traditional copyright approach fails to protect rights to databases adequately. In particular, it was felt that copyright fails to prevent the misappropriation of the *contents* of the database.[77] Even so, the EU Database Directive does not entirely depart from copyright law. It is clear from the substance of the EU Database Directive, if not the form, that vestiges of copyright law remain.

30 The EU Database Directive employs an elaborate strategy to protect rights to databases. First, it defines the meaning of database very broadly – "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means".[78] This

76 The EU Database Directive.

77 The EU Database Directive recital 39:

> [I]n addition to aiming to protect the copyright in the original selection or arrangement of the contents of a database, this Directive seeks to safeguard the position of makers of databases against misappropriation of the results of the financial and professional investment made in obtaining and collection [of] the contents by protecting the whole or substantial parts of a database against certain acts by a user or competitor[.]

78 See Art 1(2) of the EU Database Directive. The implications of this broad definition have been discussed in E Derclaye, "What is a Database?" (2002)

(*continued on the next page*)

definition is then applied to a two-tier approach that is used to protect, separately, the structure and contents of databases. On the first level, a traditional copyright approach is adopted to protect the structure of databases, that is, the "selection or arrangement" of databases.[79] Essentially, the structure of databases attracts copyright protection if it constitutes "the author's own intellectual creation".[80] This requirement of "intellectual creation" is of course a nod to the "creative spark" doctrine. Copyright law in continental Europe typically required the "creative spark" standard and, in this context, this part of the EU Database Directive was a reduction of the threshold that continental law would otherwise have required. In order to gain copyright, it will no longer suffice to rely solely on skill and effort; the structure and presentation of the data must involve creativity and not just mere adherence to obvious selection or natural rules.[81] If copyright applies, it will apply for life plus seventy years.

31 The second-tier, dealing with protection of the contents of the database, is where the EU Database Directive is truly *sui generis*. The contents of a database are protected where there has been a "substantial investment in either the obtaining, verification or presentation of the contents".[82] In this regard, three core points may be observed. First, the purpose of this database right is to guard against "extraction and/or re-utilization" of the whole or a substantial part of the database.[83] The focus is to prevent pirates

5 JWIP 981 and T Aplin, *Copyright in the Digital Society* (Hart Publishing, 2005) at pp 44–52.

79 The EU Database Directive Art 3(1).

80 The EU Database Directive Art 3(1).

81 In *Football Dataco Ltd v Yahoo! UK Ltd* Case C-604/10 (1 March 2012) (at para 38), the Court of Justice of the European Union held that the requirement of originality is met when, in the selection or arrangement of data, the author "expresses his creative ability in an original manner by making free and creative choices", thereby applying his "personal touch".

82 The EU Database Directive Art 7(1).

83 Under Art 7(2) of the EU Database Directive, "extraction" means the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form and "re-utilization" means making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission.

from reorganising or re-presenting essentially the same material in a different form. This is of course a legitimate concern. Secondly, to obtain protection, there must have been, qualitatively or quantitatively, a substantial investment in the database contents. This requirement is reminiscent of the "sweat of the brow" doctrine prevailing in Anglo-Australian jurisprudence. Finally, the right, if it attracts, expires fifteen years from the completion of the database or fifteen years from it becoming publicly available during the first fifteen-year period.[84] Crucially, time runs afresh every time there is substantial change to the database, including changes resulting from additions, deletions or alterations to the database.[85] In effect, a regularly updated database enjoys perpetual protection. This is significant where Big Data is concerned as Big Data is supposed to grow so quickly, substantially, and almost organically that any Big Data database, once protectable, may be so protected forevermore.

32 The EU *sui generis* model of database right has garnered no small amount of criticism.[86] In the main, it has been observed that there has been an overcompensation for the deficiencies of the copyright regime – the database right "substitute[s] a chronic state of overprotection for a potential state of underprotection".[87] Given the fact that the length of protection starts afresh with any substantial change, the database right creates an exclusive property regime with few public policy limitations.[88] This will result in the elimination of the market for value-added products and services and prevent data reuse. In effect, the database right creates

84 The EU Database Directive Arts 10(1) and 10(2).

85 The EU Database Directive Art 10(3).

86 See J Reichman & P Samuelson, "Intellectual Property Rights in Data?" (1997) 50 VNLR 51. The authors call the database right the "arguably most deviant" example of *sui generis* protection which is "seriously flawed" (at pp 53 and 55). See also H Deveci, "Databases: Is Sui Generis a Stronger Bet than Copyright?" (2004) 12 Int'l JL & Info Tech 178 and D Lim, "Re-defining the Rights and Responsibilities of Database Owners under Competition Law" (2006) 18 SacLJ 418.

87 See J Reichman & P Samuelson, "Intellectual Property Rights in Data?" (1997) 50 VNLR 51 at 137.

88 See also D Lim, "Re-defining the Rights and Responsibilities of Database Owners under Competition Law" (2006) 18 SacLJ 418 at para 33.

"insuperable legal barriers to entry".[89] Ultimately, all of this will work together to result in high prices for the use of public goods. This is at odds with economic efficiency which calls for the minimum incentive required to provide the impetus necessary for continued database creation.

33 The critique that the database right grants a far broader and stronger monopoly than is necessary to avert market failure has a lot of force. However, it will not do to simply tweak the *sui generis* model to recalibrate the strength of the protection afforded. The fundamental flaw lies in the fact that copyright principles have been adopted to form the foundation of the database right. However, the relevance of copyright principles may rightly be questioned in a Big Data era. These principles were formulated in an era of traditional databases in which raw data is properly structured for maximum utility. Drawing upon that underlying premise, intellectual property right protection hinges upon, amongst other things, some creativity or originality in the way the database is structured. However, where Big Data is concern, the promise is that databases will not require structuring at all or will not at least be structured in the same way. Data analytics engines will sieve out the relevant information, thus obviating the need for the structuring of data. Indeed, "[t]he current debate has been too closely tied to copyright models simply because the need for database protection legislation has been based on the perceived failings of copyright law to adequately protect digital database contents ... Future discussions should take a new turn altogether, leaving inadequacies of copyright law aside and focusing purely on the realistic commercial needs of database producers and on the needs of society, domestically and internationally."[90] The next part attempts to take this "new turn".

89 J Reichman & P Samuelson, "Intellectual Property Rights in Data?" (1997) 50 VNLR 51 at 55–56.

90 J Lipton, "Balancing Private Rights and Public Policies: Reconceptualizing Property in Databases" (2003) 18 Berkeley Tech L J 773 at 831–832.

NEW WINE, NEW BOTTLES

34 Thus far, this paper has attempted to explain the importance of big data and how it is here to stay. The author has also discussed how present regimes of intellectual property law, including patents, copyright and the *sui generis* database right, are unlikely to unlock the full, transformative potential of big data. This leads to the natural conclusion that a paradigm shift must be found, a different way to distribute and protect the economic benefits of big data. That much is, for the most part, plain. What is uncertain is the path that ought to be taken. To this end, this part discusses three possible directions:[91]

(a) the use of competition law in conjunction with copyright law,

(b) the tort of unfair competition, and

(c) a State-administered reward system.

Each of these possibilities on their own may be – and, in the case of the former two, have been – the subject matter of whole articles. In this part, the author will merely attempt to outline these ideas.

Competition law

35 Strictly speaking, this first idea is not a total departure from copyright law. Rather, the regime that is contemplated is one that would employ copyright law to allow database owners to enjoy intellectual property rights while employing competition law to regulate the exercise of those rights. On the surface, it would appear that copyright and competition law make strange bedfellows. The effect of the former is, after all, to create

91 To best of the author's knowledge, Reichman and Samuelson were the first to promote the idea of using an unfair competition approach: J Reichman & P Samuelson, "Intellectual Property Rights in Data?" (1997) 50 VNLR 51 at 139. Lim in two different articles, suggested using competition law to regulate the use of databases: D Lim, "Re-defining the Rights and Responsibilities of Database Owners under Competition Law" (2006) 18 SacLJ 418 and D Lim, "Regulating Access to Databases through Antitrust Law: A Missing Perspective in the Database Debate" (2006) Stan Tech L Rev 7.

monopolies while the object of the latter is to prevent the same as far as possible. However, it is now fairly accepted that the roles of intellectual property and competition law are in fact complementary if distinct.[92] Intellectual property law helps to create markets and products; competition law regulates markets to ensure that they are efficient. Ultimately, both regimes work to promote consumer welfare.

36 The law of copyright works *ex ante*. It establishes a bundle of statutorily conferred rights as well as stipulates a time period in which such rights may be exercised in hope that creators will thereby be incentivised to create. In this way, copyright spurs continued creativity. However, copyright pays little heed to the Goldilocks principle: it does not strive to examine each particular literary work and assess its social value to determine the appropriate period of protection. Nor does copyright measure the value of the competing creation to perform a cost-benefit analysis. Each creator is therefore given the same sledgehammer to eliminate pirates, competitors and non-competitors alike. This one-size-fits-all approach is subject only to statutory and common law defences. These defences pursue public policies that have little to do with economic efficiency. For instance, the exception of fair dealing allows for limited use of copyrighted material for non-commercial purposes such as research, news reporting, and criticism and review.[93]

37 Where databases are concerned, this is not satisfactory. Apart from conceptual difficulties,[94] there are two major problems with the use of copyright law alone from an economic perspective. First,

---

92 See, for instance, Competition Commission of Singapore, "CCS Guidelines on the Treatment of Intellectual Property Rights" (June 2007) at para 2.1 states:

> Both intellectual property ('IP') and competition laws share the same basic objective of promoting economic efficiency and innovation. IP law does this through the provision of incentives for innovation and its dissemination and commercialisation, by establishing enforceable property rights for the creators of new and improved products and processes. Competition law does this by helping to promote competitive markets, thereby spurring firms to be more efficient and innovative.

93 W Cornish, D Llewelyn & T Aplin, *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* (Sweet & Maxwell, 8th Ed, 2013) at pp 490–495.

94 Outlined at paras 24–27 above.

the length of protection granted by traditional copyright law would usually far outlast the value of the database. The monopoly created would then result in a loss of consumer welfare. This is known as a deadweight loss. Compounding the problem, the great variety of databases means that it is difficult to apply one period of protection for all databases without that period being inappropriate for the most part.[95] Separately, copyright law allows database owners to take advantage of their dominant position in two distinct ways that would be economically inefficient. First, where the database constitutes an "essential facility", the database owner may deny the use of the database to a competitor in a secondary market.[96] Where such denial results in the competitor being unable to operate in the secondary market, this would be harmful to society. Secondly, the database owner may leverage upon his dominance in one market to gain an unfair advantage in a secondary market by way of "tying" two products; he may insist that consumers purchase both products or not at all.[97] Both of these practices are not prohibited under the law of copyright.

38 Lim suggests that competition law may be used to address some of these deficiencies. This is not to say that copyright law should be abandoned. Rather, his argument is that copyright should continue to apply to databases as it conventionally does. This will provide the "push" factor for databases to be created. However, competition law may be used to "pull" database owners

95 S Leong, *Intellectual Property Law of Singapore* (Singapore Academy of Law, 2013) at para 04.050, noted that:

> Copyright as a protection regime makes no distinction between different types of factual compilations and databases. There are databases that are time sensitive and will become obsolete very quickly. The kind of protection such databases require may differ from the protection required for databases that are exhaustive in nature and which do not change very much over time once they are created.

96 For a fuller explanation of the "essential facilities" doctrine, see S M Colino, *Competition Law of the EU and UK* (Oxford University Press, 7th Ed, 2011) at para 16.3.2.

97 S M Colino, *Competition Law of the EU and UK* (Oxford University Press, 7th Ed, 2011) at para 14.5.1.1.

from exercising their rights to a manner that is economically harmful to society. In effect,[98]

> [Competition] law functions ex post to regulate the exercise of IPRs ["intellectual property rights"] following the grant. It protects the public's *commercial* interests by ensuring that IPR owners do exercise their rights to the extent granted for the specific subject matter so that market competition is not distorted and consumer welfare is not harmed. [emphasis in original]

39 Thus, what is envisaged is a system where copyright law and competition law acts as opposing forces to create a finely balanced equilibrium of database rights and responsibilities. Under this system, database owners would be allowed to enforce their rights as under the copyright regime, save for situations where to do so would be anticompetitive. In this regard, anti-competitiveness is predominantly an inquiry into whether there has been an abuse of a dominant market position.[99] Broken down, this inquiry amounts to a two-step test: whether the database owner is dominant in the relevant market and, if so, whether there has been an abuse of that dominant position.[100] Taken holistically, this test ensures that the incentivisation effect continues to apply. A database will continue to enjoy copyright protection as long as the database owner has not attained a dominant position in the market;[101] the possession of copyright alone does not guarantee a dominant market position.[102]

---

98 D Lim, "Regulating Access to Databases through Antitrust Law: A Missing Perspective in the Database Debate" (2006) Stan Tech L Rev 7 at para 31.

99 See, for instance, the Competition Act (Cap 50B, 2006 Rev Ed) s 47. See also Competition Commission of Singapore, "CCS Guidelines on the Section 47 Prohibition" (June 2007).

100 Competition Commission of Singapore, "CCS Guidelines on the Section 47 Prohibition" (June 2007) at para 3.1.

101 A database owner will not be deemed dominant unless it has substantial market power. Market power arises where a database owner does not face sufficiently strong competitive pressure and can be thought of as the ability to profitably sustain prices above competitive levels or to restrict output or quality below competitive levels. A database owner with market power might also have the ability and incentive to harm the process of competition in other ways, for example, by weakening existing competition, raising entry barriers or slowing innovation: see Competition Commission of Singapore, "CCS Guidelines on the Section 47 Prohibition" (June 2007) at para 3.3.

102 Competition Commission of Singapore, "CCS Guidelines on the Section 47 Prohibition" (June 2007) at para 4.1.

Even with a dominant market position, a database owner may still enjoy his intellectual property rights unless to do so would amount to an *abuse* of his market position.[103] Such abuse essentially means conduct that would enhance or entrench the database owner's dominant position in ways unrelated to competitive merit.[104]

40 Therefore, an intrusion into the rights of a database owner must be justified purely by reference to economic efficiency. In general, this may conceivably happen in two scenarios. Firstly, if the database qualifies as an essential facility under the essential facilities doctrine, a database owner may be forced to supply licences for others to use the database.[105] Secondly, a database owner would not be allowed to use his dominant position in one market to unfairly affect secondary markets for derivative uses of the same data.[106] These intrusions ensure that copyright does not prevent the reuse of the data in ways that do not affect the database owner's rights in the primary market. Hence, by use of the push of intellectual property law and the pull of competition law, this system aims to strike a delicate balance between protectionism and liberal reuse.

103 For examples of conduct that may constitute abuse, see s 47(2) of the Competition Act (Cap 50B, 2006 Rev Ed).

104 Competition Commission of Singapore, "CCS Guidelines on the Section 47 Prohibition" (June 2007) at para 4.5. Examples of such behaviour provided includes a refusal to supply a licence for an essential facility, tying and even an acquisition of an intellectual property right.

105 Competition Commission of Singapore, "CCS Guidelines on the Section 47 Prohibition" (June 2007) at para 4.6. See also S M Colino, *Competition Law of the EU and UK* (Oxford University Press, 7th Ed, 2011) at para 16.3.2. For examples of cases that have dealt with the application of the essential facilities doctrine to databases, see *IMS Health GmbH & Co OHG v NDC Health GmbH & Co KG* [2004] ECR I-05039 (29 April 2004) and *Radio Telefix Eireann and Independent Television Publications Ltd v Commissioner of the European Communities* [1995] ECR I-00743 (6 April 1995).

106 Competition Commission of Singapore, "CCS Guidelines on the Section 47 Prohibition" (June 2007) at para 4.9. See also S M Colino, *Competition Law of the EU and UK* (Oxford University Press, 7th Ed, 2011) at para 14.5.1.1.

Tort of unfair competition

41 One key issue with the use of the copyright-competition law framework is the fact that fundamental conceptual difficulties, expressed previously, remain unresolved. The data underlying databases remain unprotected and there will invariably be under or over-protection. The use of the American tort of unfair competition may overcome such difficulties. There is no general tort of unfair competition under the common law.[107] What is available under general common law are disparate torts, such as passing off, inducing breach of contract and conspiracy, which have anticompetitive behaviour as a commonality. However, the US has developed an unfair competition approach which may be of some utility in the context of databases. In fact, it is posited that this approach may have the desired Goldilocks effect – it will allow the courts to adjust the level of protection granted to database owners in a manner commensurate with the social value of the database.

42 The classic American tradition of unfair competition arose out of the US Supreme Court case of *International News Service v Associated Press*[108] ("*International News Service*"). Two competing news agencies, International News Service ("INS") and Associated Press ("AP"), were in the business of publishing news in the US. At the material time, the news was dominated by the events of World War I. The success of their businesses depended very much on the parties' ability to deliver timely reports. However, INS fell out of favour with the Allied Powers as a result of the way in which it reported the news. Consequently, the Allied Powers disallowed INS from using Allied Telegraph.[109] This severely crippled INS's ability to deliver the news. However, INS found a way around this problem. Its agents on the east coast of the US bought early editions of newspapers affiliated with AP and read news on the war to INS agents in California through telephones. Those agents would

107 H Carty, *An Analysis of the Economic Torts* (Oxford University Press, 2nd Ed, 2010) at p 2.

108 248 US 215 (1918).

109 *International News Service v Associated Press* 248 US 215 at 263 (1918). Brandeis J noted that "[f]or aught that appears, this prohibition may have been wholly undeserved".

then rewrite the news and publish them in competition with AP's newspapers on the west coast. Disgruntled, AP brought an action to enjoin INS from copying news published by AP.

43 The US Supreme Court found in favour of AP even though there had hitherto been no established cause of action to deal with such a situation. The majority recognised that the information found in the newspapers, being mostly factual and in the nature of current events, were not copyrightable.[110] However, the court found that the news contained economic value and a company therefore has a "quasi-property" interest in it against a competitor.[111] Notably, the court limited the period for which this proprietary right would apply in order to avoid giving AP an excessive monopoly. As was held, the view the court adopted merely "postpones participation by complainant's competitor in the processes of distribution and reproduction of news that it has not gathered, and only to the extent necessary to prevent that competitor from reaping the fruits of complainant's efforts and expenditure".[112] In other words, the court recognised that news only has value insofar as it was "hot" and beyond that initial period, it would not be economically efficient to prevent INS from entering the market, even if it did so by appropriating news from AP. Any proprietary right should not therefore last beyond that initial period.

44 While there has been some criticism of this decision, there has also been some who have regarded this case positively.[113] In particular, Gordon proposed the creation of a misappropriation tort based on the case of *International News Service* for malcompetitive copying that would provide protection not covered by patent or copyright law.[114] Specifically, she argued that the following criteria

110 *International News Service v Associated Press* 248 US 215 at 234 (1918).

111 *International News Service v Associated Press* 248 US 215 at 236 (1918).

112 *International News Service v Associated Press* 248 US 215 at 241 (1918).

113 See, for instance, W Gordon, "On Owning Information: Intellectual Property and the Restitutionary Impulse" (1992) 78 Va L Rev 149.

114 See, for instance, W Gordon, "On Owning Information: Intellectual Property and the Restitutionary Impulse" (1992) 78 Va L Rev 149.

would justify the court stepping in *ex post* to protect the creator's right:[115]

(a) the costs of developing the information product are high;

(b) the costs of copying are low;

(c) copying produces a substantially identical product;

(d) a pirate can price his product cheaply, not having substantial research and development costs to recoup;

(e) consumers prefer to buy the cheaper product, the two products being substantially the same; and

(f) such market failure can be prevented by allowing a period of protection that would allow the first mover to recoup its expenses and justify its investment in developing the informational product.

45 It has been suggested that this approach may be applied to protect databases.[116] Under this framework, judging the fairness of data reuse would depend on many factors, including the amount of data appropriated, the nature of such data, the purpose for the appropriation, the amount of investment required to compile the database, the connection between the markets in which the database owner and second mover operates, and the degree of similarity between the two products.[117] Nevertheless, such an exercise would ultimately be focused on the goal of providing the minimal protection required to prevent market failure. For databases that are an aggregation of information whose value is very short-lived, the period of protection would be accordingly short. For databases whose value continues to hold for long periods, the period of protection may be longer.

46 This approach has much to recommend. Under this system, the court can take into account a variety of factors and tailor a

115 See, for instance, W Gordon, "On Owning Information: Intellectual Property and the Restitutionary Impulse" (1992) 78 Va L Rev 149 at 149–281.

116 J Reichman & P Samuelson, "Intellectual Property Rights in Data?" (1997) 50 VNLR 51.

117 J Reichman & P Samuelson, "Intellectual Property Rights in Data?" (1997) 50 VNLR 51 at 143–144.

remedy that will suit the case at hand. This potentially allows for individualised justice and welfare maximisation. It must be noted that the use of unfair competition principles to protect databases is not unheard of; it has been observed that such an approach has been available in Europe.[118]

State-administered reward system

47 For all of its advantages,[119] the unfair competition approach faces one distinct difficulty. The success of that approach requires the court to be in possession of a lot of information in order for the court to be able to peg the period of protection at an appropriate duration. It is questionable if the court will be in possession of such information or has the expertise to use such information properly. This is particularly so when both the maker of the database and the competitor are individuals who do not have deep pockets. The court, after all, only has as much information as is provided by the parties.

48 In this respect, the next possibility for a new approach to managing the economic rights arising from big data is far superior. Traditionally, intellectual property law operates by granting proprietary rights. The previous two suggestions – the use of competition law and unfair competition principles – do not depart from that basic idea. They too operate through the grant of property rights. This last suggestion eschews the use of property rights altogether. Instead, what is posited is an *ex post* reward system administered by the State. What is envisioned is a framework where the State will grant financial rewards for the creation of databases. A database, once created, is registered and handed over to the State who will in turn release it for use by the public. The database owner does not look to any property right for impetus to create the database; rather he will look to the reward provided by the State. The reward granted need not be disbursed all at once upon registration. As an alternative, the reward may be

118 J Reichman, "Electronic Information Tools – The Outer Edge of World Intellectual Property Law" (1993) 25 Int'l Rev Indus Prop & Copyright L 446.

119 Outlined at para 46 above.

provided incrementally over the life of the database, allowing the quantum of the reward to closely track the social value of the database. Insofar as the database owner is concerned, the issue of piracy falls away. If there is any secondary reuse of the data, it falls to the State to determine if such competitors ought to be rewarded and, if so, in what magnitude.

49 This idea is not entirely original. In fact, it finds its roots in antiquity. Historians of patent law will be familiar with the fact that although patent law emerged as early as the 1400s, the patent system came under very strong attack during the period 1850 to 1875.[120] Chief amongst the criticisms of the patent system is the fact that it confers monopoly power, thus harming consumers who have to pay very high prices for inventions and who are unable to enjoy subsequent innovations that may infringe upon the patent. As a result, many countries took steps to reform or dismantle the patent system.[121] An alternative to the patent system considered was a system of rewards financially-backed by the State.[122] However, the reward system had its own critics who argued that such a regime

120 For a brief summary of this episode, see S Shavell & T Van Ypersele, "Rewards Versus Intellectual Property Rights" (2001) 44 *Journal of Law and Economics* 525 at 526. On the history of patent, see H I Dutton, *The Patent System and Inventive Activity During the Industrial Revolution 1750–1852* (Manchester University Press, 1984), F Machlup, *An Economic Review of the Patent System* (Psychology Press, 2002), C MacLeod, *Inventing the Industrial Revolution: The English Patent System, 1660-1800* (Cambridge University Press, 2010) and F Prager, "History of Intellectual Property From 1545 to 1787" (1994) 26 J Patent Office Soc'y 711.

121 S Shavell & T Van Ypersele, "Rewards Versus Intellectual Property Rights" (2001) 44 *Journal of Law and Economics* 525 at 527, records that:

> [M]any countries in Europe prepared to reform or abolish patent, and some actually did so: England established a series of royal commissions from the 1850s to the 1870s to investigate the patent system; Chancellor Bismarck recommended abolition of patent in Prussia in 1868; Holland repealed its patent system in 1869; and Switzerland, which had no patent law, rejected legislation to adopt it in 1863.

122 S Shavell & T Van Ypersele, "Rewards Versus Intellectual Property Rights" (2001) 44 *Journal of Law and Economics* 525 at 527, writes that:

> Robert Macfie, a member of Parliament in England and an influential champion of rewards, set out a proposal for a government-financed reward system to replace patent; the London *Economist* pressed for adoption of a reward system; and economists examined rewards in professional journals, books, pamphlets, and conferences.

might be administratively difficult to implement.[123] Ultimately, the patent system prevailed in this contest of ideas but this was not because it was found to be economically superior to the reward system; rather the Long Depression of the 1870s in Europe and the US turned public sentiment against free trade and towards greater protection of labour.[124]

50 In a seminal paper, Shavell and Van Ypersele studied the pros and cons of the intellectual property and reward systems from an economic perspective.[125] Applying economic analysis, they found that a proprietary system "does not enjoy any fundamental advantage over the reward system".[126] More specifically, both systems enjoy different advantages. The reward system has the benefit of avoiding the deadweight loss that intellectual property rights suffer from due to monopoly pricing. However, patent law may possibly provide more appropriate incentives to innovate as it "harnesses the private information of the innovator about the value of the innovation".[127] In other words, in a situation where the State knows very little about the social value of the product, patent law will incentivise better than the reward system. This is because the inventor will know more about the demand for the potential invention and the amount of investment will be accordingly linked to actual social surplus.

51 Key to this conclusion is the view that the State is in a poor position to gather the necessary information to value the invention appropriately. If it were otherwise, it is implicit in their article that the reward system would be clearly superior to the intellectual property rights system.[128] As they also conceded, the assumption

123 See S Shavell & T Van Ypersele, "Rewards Versus Intellectual Property Rights" (2001) 44 *Journal of Law and Economics* 525.

124 See S Shavell & T Van Ypersele, "Rewards Versus Intellectual Property Rights" (2001) 44 *Journal of Law and Economics* 525.

125 See S Shavell & T Van Ypersele, "Rewards Versus Intellectual Property Rights" (2001) 44 *Journal of Law and Economics* 525.

126 See S Shavell & T Van Ypersele, "Rewards Versus Intellectual Property Rights" (2001) 44 *Journal of Law and Economics* 525 at 525.

127 See S Shavell & T Van Ypersele, "Rewards Versus Intellectual Property Rights" (2001) 44 *Journal of Law and Economics* 525 at 530.

128 As stated in S Shavell & T Van Ypersele, "Rewards Versus Intellectual Property Rights" (2001) 44 *Journal of Law and Economics* 525 at 541, "the government's

(*continued on the next page*)

that the State is in possession of less information than the inventor may not necessary be true. Obviously the government can rely on sales data since the rewards are distributed *ex post*. Further, they also point out that in certain circumstances, the government can attempt to measure the demand curve more accurately. It can, for instance, estimate demand elasticities by undertaking surveys.[129]

52 Applying all of these propositions to a big data context, it becomes clear that a reward system is *eminently* suitable to govern the distribution of economic benefits of electronic databases. This is because the potential for the government to harness information about the demand for a particular database is infinite. After all, big data techniques may themselves be applied upon databases, if necessary. All sorts of data and metadata may be collected without the end user even being consciously aware. The State will surely be able to not just ascertain the number of users, but also the geographical location of these users, for how long the database is used, in what manner the data is arranged, what substitutes they look to, *etc*. Even if necessary data cannot be captured from the natural use of the database itself (for instance, the age profile of the users), the State can easily make the use of the database contingent upon the provision of such data. In other words, the possibilities are limitless. The one weakness that prevents the reward system from being a serious consideration becomes an unquestionable strength in the big data context. In an age of big data, the State may possibly be in a position of almost perfect information. Not only will there be no deadweight loss from monopolistic practices, the State will be able to tailor the reward, over time if necessary, in as economically efficient a manner as possible. This makes the reward system the most economically efficient way of distributing the economic benefits of databases.

knowledge about the social value of innovations, embodied in its probability distribution over demand curves, is important to the performance of the reward system and to that of the optional reward system".

129 See S Shavell & T Van Ypersele, "Rewards Versus Intellectual Property Rights" (2001) 44 *Journal of Law and Economics* 525 at 541.

CONCLUSION

53 There is little doubt that one lives in an era that presents both exciting possibilities and tremendous challenges. It also appears that the current patent-copyright paradigms that dominate intellectual property law seem ill-suited to cope with the challenge of properly allocating the economic benefits of databases. Neither does the *sui generis* EU database right appear to be the correct solution. It becomes incumbent upon one to then meet this challenge by finding new bottles for the new wine of big data, just as copyright was found as a solution for the transformative invention of mass printing.

54 In the Global Technology Conference held in Singapore in 2015, it was remarked that the way forward is through "local experimentation" by "having legislators address this challenge on a national rather than international basis as an initial matter".[130] To that end, this paper has put forward three distinct possibilities for national legislators to ponder over. Each of these suggestions attempts to find a way to strike the balance between incentivising creation of big data and allowing liberal, if not free, reuse. The first utilises two powerful forces, copyright law and competition law, in tandem to achieve a delicate balance; the second promulgates a court-led initiative using unfair competition principles; and the last proposes a State-administered reward system. For the sake of brevity, this paper can only outline the basic shapes of these systems. Clearly, the working details of such systems must be ironed out at a national level. Even if an answer cannot be found within these suggestions, it suffices to demonstrate that a paradigm shift in the way one thinks about distributing the economic benefits of big data is both necessary and realistic.

---

130 Transcript recorded by the author, and vetted by the speaker, Paul Goldstein, at the Global Technology Conference in Singapore (29–30 June 2015).

The Digital Big Bang and its Implications on Discovery in Litigation

The age of data has revolutionised many areas of life. Slowly but surely, the practice of litigation is forced to confront this new digital reality. The importance and difficulty in grappling with large volumes of documents and information has spawned new technologies and markets. This article explores how some of those technologies affect the practice of litigation through the lens of the discovery process.

Nicholas **POON***
LLB (Singapore Management University);
Assistant Registrar, Supreme Court of Singapore.

INTRODUCTION

1 The world as one knows it today is very different from that which existed before the Internet was invented, which itself has become so mundane that those living in most developed cities and even some developing cities take it for granted. Revolutionary as the Internet is, it was but another leap forward in the ongoing information technology ("IT") revolution that began with the introduction of personal computers. The Internet introduced the ability to easily transmit digitised information electronically without dependence on physical media.

2 The invention of physical writing media from papyrus to paper has propelled the development of mankind, by enabling humans to accumulate and transmit knowledge and information over space and time. The conduct of most human affairs will be unimaginable, even today, without this ability to generate and keep records. But it is the relatively new-found ability to accumulate and transmit knowledge and information through digital media that promises to dwarf the accomplishments of all things written or printed.

3 This ability to digitise, store and electronically transmit information greatly enhances our ability to generate and disseminate knowledge. There is now so much information

generated daily – on the scale of the petabyte which is one million gigabytes[1] – that new industries have been built around big data: for example, data storage (like cloud computing) and data analytics. Major technology companies from Adobe to Amazon, Microsoft to Baidu, are spending billions to build up their cloud and web storage capabilities.[2] A Bloomberg article sums it up in "The Cloud is Raining Cash on Amazon, Google, and Microsoft".[3]

EXPLOSION OF DATA AND LITIGATION PRACTICE: WHY IS IT IMPORTANT TO LEGAL PRACTITIONERS

4 While the advent of IT has ushered humankind into a new world order dominated by computer devices, new problems have emerged. The more obvious problems associated with IT are issues of privacy, abuse of confidential information and intellectual property. But this new reality has implications on the law beyond the recognition of new substantive legal rights and obligations between people or corporations. The way information is transmitted, secured and handled has deep repercussions on the way those substantive legal rights are vindicated through the litigation process.[4] One such aspect is the discovery (or disclosure) procedure[5] under which parties are expected to disclose, either voluntarily or by an order of court, information that is relevant and necessary for the fair disposal of the dispute.

---

* Many of the ideas contained in this article are taken from the 6th panel discussion entitled "Judicial Panel on Data Protection and Data Analytics in Discovery" featuring the David Harvey J, Lee Seiu Kin J, Andrew Peck J and chairperson Chris Dale. The panellists, together with Yeong Zee Kin, also contributed editorial suggestions which vastly improved earlier drafts. Needless to say, all errors and infelicities remain the author's.

1 R C Losey, "Predictive Coding and the Proportionality Doctrine: A Marriage Made in Big Data" (2013–2014) 26 *Regent University Law Review* 6 at 9.

2 D Streitfeld & N Wingfield, "With Amazon Atop the Cloud, Big Tech Rivals are Giving Chase" *The New York Times* (23 April 2015).

3 J Clark, I King & D Bass, "The Cloud is Raining Cash on Amazon, Google, and Microsoft" *Bloomberg Business* (23 October 2015).

4 Arbitration and other modes of dispute resolution are equally affected but for convenience only court litigation will be referred to.

5 Particularly relevant in jurisdictions of the common law tradition.

5 Broadly speaking, in the pre-computer era, there was a limit to the quantity of physical documents that could be brought into existence. The process was hence manageable. However in the present day, with documents that are generated without the physical limitations of atoms, and which may be easily reproduced manifold (for example, the "Reply All" function in email), the traditional manner in which discovery is carried out breaks down and technology must be prayed in aid of the problem that it had created in order to ensure that costs of litigation do not spiral out of control. That is why courts have, in recent times, found it necessary to emphasise the principle of proportionality in discovery proceedings. The emergence of this vital principle will be elaborated upon in greater detail below, after a brief survey of the implications of the digital big bang on the key steps in the discovery process.

The key steps in discovery: identifying, obtaining and producing information

6 In every instance of discovery, regardless of the type of information in question, lawyers and courts have to grapple with three very important considerations:

(a) what type of information is relevant,

(b) who has possession of, custody of, or power over that information, and

(c) how may that information be obtained.

However, the application of these questions in the context of digital information and big data presents complications that do not arise in the application of the same questions to information captured in other forms, such as physical records. A lawyer's role in the discovery process for a case involving digital data may therefore be significantly different from the same role in a case that involves primarily physical records.

What type of information is relevant

7 First, lawyers must be cognizant of the types of information that may be relevant. Most individuals have access to and are connected to at least two digital devices in the course of a normal day: our mobile phone and computer. These devices in turn store copious amount of information associated with the individual. The information could be about the individual – one's heart rate, names and contacts of friends and families, places one frequents, lifestyle preferences – or it could be about people that come into contact with the individual through messaging, photographs, and other digital sharing media.

8 The content created on these devices is but one type of information. From who the individual has communicated with and what was said, to what websites the individual has visited and how much time was spent at each website, to even the number of clicks and keystrokes entered, there is a digital, invisible diary of our everyday lives lying somewhere (or in multiple places) that one either do not know about or do not bother to worry about because they appear so irrelevant and far removed, that is, until a dispute arises.

9 Transmission of such content, too, has taken on more significance. Since the advent of the Internet age and up to very recently, the form of digital data that litigation cared about predominantly is emails. But that was just a function of how communication used to take place in the last couple of decades. Instant communication is so powerful now that many contracts are concluded by instant messages, whether it is via SMS, in a WhatsApp chat or over Facebook. People can be, and are increasingly, even sued for what they say on Twitter.[6]

10 As the world smartens beyond computers and mobile phones into transport vehicles such as cars, trains, airplanes or general household appliances such as refrigerators, television sets, entertainment systems, security access systems, the sources of data and information will correspondingly, and surreptitiously, increase.

6 See, *eg*, *Cairns v Modi* [2012] EWHC 756; [2012] EWCA Civ 1382.

The inevitable coming of the Internet of Things – where everyday accessories are interconnected, via the Internet – will open up yet another Pandora's box of new sources of digital information.

11 With so much data created and stored, often in places that even one is unaware of, there is a high propensity going into any dispute that some useful information is not being tapped. After all, one does not know what one does not know. To be effective in this digital age, lawyers must therefore familiarise themselves with the data revolution, to know what type of information is available and could potentially be relevant in a lawsuit.

Who has possession of, custody of or power over that information

12 Once lawyers identify what data needs to be extracted and produced in a litigation, they may realise that the data is not in their client's possession. It may be in the possession of the other parties to the dispute, or it may even be in the possession of a third party (such as, a service provider).

13 Take for example a claim for breach of a duty of confidentiality, where it is alleged that sensitive information and trade secrets were exchanged in private messages on Facebook. In this situation, who owns the private message? And regardless of who the owner is, who has access or control over the contents of these digital inboxes? Is it the account holder, or is it Facebook, or is it the party hosting the servers on which these messages are stored?

14 For a simpler example, think of the GPS-enabled mapping software installed on your mobile phones. Suppose the location, and where one has been in the last 24 hours, is a relevant issue in a dispute. Against whom can an order to disclose the individual's last known coordinates be made? The answer would, probably, depend on where that information is stored, and who is storing it. Is it the data service provider?[7] Or the software company which operates

7 In the US Supreme Court decision of *United States v Jones* 132 S Ct 945 (2012) at 11–12, Alito J, with whom Ginsburg J, Breyer J and Kagan J agreed, noted:

(*continued on the next page*)

and offers the application? Or the mobile phone manufacturer *qua* manufacturer or *qua* the provider of the mapping service or the find-your-phone-service?[8] Or both? Geotagging therefore has implications far beyond keeping the world informed of where the best restaurants can be found.

15 The "who" in the above situations is not just an academic hypothetical question because it informs the discussion as to firstly, whether the information can even be extracted or ordered to be produced by the court, and secondly, how such an order may be made or enforced. This leads to the next question.

How to obtain that information

16 After the party in possession, custody or control of the information is identified, the next step is to obtain a disclosure order against that party. This sounds like a standard application of the domestic laws governing disclosure, but there are complications.

17 One such complication is where the information to be disclosed is held by a subsidiary located in a foreign jurisdiction, as

> [C]ell phones and other wireless devices now permit wireless carriers to track and record the location of users —and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States. For older phones, the accuracy of the location information depends on the density of the tower network, but new 'smart phones,' which are equipped with a GPS device, permit more precise tracking. For example, when a user activates the GPS on such a phone, a provider is able to monitor the phone's location and speed of movement and can then report back real-time traffic conditions after combining ('crowdsourcing') the speed of all such phones on any particular road. Similarly, phone-location-tracking services are offered as 'social' tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.

8 See for example, C Williams, "Apple iPhone Tracks Users' Location in Hidden File" *The Telegraph* (20 April 2011).

is the case in an ongoing dispute between the US government and Microsoft.[9] The salient facts are as follows.

18 The 1986 Stored Communications Act[10] ("SCA") allows the US government to obtain a warrant that requires an internet service provider ("ISP") to produce customer information, emails, and other materials upon showing of probable cause. In December 2013, as part of criminal investigation, federal prosecutors sought and obtained a warrant authorising the search and seizure of information associated with a specific web-based email account stored by Microsoft, which determined that while some information was stored on servers in the US, there was some information which was stored on servers which belong to its local subsidiary located in Dublin, Ireland.

19 Microsoft handed over the information from the US servers, and moved to quash the warrant to the extent that it directed the production of information stored abroad, on the ground that rule 41 of the Federal Rules of Criminal Procedure[11] does not permit courts to issue warrants for the search and seizure of property outside the territorial limits of the US. Microsoft said that the proper channel for the US government to obtain the information it wanted was through the Mutual Legal Assistance Treaty[12] which the US had with Ireland. This line of argument was dismissed by the court, twice, first before the magistrate judge, and later, before a district judge.

20 One of the reasons for the court's rejection of Microsoft's argument is that the warrant is an extension of the court's power over a party over whom it has personal jurisdiction, notwithstanding that the property in question is located overseas. Another and more important reason is that the location of the information is not tied to the location of the servers, but the location of the ISP, which in Microsoft's case, was the US. Yet another reason was that Congress' intention under the SCA was to

9 *Re a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation* (29 August 2014) [2014] WL 4629624 (SDNY).

10 18 USC (US) §§ 2701–2712.

11 As amended 1 December 2015.

12 Signed at Washington on 6 January 1994.

compel ISPs to produce information "under their control", even if it was stored abroad; location of the servers storing that information is therefore irrelevant.

21 The situation was complicated by the fact that Ireland's municipal laws which Microsoft's subsidiary is naturally subjected to, including laws protecting privacy such as the Data Protection Acts 1988 and 2003,[13] permit the disclosure of personal data only in very limited circumstances, for instance, by an order of a Irish court. That was exactly what Microsoft highlighted in their brief in the appeal which has not yet been ruled on by the US Court of Appeals for the Second Circuit.

22 Microsoft further emphasised, in its opening brief in the appeal, the far-reaching practical implications which it said were self-evidently undesirable:[14]

> Imagine this scenario. Officers of the local Stadtpolizei investigating a suspected leak to the press descend on Deutsche Bank headquarters in Frankfurt, Germany. They serve a warrant to seize a bundle of private letters that a New York Times reporter is storing in a safe deposit box at a Deutsche Bank USA branch in Manhattan. The bank complies by ordering the New York branch manager to open the reporter's box with a master key, rummage through it, and fax the private letters to the Stadtpolizei.

23 While this case may be slightly more peculiar to the US because of the invocation of the SCA, the concerns of extraterritoriality are not to be treated lightly because information and data, especially those that are processed by the major technology companies like Microsoft, Google and Apple, are stored around the world and hence subject to the laws of multiple jurisdictions. In this day and age, lawyers cannot expect to thrive with just their knowledge of domestic procedural law.

13 Data Protection Commissioner, Data Protection Acts 1988 and 2003: Informal Consolidation (January 2009).

14 See http://digitalconstitution.com/wp-content/uploads/2014/12/Microsoft-Opening-Brief-120820141.pdf (accessed 2 March 2016).

Digesting the information obtained

24 Not all information that is associated with the dispute and can, in practical terms, be obtained ends up in court proceedings. What type of information ends up in court proceedings depends to a large extent on the filtration process applied to the raw data or information, such that only data relevant to the precise cause of action is sieved out and disclosed. This is a necessary step particularly in relation to storage platforms that can house huge quantities of data such as cloud storage. According to one survey, cloud forensics is one of the reasons for the growth in spending on electronic discovery services from US$2.7bn in 2007 to US$4.6bn in 2010.[15]

25 Retrieving digital information with that level of precision is no longer a simple task of isolating a few key words or searches and expecting a short list of hits. Specificity is key. Accordingly, discovery in litigation is not as simple now as pulling up a series of emails, or files stored in one or a few computers and providing the same to the other party. A system, or at least an approach, is needed to translate useless digits of electronically stored information ("ESI") into meaningful data which can serve as evidence in court proceedings.

26 That is where tools, specially developed to assist in the filtration process, come in handy. Developed just in the last decade or so, technology-assisted review ("TAR") tools, as these software tools are called, enable users to sift through large amounts of data for patterns using preset parameters. TAR has been authoritatively defined as:[16]

> A process for Prioritizing or Coding a Collection of Documents using a computerized system that harnesses human judgments of one or more Subject Matter Expert(s) on a smaller set of Documents and then extrapolates those judgments to the remaining Document

15 G Lawton, "Cloud Computing Crime Poses Unique Forensic Challenges" (January 2011) <http://searchcloudcomputing.techtarget.com/feature/Cloud-computing-crime-poses-unique-forensics-challenges> (accessed 19 August 2015).

16 M Grossman & G Cormack, "The Grossman-Cormack Glossary of Technology-Assisted Review" (2013) Fed Courts L Rev 7 at 32.

> Collection. Some TAR methods use Machine Learning Algorithms to distinguish Relevant from Non-Relevant Documents, based on Training Examples Coded as Relevant or Non-Relevant by the Subject Matter Experts(s), while other TAR methods derive systematic Rules that emulate the expert(s)' decision-making process. TAR processes generally incorporate Statistical Models and/or Sampling techniques to guide the process and to measure overall system effectiveness.

27 This computer, analytics-based review approach is not only helpful in managing copious amount of ESI, it also reduces man-hours required to manually sort out documents, and decreases the error rate and inconsistencies produced by manual review,[17] all of which ultimately lowers legal costs associated with discovery.[18] It is worth mentioning that traditional document review methods have been estimated by the *Rand Report* – under the auspices of the Rand Institute for Civil Justice – to constitute 73% of the total cost discovery where ESI is involved.[19] Unsurprisingly, therefore, TAR has been gaining prominence in litigation disputes, with Peck J in *Rio Tinto plc v Vale SA*[20] ("*Rio Tinto*") going out on a limb to say

17 The inconsistency rate between reviewers is typically as high as 70%; in other words, different reviewers looking at the same document would only agree with each other on the relevance of those documents an average of 30% of the time: E M Voorhees, "Variations in Relevance Judgments and the Measurement of Retrieval Effectiveness" (2000) 36 Info Processing & Mgmt 697 at 701. In a later study, the agreement rate was calculated to be 16%: see H L Roitblat, A Kershaw & P Oot, "Document Categorization in Legal Electronic Discovery: Computer Classification vs Manual Review" (2010) 61 J Am Society for Info Sci & Tech 70 at 74; and M R Grossman & G V Cormack, "Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient than Manual Review" (2011) 17 Rich J L & Tech 11 at 10–11.

18 The Sedona Conference, "The Sedona Conference Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery" (2007) 8 *Sedona Conference Journal* 189 at 195 <https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20Best%20Practices%20Commentary%20on%20Search%20%2526%20Retrieval%20Methods> (accessed 11 Nov 2015).

19 N M Pace & L Zakaras, *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery* (Rand Institute for Civil Justice, 2012) at p 97.

20 14 Civ 3042 (RMB)(AJP) (2 March 2015).

that TAR will be approved by courts whenever it is requested by the producing party.[21]

28 What is surprising is that notwithstanding judicial endorsement of TAR,[22] it has not yet caught on in a bigger way. This is, in part, attributable to the broader conundrum within the legal profession: whether to continue conducting discovery as it has always been practiced, in other words, in the paper world, or alternatively, embrace new ways of thinking in today's digital world.[23]

29 While the legal profession has made some progress in generally acknowledging the new reality of the digital world and its demands on the way discovery has to be conducted,[24] the rate of buy-in for TAR in particular has been painfully slow. There is no escaping from the fact that lawyers, across the board and generally speaking, are responsible. This has happened for at least two reasons.

30 The first is that lawyers are themselves not even familiar with the "what" and "who" questions described earlier. TAR is irrelevant to those who do not even understand that there is digital information out there that could benefit from review and management. Add to that the preference of lawyers to operate within their comfort zone, and their ignorance of the power and utility of TAR, it is little wonder that TAR has not gained more

---

21 *Rio Tinto plc v Vale SA* 14 Civ 3042 (RMB)(AJP) (2 March 2015) available at http://pdfserver.amlaw.com/ltn/14-3042_Peck_Order.pdf (accessed 8 March 2016) at p 2.

22 In addition to *Rio Tinto plc v Vale SA* 14 Civ 3042 (RMB)(AJP) (2 March 2015), see also *National Day Laborer Organizing Network v US Immigration & Customs Enforcement Agency* 877 F Supp 2d 87 at 109 (2012) (SDNY) and *Victor Stanley, Inc v Creative Pipe, Inc* 250 FRD 251 at 256–257 (2008).

23 The Sedona Conference, "The Sedona Conference Commentary on Achieving Quality in the E-Discovery Process" (2009) 10 *Sedona Conference Journal* 229 at 302 <https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20Commentary%20on%20Achieving%20Quality%20in%20the%20E-Discovery%20Process> (accessed 11 November 2015).

24 The Sedona Conference Working Group Series, "The Sedona Conference Commentary on Achieving Quality in the E-Discovery Process" (WG1, December 2013) at p 1.

traction.[25] The truth is that, its name and abbreviation notwithstanding, TAR is not *that* alien a concept to grasp. Lawyers, like most other people connected to the digital world, experience it all the time in their everyday lives. Whether it is navigating Netflix or googling, the predictive technology inherent in TAR is what enables websites to suggest products or features based on our browsing behaviours. On this note, efforts such as the *Grossman-Cormack Glossary of Technology-Assisted Review*[26] to create a common vocabulary, including the aforementioned definition of TAR, to advance the appreciation and development of this area of litigation practice are to be welcomed.

31 The second, arguably more pressing concern, is even if lawyers know what and who to look out for, they are generally reluctant to change.[27] They either simply do not appreciate the value of TAR,[28] or worse still, are overly, unduly and even irrationally protective over the type of work that has to be handled by people who are qualified to be lawyers. It would be unfair to pin everything on profit motivation, which is what a cynic may use as an explanation – lawyers manually sifting through documents while charging by the hour will invariably generate more profit for the firm than a computer doing the same job at a much faster rate (leaving aside for the moment the legitimate assumption that TAR will produce more accurate results). But the profit margin that human review inherently affords is undeniably lucrative.[29]

32 Nevertheless, resisting TAR for short-term gains is probably not sustainable. Susskind warns of the danger of complacency and

25 R C Losey, "Predictive Coding and the Proportionality Doctrine: A Marriage Made in Big Data" (2013-2014) 26 *Regent University Law Review* 6 at 11–13.

26 (2013) Fed Courts L Rev 7.

27 Although this is a very generalised statement, it is not without basis: see for example, S Slater, "Corporate Counsel Slow to Embrace E-Discovery Technology Advances According to Survey by BDO Consulting" (21 October 2015).

28 G A Vance, "Confessions of an E-Discovery Lawyer: We're Light Years Behind" *LegalTech News* (23 June 2015).

29 The same point was alluded to in the *Rand Report*: see N M Pace & L Zakaras, *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery* (Rand Institute for Civil Justice, 2012) at p 76.

fossilisation of old practices befalling the legal profession.[30] On the contrary, disruptive legal technologies, of which TAR is just one, should not be viewed as the enemy, but the angel of salvation from unbearable hours of mundane, brain-numbing document review work, and for at least three good reasons.

33 First, a lawyer who can spend one hour less reviewing a document manually can spend that extra hour gained refining the strategy that will win the case, managing his client, preparing the evidence and so on. In the long run, the value from such higher order services will translate to a more sustainable, if not profitable, practice. Second, as alluded to briefly earlier, it is far more likely that a manual human inspection will be less accurate and effective than a TAR-inspection.[31] It must be remembered that an ineffective and unreliable discovery system can prejudice the final result. Third, there will be firms who will be employing various forms of TAR to their advantage and to the disadvantage of their opponents who do not have such capabilities. So, the question for lawyers is not whether TAR spells leaner bills for their clients, but really one of survival. To employ a tennis metaphor made famous by Lord Mance in a leading UK Supreme Court decision,[32] while clients may be willing to put up with starting a dispute without the advantage of serve, very few clients can stomach a handicap of 0-40 despite paying a premium.

34 There are, of course, early adopters within the legal profession who believe in the future of TAR. To bolster their confidence in the system, and to turn the naysayers, it is imperative that the courts redouble their efforts at cultivating an efficient and seamless electronic discovery ecosystem. This may be easier said than done,

30 See generally, R Susskind, *Tomorrow's Lawyers: An Introduction to Your Future* (Oxford University Press, 2013).

31 See D Blair & M Maron, "An Evaluation of Retrieval Effectiveness for a Full-Text Document-Retrieval System" (1985) Communications of the ACM 289. For a more recent study, see B Hedin *et al*, "Overview of the TREC 2009 Legal Track" at http://trec.nist.gov/pubs/trec18/papers/LEGAL09.OVERVIEW.pdf (accessed 4 September 2015).

32 In *Dallah Real Estate and Tourism Holding Company v The Ministry of Religious Affairs, Government of Pakistan* [2010] UKSC 46 at [30].

but it must be done. In this connection, courts should be alive to three areas of concern.

35 The first is the residual skepticism over the reliability of TAR. It is true that TAR, particularly those based on predictive coding, is only as effective as the source document is. If there are errors in the source document, such as typographical errors, TAR may be less reliable than a human eye which can instantly recognise the typographical errors (assuming the eye has not glossed over the words, that is). It is also true that the TAR algorithm may miss out relevant documents. TAR is not the panacea. As Peck J explained in his seminal article:[33]

> [I]f the use of predictive coding is challenged in a case before me, I will want to know what was done and why that produced defensible results. I may be less interested in the science behind the "black box" of the vendor's software than in whether it produced responsive documents with reasonably high recall and high precision ... Proof of a valid "process," including quality control testing will be important.

36 However, there are many answers that can be given to these fears. First, practice approximates perfect. More frequent and extensive usage of TAR will enable both lawyers and the service providers of TAR to get a better handle of the needs and nuances of litigation, thus resulting in a more effective deployment of TAR. Second, the more adopters of TAR there are, the more investments will go into improving the various technologies, and the more accurate and reliable the technologies will be. The current level of optical character recognition technology is a good example of how much scope for improvement there is in any given technology. Third, even though the process is not perfect, there are safeguards that can be built into the process to control the quality of the output. Fourth, in any event, the real comparison is not between the ideal TAR system and the present ones available, but between current technology and manual review, on the whole. In efficacy terms, there is no doubt who is the winner in that contest.

33 A Peck, "Search, Forward" (2011) LTN 25 at 29.

37 The second area of concern relates to disputes over protocols designed for the purposes of TAR. Recently, the court in *Rio Tinto* appointed a special master to help the parties resolve disputes over the execution of their negotiated TAR predictive coding protocol.[34] The fact that a dispute even arose is noteworthy, not so much because it suggests the ineffectiveness of TAR, but that such disputes which invariably lengthens the dispute resolution process and inflates legal fees and costs if left unchecked have the propensity to undermine the broader electronic discovery movement.

38 Last but not least, transparency expectations, especially over methodologies, have also had a chilling effect on adoption. It was a major issue in *Monique Da Silva Moore v Publicis Groupe SA and MSL Group*[35] ("*Da Silva*") and *Re Actos (Pioglitazone) Products Liability Litigation*.[36] In *EORHB, Inc v HOA Holdings LLC*,[37] the court ordered the parties to show cause why they should not select and share a single TAR vendor (even though the court eventually respected the parties' desire not to adopt that approach). Anecdotally, when lawyers and their clients hear that they may need to share documents that are not relevant to the litigation, many of them would prefer not to share those documents than reap the benefits of partaking in TAR.[38] Proponents of TAR, including the courts, must therefore work towards engineering a framework for the disclosure of training sets and non-responsive ESI that adequately balances the needs and interests of the disclosing party as well as the recipient party.

39 The hard truth as parties and courts have come to realise is that not all TAR tools are alike or equally effective, and without transparency and cooperation, "predictive coding" is nothing but a

34 *Rio Tinto plc v Vale SA* 14 Civ 3042 (RMB)(AJP) (2 March 2015). See also http://www.recommind.com/blog/predictive-coding-protocol-comes-fire-judge-peck-appoints-special-master-rio-tinto (accessed 3 March 2015).

35 [2013] WL 4483531 (SDNY).

36 Case Management Order [2012] No 6:11-md-2299 (W D La, 27 July 2012).

37 *EORHB, Inc v HOA Holdings LLC* [2013] WL 1960621 (Del Ch).

38 According to the law firm, Gibson Dunn in their "2015 Mid-Year E-Discovery Update" (15 July 2015) <http://www.gibsondunn.com/publications/Pages/2015-Mid-Year-E-Discovery-Update.aspx> (accessed 4 September 2015).

magic word.[39] It is against this backdrop that attention may be paid to the Sedona Conference Cooperation Proclamation framework, which objective is:[40]

> [T]o promote open and forthright information sharing, dialogue (internal and external), training, and the development of practical tools to facilitate cooperative, collaborative, transparent discovery.

Costs of technology-assisted review and proportionality in litigation

40 As the preceding paragraphs suggest, the cost of sorting out digital information for the purposes of discovery is not an inexpensive endeavour. Cost is a material and legitimate issue to be concerned about because calibrating the right balance between ensuring all the relevant evidence is before the court on the one hand, and ensuring the costs of litigation which includes the costs associated with producing the evidence remains manageable on the other, is a pivotal consideration that prevails in discovery processes of all nature. The most comprehensive collection of all the available material is an evidential ideal, but it is equally if not more important to assess at every stage of the proceedings what information is actually needed to bring or defend a case and what is the cheapest way of getting the adequate minimum in front of the court.

41 As was stated in *Breezeway Overseas Ltd v UBS AG*:[41]

> The perennial tension in the law of civil procedure, *viz*, the attempt to achieve both justice and efficiency, comes to the forefront in the discovery process. On the one hand, it is *ex hypothesi* in the interest of justice that all relevant material is discovered, while on the other, there is a pressing need to ensure efficiency lest injustice be

39 W P Butterfield, C R Crowley & J Kenney, "Reality Bites: Why TAR's Promises Have Yet to be Fulfilled" (Presented at DESI V: Workshop on Standards for Using Predictive Coding, Machine Learning and Other Advance Search and Review Methods, 14 June 2013) <http://www.umiacs.umd.edu/~oard/desi5/additional/Butterfield.pdf> (accessed 4 September 2015).

40 The Sedona Conference, "The Sedona Conference Cooperation Proclamation" (2009) 10 *Sedona Conference Journal* 331 (Supplement) at 331.

41 *Breezeway Overseas Ltd v UBS AG* [2012] 4 SLR 1035 at [20].

occasioned through the well-meaning but disproportionate attempt to ensure that all relevant material is disclosed.

42 It is axiomatic why proportionality (and reasonableness), not perfection,[42] is the cornerstone of discovery regimes in litigation. Justice is only as meaningful as it is accessible, and it is only accessible when it is not priced out of reach. Fixation with complete discovery can undermine the judicial process and hide the truth from being revealed. As Clarke J of the Supreme Court of Ireland puts it, "discovery remains an important tool for establishing the truth while at the same time ensuring that the cost and complexity of discovery does not, of itself, become a barrier to the truth being established".[43]

43 Therefore, the application of TAR, however large its benefits, is not exempt from scrutiny under the proportionality principle. Indeed, proportionality is not always or easily achievable especially in relation to disputes involving huge amounts of data or disputes between parties with a vast disparity in IT capabilities. As the new entrant seeking to dislodge the accepted, conventional practice of manual review, there is even more expectation on TAR to demonstrate that it is capable of producing optimum results at affordable prices.

44 Although the empirical evidence is in TAR's favour,[44] there is still a real and inherent possibility in every case for costs to escalate out of control, which will happen if lawyers for the disputing parties refuse to cooperate. This needs to be acknowledged and tackled.

---

42 See S Wortzman, "E-discovery the Basics: From Proportionality to Technology Assisted Review" presented at the Canadian Bar Association– 2012 Annual Competition Law Fall Conference (20–21 September 2015). In *Chen-Oster v Goldman, Sachs & Co* 285 FRD 294 at 306 (2012) (SDNY), the court said the "standard for the production of [electronically stored information] is not perfection".

43 The eDiscovery Group of Ireland, "Good Practice Guide to Electronic Discovery in Ireland" (16 April 2013).

44 See C H Paskach, F E Nelson & M Schwab, "The Case for Technology Assisted Review and Statistical Sampling in Discovery" (Position Paper for DESI VI Workshop, ICAIL Conference, 8 June 2015) <http://www.umiacs.umd.edu/~oard/desi6/papers/paskach.pdf> (accessed 24 November 2015).

45 Where ESI is involved, the inherent informational asymmetry present in litigation is heightened. The requesting party generally develops requests without actual access to the information requested,[45] and is very much at the mercy of the disclosing party. Accordingly, it is only with cooperation in identifying and fulfilling legitimate discovery needs, and also in avoiding requests for discovery in circumstances where the cost and burden of such discovery is disproportionately large to what is at stake in litigation, that inefficiencies both in terms of time and costs can be kept to a minimum.

46 Lawmakers have a big part to play in moving this transition along, which will reduce the incidence of disputes about the adequacy of discovery of ESI.[46] For instance, rule 26(g) of the Federal Rules of Civil Procedure[47] in the US, requires that every discovery disclosure, request, response or objection must be signed by at least one attorney of record, or the client if unrepresented. By signing, the attorney in effect warrants that the disclosure or discovery request is based on a belief formed after reasonable inquiry, is not interposed for any improper purpose, and is neither unreasonable nor unduly burdensome or expensive. Sanction may follow if an attorney violates this rule. The more lawyers hold themselves to the higher standards like those implicit in rule 26(g), the easier it will be to engender cooperation in individual cases.[48]

---

45 D W Oard & W Webber, "Information Retrieval for E-Discovery" (2013) 7 Foundation & Trends in Info Retrieval 99 at 106.

46 In *EEOC v McCormick & Schmick's Seafood Rests, Inc* [2012] WL 380048 at 4 (D Md), the court observed that where a producing party "generates the search terms on its own, the inevitable result will be complaints that the terms were inadequate".

47 As amended 1 December 2015.

48 See *Mancia v Mayflower Textile Services Co* 253 FRD 354 at 357–358 (2009) (D Md) where Grimm J noted:

> One of the most important, but apparently least understood or followed, of the discovery rules is Fed R Civ P 26(g), enacted in 1983. The rule requires that every discovery disclosure, request, response or objection must be signed by at least one attorney of record, or the client, if unrepresented. … The signature 'certifies that to the best of the person's knowledge, information, and belief *formed after a reasonable inquiry*,' the disclosure is complete and correct, and that the discovery request, response or objection is: (a) consistent with the rules of procedure and

(*continued on the next page*)

47 The latest set of proposed amendments to rules 1, 16 and 26 of the US Federal Rules of Civil Procedure[49] came into effect 1 December 2015, encourages greater cooperation between parties, more intense judicial case management, and stronger emphasis on the principle of proportionality in discovery proceedings, all with the overarching objective of securing the just, speedy and inexpensive determination of every action, is another small step in the right direction. Legislative steps such as these will undoubtedly consolidate the gains made in sharpening the focus of discovery applications.

48 Nonetheless, for a broader overhaul in philosophy from opposition to one of cooperation whenever TAR is employed in discovery, it is the courts who have the greatest role to play. First, courts should exert more control over the discovery process, for instance, by laying down more specific and extensive rules and guidelines for the production of ESI.

49 Grimm J's model standard discovery order is a helpful starting point. In it, he suggests that courts may stipulate that absent an order of court upon a showing of good cause, a party from whom ESI has been requested shall not be required to search for responsive ESI:[50]

> (a) from more than ten (10) key custodians;
>
> (b) that was created more than five (5) years before the filing of the lawsuit;

---

warranted by existing law (or by a nonfrivolous argument for extending, modifying, or reversing existing law, or for establishing new law); (b) is not interposed for any improper purpose (such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation); and (c) is neither unreasonable nor unduly burdensome or expensive, (considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action). … If a lawyer or party makes a Rule 26(g) certification that violates the rule, without substantial justification, the court (on motion, or *sua sponte*) must impose an appropriate sanction, which may include an order to pay reasonable expenses and attorney's fees, caused by the violation.

49 As amended 1 December 2015.

50 See http://iaals.du.edu/sites/default/files/documents/publications/grimm_discovery_order.pdf (accessed 22 September 2015).

(c) from sources that are not reasonably accessible without undue burden or cost; or

(d) for more than 160 hours, inclusive of time spent identifying potentially responsive ESI, collecting that ESI, searching that ESI and reviewing that ESI for responsiveness, confidentiality, and for privilege or work product protection.

50 Second, once the rules and guidelines are established, courts must not hesitate to police them with sanctions,[51] or at the very least, show their displeasure when standards are not complied with.[52] The worst rules are those which everyone knows are symbolic, because not only is the intended effect not realised as the rules will invariably be disregarded, the principle underlying those rules will be disrespected.

51 Last but certainly not the least, courts should make the electronic discovery waters easier to navigate. Supporting legal education is the most obvious way, because until lawyers are educated about the fundamentals of e-discovery technologies and the capabilities of the e-discovery industry service providers, they will never be able to properly advise their client or execute the process.[53] In *Zubalake v UBS Warburg*,[54] the court even noted that it was an obligation of the counsel to identify "key players" and communicate with them "to understand how they stored information" relevant to the proceedings.[55]

---

51 See for example, *EI du Pont de Nemours & Co v Kolon Industries, Inc* 911 F Supp 2d 340 (2012) (ED Va); *Innospan Corp v Intuit, Inc* [2012] WL 1144272 (ND Cal); *Taydon v Greyhound Lines, Inc* [2012] WL 2048257 (DDC).

52 See for example, *Clay v Consol Pa Coal Co* 2013 US District LEXIS 129809 at 4 (ND W Va); *1100 West, LLC v Red Spot Paint & Varnish Co* [2009] WL 1605118 at 29 (SD Ind); and *Phoenix Four, Inc v Strategic Resources Corp* [2006] WL 1409413 at 6 (SDNY).

53 P Oot, A Kershaw & H L Roitblat, "Mandating Reasonableness in a Reasonable Inquiry" (2010) 87 Denv U L Rev 533 at 535; and L Katz, "A Balancing Act: Ethical Dilemmas in Retaining E-Discovery Consultants (2009) 22 Geo J Legal Ethics 929 at 940–941.

54 229 FRD 422 (2004) (SDNY).

55 *Zubalake v UBS Warburg* 229 FRD 422 at 432 (2004) (SDNY).

52 Other ways for the courts to advance the e-discovery movement include providing objective definitive guidance through judgments and rulings. The lack of such guidance in the search process, for instance, has been well-documented.[56] Moreover, proportionality and reasonableness are relatively amorphous concepts with contours that are not always visible or even fixed. A reasonable search is reasonable not on some idealised notion of adequacy, but "reasonable under the circumstances".[57] Maximum effort should therefore be directed at giving clearly articulated guidance in court decisions on the factors relevant to the court's determination.

53 The courts should also establish and refresh, where necessary, guidelines and practice directions on electronic discovery.[58] Legal ethics codes should also be revised to reflect the principle, and reality, that cooperation between lawyers does not conflict with their duty to advance their client's interest, but enhances it, as was so eloquently explained in the Sedona Conference Cooperation Proclamation.[59] Needless to say, the courts should as far as possible overtly champion the use of TAR, as the Singapore courts have done on several occasions, including in *Global Yellow Pages Ltd v Promedia Directories Pte Ltd*[60] where the court stated that search technologies and document review and management tools can "bring efficiency to civil litigation practice, especially during discovery … [and which] if used adroitly, will lower the costs of litigation".[61]

---

56 The Sedona Conference, "The Sedona Conference Commentary on Achieving Quality in the E-Discovery Process" (2009) 10 *Sedona Conference Journal* 229 at 315–316 <https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20Commentary%200n%20Achieving%20Quality%20in%20the%20E-Discovery%20Process> (accessed 11 November 2015).

57 *Re Delta/Airtran Baggage Fee Antitrust Litigation* 846 F Supp 2d 1335 at 1350 (2012) (ND Ga).

58 Practice Direction 3 of 2009; Pt V of the Supreme Court Practice Directions.

59 The Sedona Conference, "The Sedona Conference Cooperation Proclamation" (2009) 10 *Sedona Conference Journal* 331 (Supplement) at 331.

60 [2013] 3 SLR 758.

61 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2013] 3 SLR 758 at [41]. See also *Sanae Achar v Sci-Gen Ltd* [2011] 3 SLR 967 at [13]–[14].

54 In the end, however, judicial signaling and thought leadership can only go so far. The ultimate responsibility for adapting to the times lies with the lawyers. Fortunately, there are a few bright spots. In May 2015, Dentons, a global law firm, announced that it was launching a new initiative called NextLaw Labs which will develop, deploy and invest in new technologies and processes to transform the practice of law around the world.[62] As law firms extend their services beyond their home borders, there is every chance that there will be cross-pollination of technology-driven best practices and philosophies.

CONCLUSION

55 In this golden age of data generation, one is guaranteed that litigation practice in the 21st century will not be homogenous. One began this century with emails, telephone records and recordings as the major sources of digital data in litigation. What one will see at the end of the century in all probability has not yet been invented. What one can be certain about is that emails, telephone records and recordings will probably feature very little in the discovery process because new technologies will take their place. Knowing that now, lawyers who wish to stay ahead of their peers will take concrete steps to keep up with the technology, understand the opportunities TAR bring, and apply those customised technologies when the situation calls for it. Those who choose not to do so will very quickly find themselves fossilised in the permafrost of irrelevance.

---

62 See Dentons website http://www.dentons.com/en/whats-different-about-dentons/connecting-you-to-talented-lawyers-around-the-globe/news/2015/may/dentons-launches-nextlaw-labs-creates-legal-business-accelerator (accessed 14 December 2015).

The Global Technology Law Conference 2015, held over two days on 29 and 30 June 2015, is the second in a series of international conferences delving into the issues thrown up by the collision of law and disruptive technologies. The conference grappled with legal and regulatory issues in the wake of financial technologies, or Fintech, and the challenges to data protection and intellectual property law associated with big data.

This book collects a series of articles that deal with these topics in much greater depth. The views articulated at the conference form the bedrock of these articles. It is hoped that the ideas and views captured between these covers will contribute to the development of jurisprudence in this exciting and ever-changing area of law.

ISBN 978-981-09-8864-7